

Zero Trust Network Access

Alejandro Leal

January 29, 2024



LEADERSHIP
COMPASS
2024

Zero Trust Network Access (ZTNA) is becoming increasingly essential as organizations adapt to remote work, cloud adoption, and the growing sophistication of cyber threats. Unlike traditional perimeter-based security models, ZTNA treats every user, application, or resource as untrusted and enforces strict security, access control, and comprehensive auditing to ensure visibility and accountability of all user activities. In this Leadership Compass, we provide an overview of the existing solutions implementing a holistic approach to Zero Trust methodology, enabling secure yet convenient access to business applications and resources for users, regardless of their location. A comprehensive examination of the market segment, vendor service functionality, relative market share, and innovative approaches to providing ZTNA solutions are all contained in this report.

Contents

Contents	2
Executive Summary	4
Highlights	5
Market Segment	6
Delivery Models	7
Required Capabilities	9
Leadership	10
Overall Leadership	11
Product Leadership	12
Innovation Leadership	14
Market Leadership	16
Correlated View	18
The Market/Product Matrix	19
The Product/Innovation Matrix	21
The Innovation/Market Matrix	23
Products and Vendors at a Glance	25
Product/Vendor evaluation	28
Spider graphs	28
Absolute Software – Absolute Software Secure Access	30
Akamai Technologies – Akamai Enterprise Application Access, Akamai MFA	33
Barracuda Networks – Barracuda CloudGen Access	36
Broadcom – Symantec Zero Trust Network Access (ZTNA)	39

Cato Networks – Cato SASE Cloud.....	42
Check Point – Quantum SASE.....	45
Cisco – Secure Access.....	48
Cloudflare – Cloudflare Access.....	51
Ergon – Airlock Secure Access Hub.....	54
Fortinet – Fortinet Universal ZTNA.....	57
Forum Systems – Forum Sentry.....	60
Ivanti – Ivanti Neurons for Zero Trust Access.....	63
Jamf – Jamf Connect.....	66
Lookout – Lookout Secure Private Access.....	69
NetFoundry – CloudZiti and OpenZiti.....	72
Sophos – Sophos ZTNA.....	75
Systancia – Systancia Gate.....	78
TrustBuilder – TrustBuilder.io.....	81
Zero Networks – Zero Networks Connect.....	84
Vendors to Watch.....	87

Executive Summary

Traditional network security models have faced unprecedented challenges in adapting to the demands of a rapidly changing digital environment. As businesses embrace digital transformation and become increasingly cloud-native, mobile, and interconnected, the corporate network perimeter is gradually disappearing, exposing users to malware, ransomware, and other cyber threats. Traditional perimeter security tools no longer provide adequate protection from these threats. But even more so, traditional remote access solutions like virtual private networks (VPN) can no longer ensure the scalability and performance needed for the increasingly mobile and remote workforce.

VPN is a typical example of a technology that was never designed for the purposes it is used nowadays. Besides creating potential bottlenecks by forcing companies to backhaul remote users' traffic to a central location and thus negatively affecting performance and productivity, VPN appliances grant those users full, uncontrolled access to entire local area networks (LANs). This dramatically expands the attack surface of corporate networks, provides easy lateral movement for potential attackers, and enables uncontrolled access to internal resources with implicit trust.

Unlike traditional perimeter-based security models that assume trust within the network, Zero Trust Network Access (ZTNA) adopts a more granular and identity-centric approach. An infrastructure designed around this model treats every user, application, or resource as untrusted and enforces strict security, access control, and comprehensive auditing to ensure visibility and accountability of all user activities. This Zero Trust philosophy has become increasingly relevant as organizations grapple with the proliferation of remote work, cloud adoption, and the growing sophistication of cyber threats. It is also important to emphasize that Zero Trust is not only about networks, but about identities, devices, systems, and applications. It is about ubiquitous and continuous verification of device security and identity authentication.

As a concept, ZTNA is based on the assumption that any network is always hostile, and thus, any IT system, application, or user is constantly exposed to potential external and internal threats. Often expressed as "never trust, always verify," ZTNA is an embodiment of the principle of least privilege, and at its core mandates that every access request be properly authenticated and authorized. Proper access management in service of ZTNA means considering the requesting user's attributes, authentication and environmental context, permissions and roles, source device information, and the requested resource attributes. Zero Trust Architecture implies a concept where clients can access services from everywhere, not relying only on internal network security mechanisms.

This approach ensures that access policies can be defined in a much more granular fashion per individual application or service by establishing secured point-to-point tunnels between clients and services. Each of these sessions is always authenticated and continuously monitored to prevent malicious activities. Access and security policies are managed centrally and enforced across hybrid IT environments (on-premises, multi-cloud, or mobile).

One of the fundamental misconceptions the industry experts are still struggling to explain to the public is that Zero Trust is not an off-the-shelf product, but a journey that begins with a

long-term business strategy and focuses on a step-by-step implementation, using existing or readily available tools and technologies, while maintaining the continuity of business processes and avoiding adding even more complexity to the existing architecture. Overcoming these challenges requires a holistic approach, involving careful planning, stakeholder education, and collaboration with experienced cybersecurity professionals.

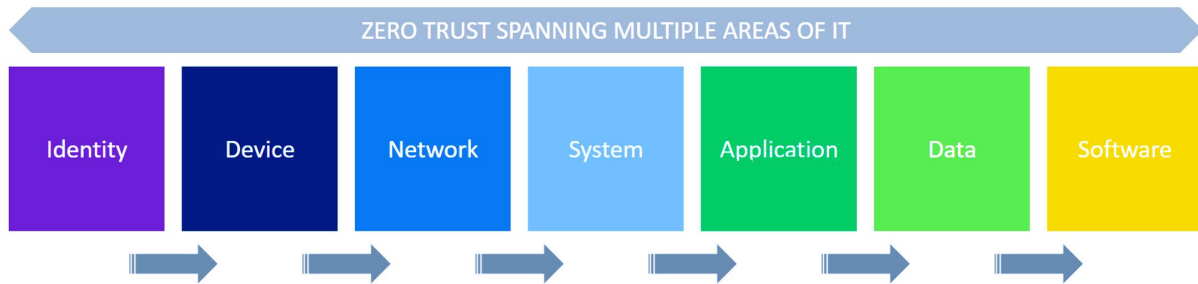


Figure 1: Zero Trust spanning multiple areas of IT

In this Leadership Compass, we provide an overview of the existing solutions implementing this approach. They might be based on different underlying technologies and focus on different aspects of the Zero Trust methodology, but fundamentally, all of them solve the same problem: enabling secure yet convenient access to business applications and other resources for users regardless of their location, whether in an office, at home or anywhere else.

To better understand the fundamental principles this report is based on, please refer to [KuppingerCole’s Research Methodology](#).

Highlights

- The market for ZTNA solutions is currently experiencing significant growth. Both large established vendors and small but innovative startups are offering a multitude of solutions that promise to address various usage scenarios: simplified cloud migration, seamless hybrid and multi-cloud architectures, or a modern replacement for VPN.
- KuppingerCole Analysts predicts that the Zero Trust Network Access Market will reach \$7.34 billion in 2025, with a Compound Annual Growth Rate (CAGR) of 17.4%. The largest share of the global revenue in this market segment is North America, currently representing 47.4% of the total market size. It is followed by EMEA and APAC with 25.7% and 18.2% respectively.
- The emergence of the ZTNA paradigm signifies a pivotal shift in security strategy, reflecting the realization that the conventional castle-and-moat approach is no longer sufficient in safeguarding today's dynamic and distributed IT ecosystems. Unlike traditional perimeter-based strategies, ZTNA operates under the assumption that no entity, whether inside or outside the network, should be inherently trusted.
- Zero Trust architectures have gained enormous popularity as more secure, yet flexible and future-proof alternatives to traditional perimeter-based security. By eliminating the very notion of a trusted system, ZT architectures enforce strict identity

verification and least-privilege access policies for every user, device, or application, regardless of where they are located.

- ZTNA is the key technology that enables modern Zero Trust architectures, together with comprehensive identity management, strong multi-factor authentication, and real-time behavior analytics. Besides dramatically reducing the attack surface and preventing lateral movement for hackers (and thus significantly improving security posture), it has the potential to greatly simplify both the users' and administrators' experiences.
- While ZTNA offers enhanced security by adopting a least-privilege access model, potential downsides include the need for careful implementation and potential complexity, especially in larger organizations.
- The Overall Leaders in Zero Trust Network Access are (in alphabetical order): Absolute Software, Akamai Technologies, Broadcom, Cato Networks, Check Point, Cisco, Cloudflare, Fortinet, Jamf, Lookout, NetFoundry, and Sophos.

Market Segment

This report shows that the ZTNA market is diverse, with different vendors offering specialized solutions to address specific aspects of ZTNA. While some vendors offer comprehensive ZTNA solutions that address multiple use cases and deployment scenarios, it's important to understand the specific strengths of each vendor. The diversity of organizational requirements, infrastructure, and use cases often leads to a best-of-breed approach, where the strengths of different vendors are leveraged to create a robust and customized ZTNA strategy. Enterprises should carefully evaluate their unique needs, taking into account factors such as scalability, integration capabilities, and specific security requirements, to determine the vendor that best aligns with their ZTNA goals.

The ZTNA market was catalyzed in response to the shift to remote and hybrid work and the limitations of traditional virtual private network (VPN) and perimeter-based security models. Recognizing the need for a more granular, identity-centric, and adaptive security approach, vendors began developing solutions that align with the principles of Zero Trust. This market evolution is fueled by a collective industry realization that securing access to critical resources must be based on continuous verification and authorization, irrespective of the user's location or the device used.

As opposed to traditional network-centric architectures, ZTNA platforms work completely independently from the underlying hardware, appliances, switches, or other network devices and can be deployed across multiple environments and managed from a centralized control plane. This approach ensures that access policies can be defined in a much more granular fashion per individual application or service by establishing secured point-to-point tunnels between clients and services. Each of these sessions is always authenticated and continuously monitored to prevent malicious activities. Access and security policies are managed centrally and enforced across hybrid IT environments (on-premises, multi-cloud, or mobile).

As a result, users are only granted access to the necessary applications and data, greatly reducing the overall attack surface and practically eliminating lateral movement. Since only the

control plane is centralized, no bottlenecks are introduced into the data plane, ensuring scalability and consistent user experience. ZTNA architectures provide a unified layer of abstraction that ensures that enterprise application access can be entirely driven by common policies regardless of their deployment – this enables multiple scenarios like simplified cloud migration, seamless hybrid, and multi-cloud architectures, and an additional security layer for mitigating network-based attacks.

Most recently, the concept of Secure Access Service Edge (SASE) has emerged, which converges network and security solutions into a unified and tightly integrated platform that is entirely delivered from the cloud, dramatically reducing the complexity of corporate network infrastructures, and offering consistent productivity and protection at a global scale. However, in this Leadership Compass, we do not plan to cover all aspects of modern Zero Trust and SASE architectures, although we do recognize that some vendors are offering their ZTNA products as a part of bigger SASE solutions.

Instead, in this report, we delve into the intricacies of the ZTNA market, exploring the key players, technological innovations, and broader implications for cybersecurity and IT professionals. As organizations seek more resilient and agile security postures, understanding the principles and implementations of ZTNA will be critical to navigating the complex cybersecurity landscape of the future. Therefore, we are looking for comprehensive, scalable and flexible platforms that enable organizations to replace their legacy solutions and VPNs with fine-grained, secure, authenticated and audited access to corporate applications and resources that works consistently across heterogeneous IT environments.

We expect these solutions to implement management on the application, not networking level, maintaining uniform policies regardless of location, even across the public Internet. We presume modern ZTNA solutions to be scalable without practical limitations, based on open identity and security standards, and agnostic to the specific application or network protocols.

Delivery Models

To meet the diverse needs of organizations, ZTNA solutions can be deployed in a variety of ways. One of the defining features of Zero Trust as a concept is that its principles are universally applicable to a wide variety of use cases covering nearly every area of the IT industry. This is one of the biggest reasons for its enduring popularity – applying ZT strategically can help to dramatically reduce overall complexity and minimize the technical debt of any organization’s existing IT landscape. However, most products currently offered under the “Zero Trust” label are only designed to address a specific, often quite narrow selection of those use cases.

For example, some solutions are designed to meet the needs of a mobile workforce. These solutions ensure secure access for users connecting from different locations, often using various devices. Some ZTNA solutions prioritize identity as a crucial parameter in the security equation. This approach emphasizes verifying and continuously monitoring the identity of users throughout their access journey. Therefore, organizations must carefully evaluate ZTNA offerings to ensure that they address their unique requirements and provide security measures for different types of users and scenarios.

Even within the fairly specific segment of ZTNA solutions, we can find products targeted toward solving problems so substantially different that it implies radically different architectures and deployment scenarios. Although “VPN replacement” or rather the enablement of convenient and yet secure remote access to business resources is currently the most popular driver for ZTNA adoption, it is by no means the only one.

Securing access to sensitive data in complex hybrid and multi-cloud environments, securing data flows in distributed cloud-native applications, enabling secure and compliant onboarding of BYOD devices in organizations, and preventing lateral movement of malware and malicious actors these are just a small subset of popular applications of ZTNA architectures. Some of these use cases imply a massively scalable, cloud-native architecture that can accommodate complex traffic patterns between thousands of microservices or other cloud workloads. Others might benefit from a fully managed offering delivered as a service. For others still, the ultimate deployment flexibility across hybrid environments is a crucial factor.

Whether such scenarios place more focus on adaptive access management, threat prevention, data loss or security analytics can also greatly affect the choice of the most appropriate solution for your specific ZTNA project. A fundamental difference between modern ZTNA and legacy VPN solutions is the separation of control and data planes, which can be set up in different environments and still enable a single point of management and visibility across complex deployments. Most vendors offer a fully managed cloud-based control plane for their customers as an option, while other vendors focus on SaaS delivery as their only solution. Organizations operating in highly regulated industries or large enterprises might require a fully on-premises deployment, even for their control planes, which is addressed by some vendors offering their products in a fully containerized form.

Since the data plane of a ZTNA architecture must by its very nature encompass the whole corporate networking landscape and even go beyond it to accommodate remote workers, vendors usually offer a broad variety of deployment options for their gateway components, which perform traffic routing and access management. These can vary from a simple piece of software to be deployed into an application container to an enterprise-grade customer-managed on-premises gateway setup or even an SDK to be embedded directly into a microservice. The scope of different use cases and deployment scenarios vary between vendors—some would offer a broad range of connectivity options, while others would focus more on the scalability and ease of deployment of their managed cloud-native solutions.

In any case, connecting an end-user device to a ZTNA platform requires an agent, a piece of software not dissimilar from a traditional VPN client. These agents come in various shapes as well. Some are highly specialized, others support multiple connectivity options (to enable coexistence with legacy VPNs, for example), and some vendors even have partnerships with third party companies to include their technology into existing endpoint agents.

Since the minimization of the overall number of agents deployed to endpoint devices is a popular usability requirement, many vendors even include agentless capabilities in their products. However, it is important to stress that this functionality is usually limited to a small number of supported protocols (HTTP for web apps, RDP for remote desktop, and SSH for remote shell access) and, arguably, does not fully conform to the tenets of Zero Trust. Still, it

remains a very popular feature that enables additional use cases for ZTNA solutions – such as providing fine-grained and controlled access to contractors and external administrators without any investment into additional infrastructure.

In the end, understanding the balance between the most urgent business drivers and pain points within the organization and the investments and changes required for the strategic implementation of Zero Trust should be the primary decision factor for choosing the most appropriate deployment model. The choice of deployment model depends on factors such as organizational structure, security requirements, scalability needs, and the geographic distribution of users and resources. However, one should always keep in mind that the journey toward Zero Trust is a never-ending one, and requirements tend to change quickly. Deployment flexibility determined by the range of the deployment scenarios supported by a vendor is, therefore, an important consideration for any purchase decision. Organizations should conduct a thorough analysis of their specific requirements, considering performance, scalability, user experience, security, compliance, resource control, integration, and cost implications to select a deployment model that aligns with their overall objectives and priorities.

Required Capabilities

ZTNA solutions play a crucial role in today's cybersecurity landscape, requiring specific capabilities to ensure protection. These solutions fundamentally align with the principles of Zero Trust, extending its influence across devices, networks, systems, applications, and data. This holistic perspective aligns with the broader Zero Trust framework, emphasizing the importance of trust verification at every layer. Therefore, ZTNA has proven to be the most popular first step towards the strategic adoption of Zero Trust for organizations of all sizes and industries around the world.

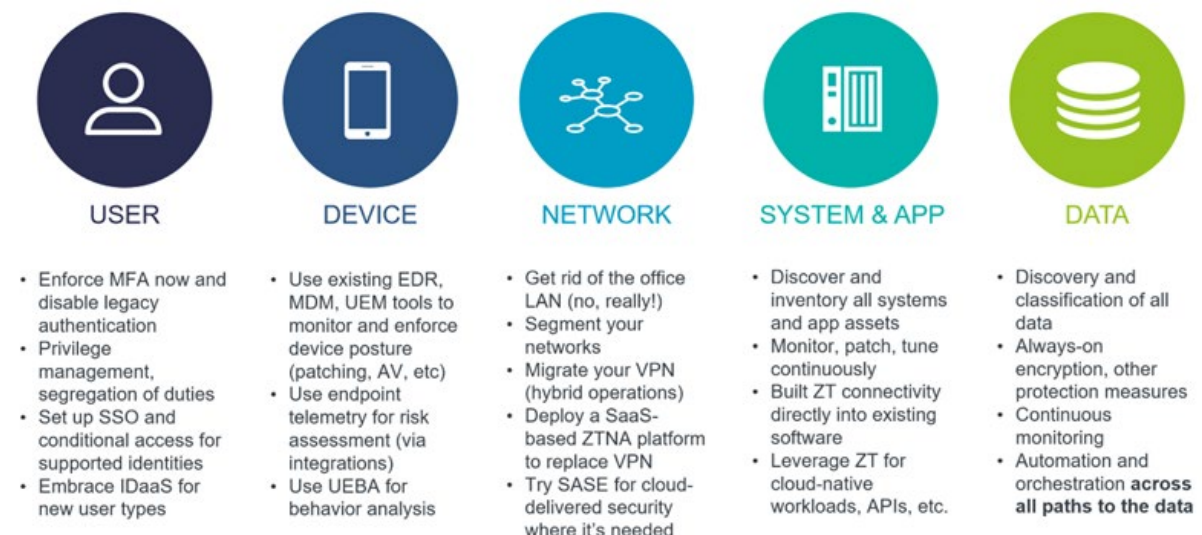


Figure 2: Zero Trust as an integral part of every IT aspect

In this Leadership Compass, we focus primarily on solutions that can address all of the use cases listed below, at least to a sufficient degree. To ensure a comprehensive and rigorous assessment, we have identified the following required capabilities.

- Application-level, not network-level segmentation
- No reliance on inbound connections
- Separation of control and data planes
- Cloud-only, on-premises, or hybrid deployments
- Scalable, decentralized architecture to reduce latency
- Centralized, unified deployment and management across hybrid networks
- Unified, network-agnostic access policy management
- Encryption of all network connections
- Strict identity verification for each session
- Device posture validation as a prerequisite for access
- Multi-factor authentication, single sign-on support
- Continuous session monitoring, anomaly detection
- Additional threat protection capabilities
- Built-in reporting and compliance audit functions

When evaluating ZTNA platforms, organizations should carefully evaluate how each solution addresses these requirements to ensure that they select a platform that aligns with their security goals and operational needs. In this report, we explicitly exclude solutions that are based on the coarse-grained access control paradigms like traditional VPNs or products not focusing on application-level segmentation. This also includes alternative approaches toward Zero Trust implementation such as reverse-proxy architectures. We also expect software-defined perimeter solutions not to require deployments of additional specialized hardware or making substantial changes in existing network infrastructures.

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept (PoC) and pilot phase, based on the specific criteria of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership

- Innovation Leadership
- Market Leadership

Overall Leadership

The Overall Leadership rating provides a consolidated view of all-around functionality, innovation, market presence, and financial position. However, these vendors may differ significantly from each other in terms of product features, platform support, and integrations. Therefore, we strongly recommend looking at all the leadership categories as well as each entry in chapter 5 to get a comprehensive understanding of the players in this market and what use cases they support best.

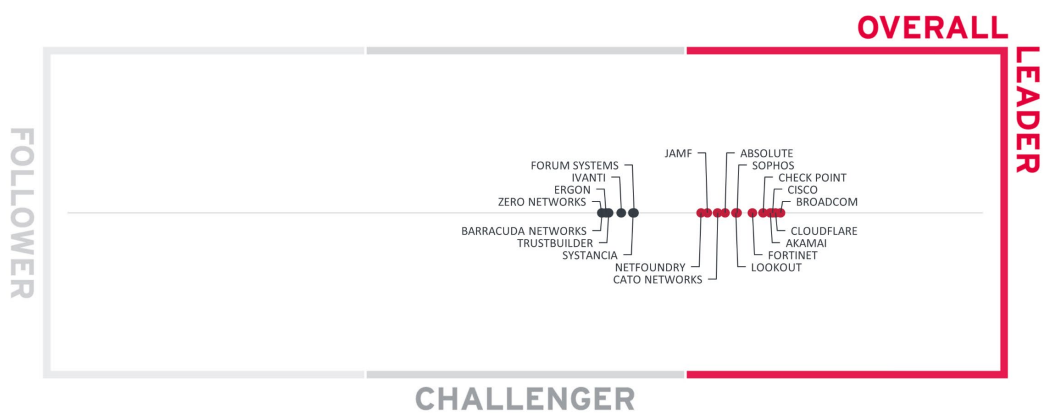


Figure 3: The Overall Leadership rating for the ZTNA market segment

Overall Leaders are (in alphabetical order):

- Absolute
- Akamai
- Broadcom
- Cato Networks
- Check Point
- Cisco
- Cloudflare
- Fortinet
- Jamf
- Lookout
- NetFoundry
- Sophos

Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services. In the Product Leadership rating, we look specifically for the functional strength of the vendors' solutions, regardless of their current ability to grab a substantial market share.

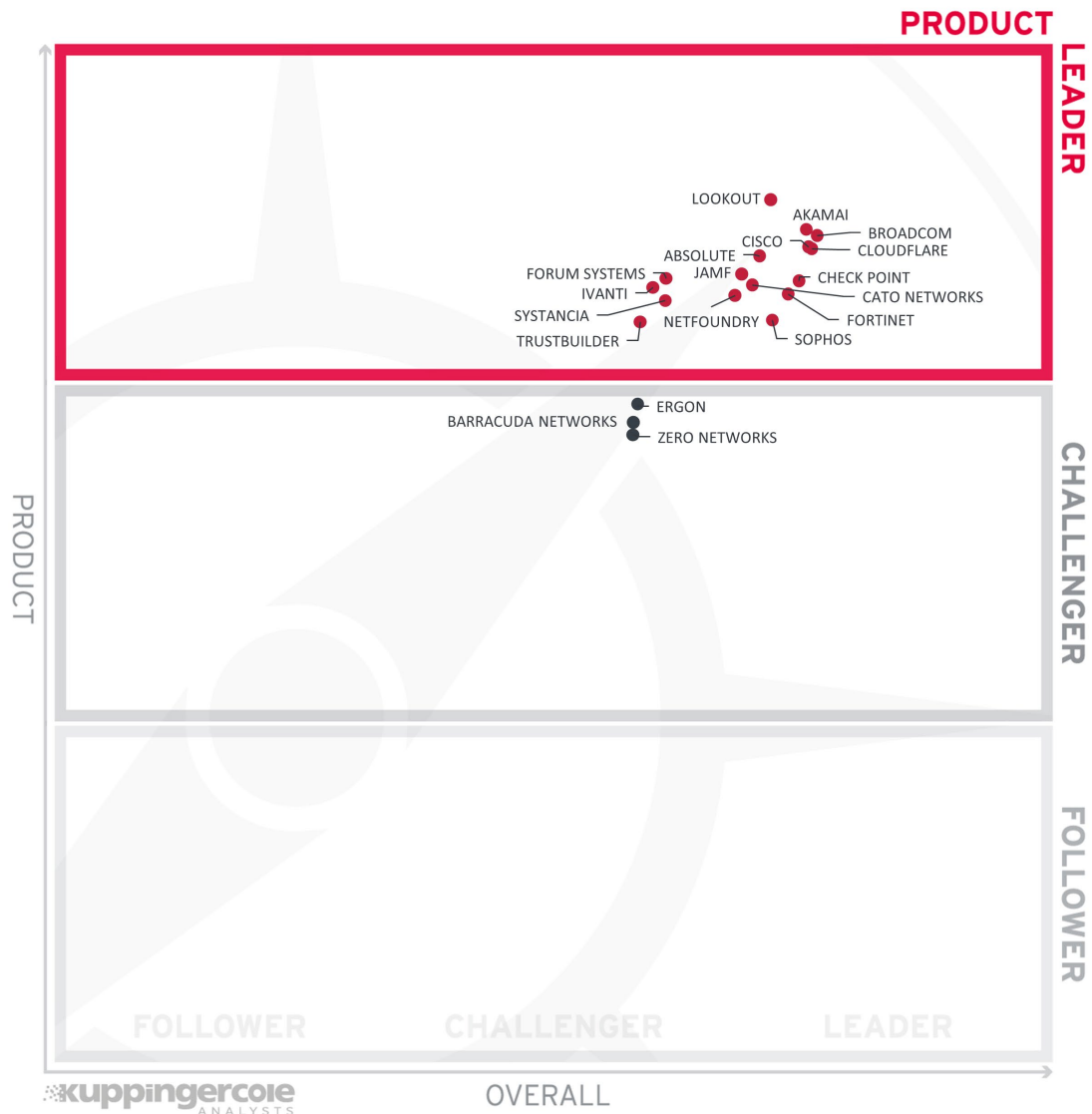


Figure 4: The Product Leaders in the ZTNA market

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

Product Leaders (in alphabetical order):

- Absolute
- Akamai
- Broadcom
- Cato Networks
- Check Point
- Cisco
- Cloudflare
- Fortinet
- Forum Systems
- Ivanti
- Jamf
- Lookout
- NetFoundry
- Sophos
- Systancia
- TrustBuilder

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

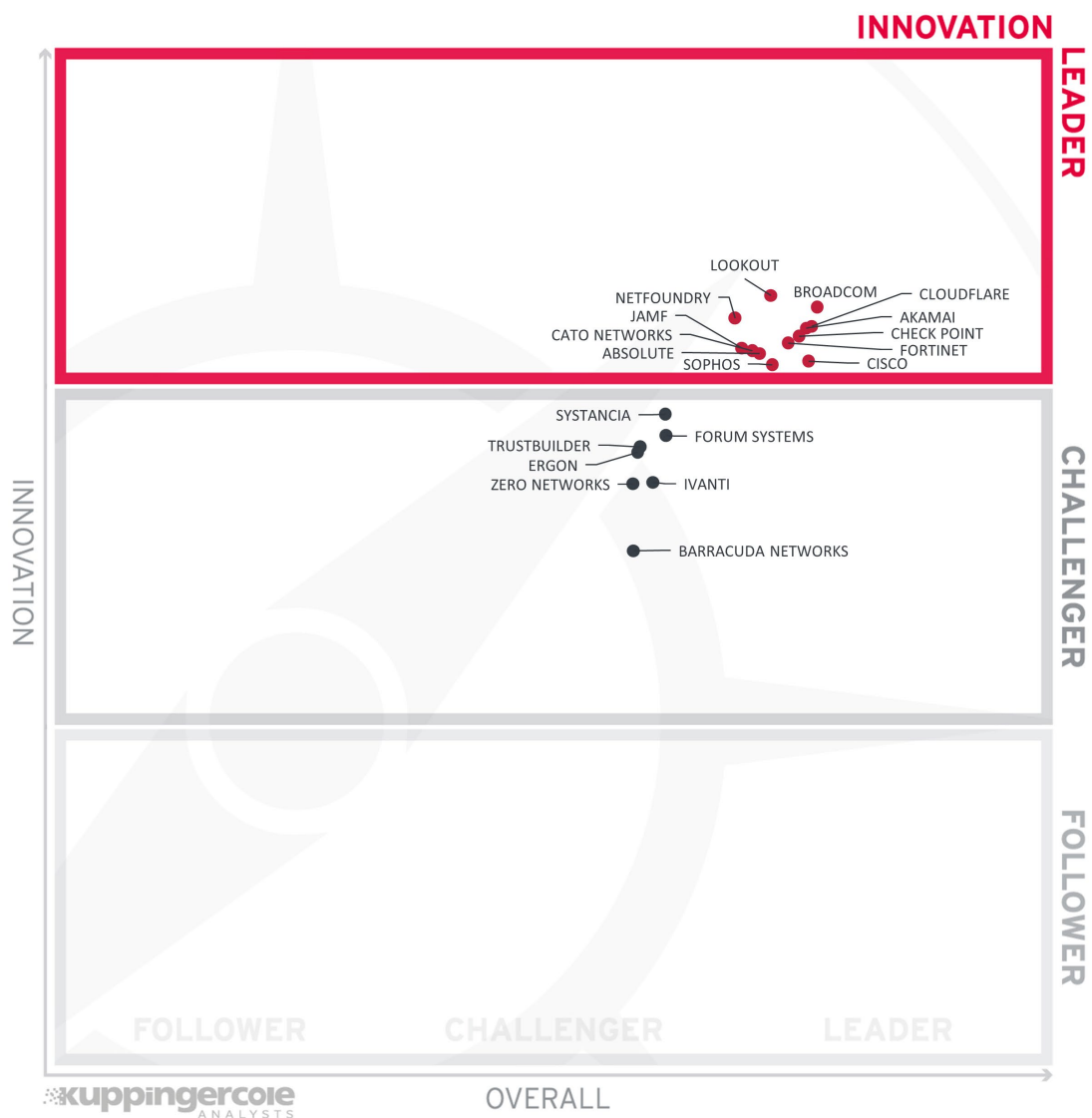


Figure 5: The Innovation Leaders in the ZTNA market

Innovation Leaders (in alphabetical order):

- Absolute

- Akamai
- Broadcom
- Cato Networks
- Check Point
- Cisco
- Cloudflare
- Fortinet
- Jamf
- Lookout
- NetFoundry
- Sophos

Market Leadership

Lastly, we analyze Market Leadership. This is an amalgamation of the number of customers, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

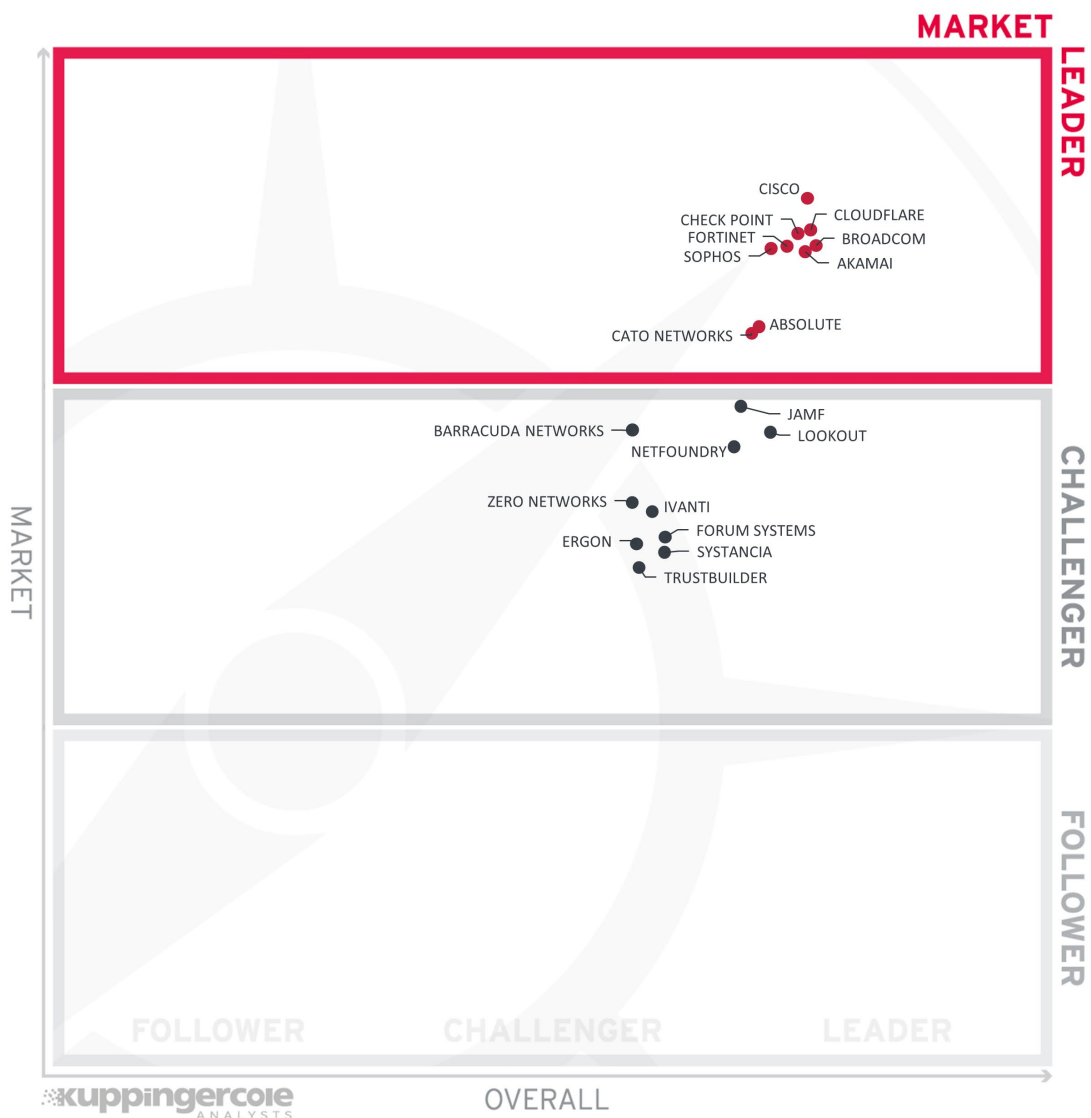


Figure 6: The Market Leaders in the ZTNA market

Market Leaders (in alphabetical order):

- Absolute
- Akamai
- Broadcom
- Cato Networks
- Check Point
- Cisco
- Cloudflare
- Fortinet
- Sophos

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix

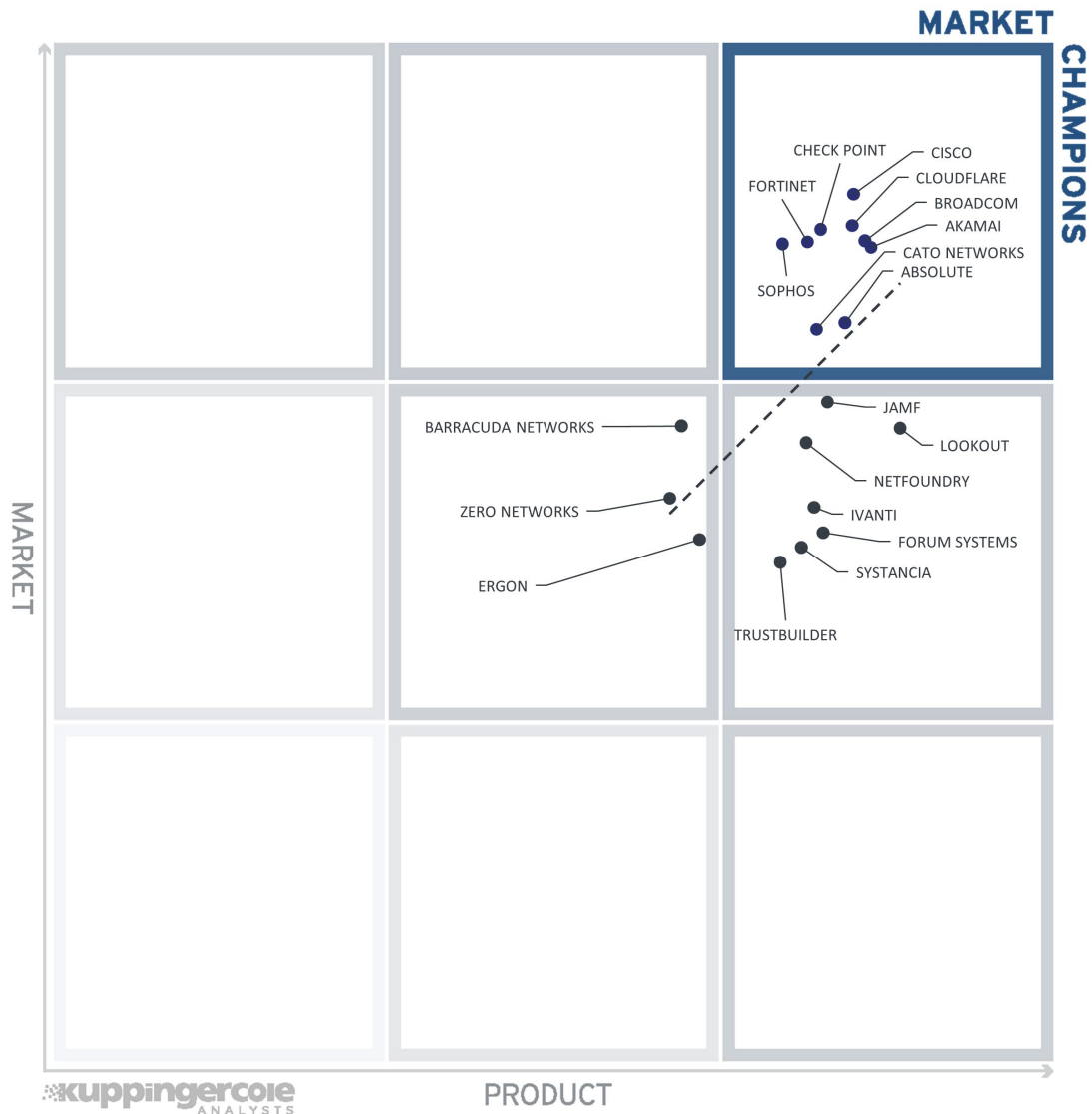


Figure 7: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line could be considered “overperformers” when comparing Market Leadership and Product Leadership.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

In the upper right segment, we find “Market Champions.” Here we see a group of long-established players in the same box, including (in alphabetical order) Absolute, Akamai, Broadcom, Cato Networks, Check Point, Cisco, Cloudflare, Fortinet, and Sophos.

In the middle right-hand box, we see a number of vendors that deliver strong product capabilities for ZTNA but are not yet considered Market Champions. Forum Systems, Ivanti, Jamf, Lookout, NetFoundry, Systancia, and TrustBuilder have a strong potential to improve their market position due to the more robust product capabilities they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not market leaders. They also have moderate market success as compared to market champions. These vendors include (in alphabetical order): Barracuda Networks, Ergon, and Zero Networks.

The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

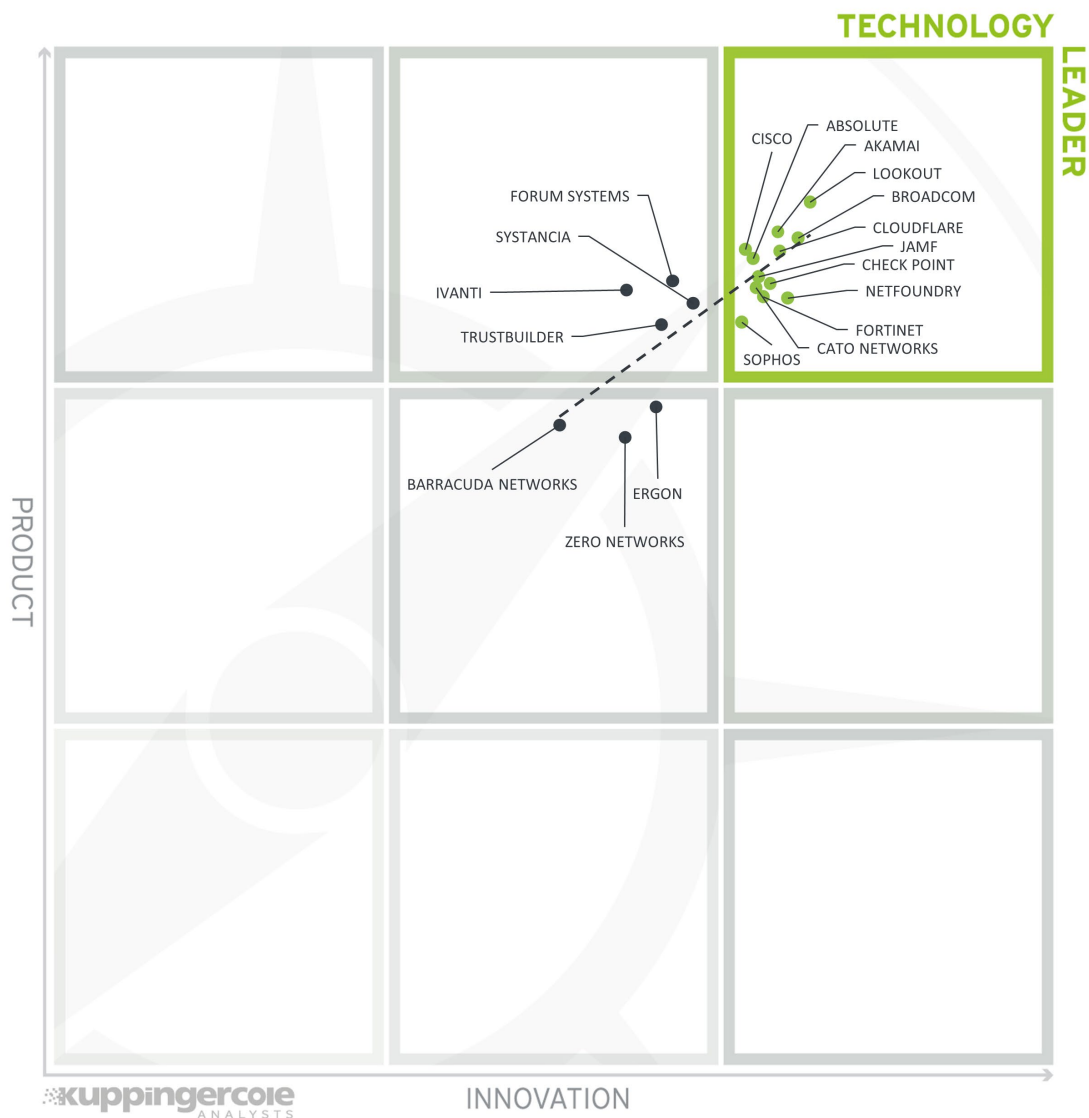


Figure 8: The Product/Innovation Matrix

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating. Many vendors placed close to the dotted line, indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most leading vendors scattered throughout the box in the upper right corner. The leading vendors are Absolute, Akamai, Broadcom, Cato Networks, Check Point, Cisco, Cloudflare, Fortinet, Jamf, Lookout, NetFoundry, and Sophos.

Four vendors appear in the top middle box with good products but less innovation than the leaders, including Forum Systems, Ivanti, Systancia, and TrustBuilder.

The rest of the vendors appear in the middle box, showing both innovation and product strength, which includes (in alphabetical order): Barracuda Networks, Ergon, and Zero Networks.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

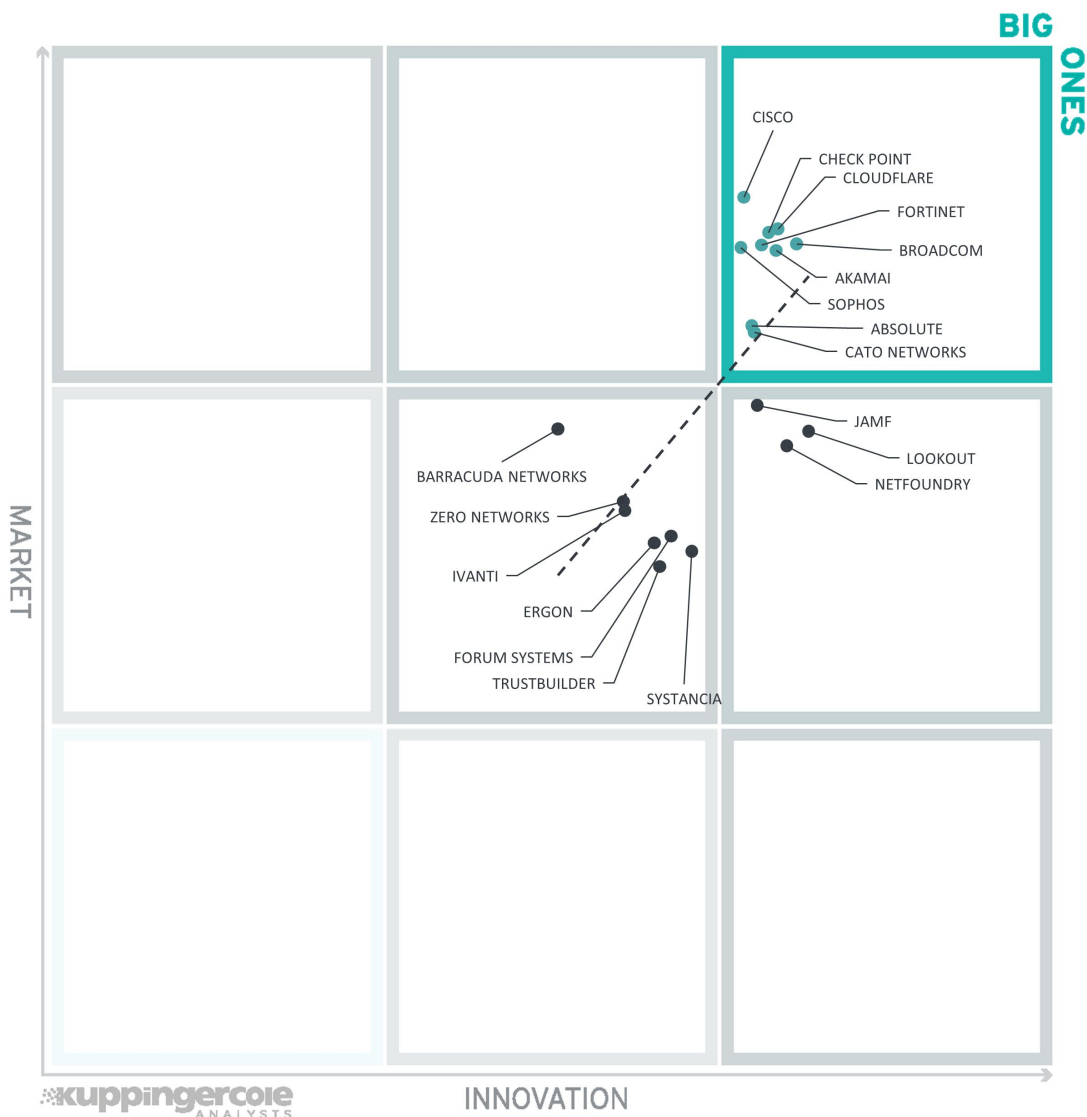


Figure 9: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

In the upper right-hand corner box, we find the “Big Ones” in the ZTNA market. We see (in alphabetical order) Absolute, Akamai, Broadcom, Cato Networks, Check Point, Cisco, Cloudflare, Sophos, and Fortinet.

Three vendors, Jamf, Lookout, and NetFoundry, are shown in the middle right box showing good innovation with slightly less market presence than the vendors in the “Big Ones” category.

The segment in the middle of the chart contains a third of the vendors rated as challengers both for market and innovation, which includes (in alphabetical order) Barracuda Networks, Ergon, Forum Systems, Ivanti, Systancia, TrustBuilder, and Zero Networks.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Zero Trust Network Access. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name

Vendor	Security	Functionality	Deployment	Interoperability	Usability
Absolute Software	Strong Positive	Positive	Strong Positive	Strong Positive	Positive
Akamai Technologies	Strong Positive	Strong Positive	Positive	Strong Positive	Positive
Barracuda Networks	Positive	Positive	Positive	Positive	Positive
Broadcom	Strong Positive	Strong Positive	Strong Positive	Positive	Positive
Cato Networks	Strong Positive	Positive	Strong Positive	Neutral	Positive
Check Point	Strong Positive	Positive	Positive	Positive	Strong Positive
Cisco	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Cloudflare	Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Ergon	Strong Positive	Positive	Positive	Positive	Positive
Fortinet	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Positive
Forum Systems	Strong Positive	Positive	Positive	Strong Positive	Positive
Ivanti	Positive	Strong Positive	Positive	Positive	Strong Positive
Jamf	Positive	Strong Positive	Positive	Positive	Strong Positive
Lookout	Strong Positive	Strong Positive	Positive	Positive	Strong Positive

NetFoundry	Strong Positive	Positive	Positive	Positive	Strong Positive
Sophos	Strong Positive	Positive	Positive	Positive	Strong Positive
Systancia	Strong Positive	Positive	Strong Positive	Neutral	Strong Positive
TrustBuilder	Positive	Positive	Positive	Positive	Positive
Zero Networks	Positive	Positive	Positive	Positive	Positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
Absolute Software	Positive	Positive	Positive	Positive
Akamai Technologies	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Barracuda Networks	Neutral	Neutral	Positive	Neutral
Broadcom	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Cato Networks	Positive	Positive	Positive	Neutral
Check Point	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Cisco	Positive	Strong Positive	Strong Positive	Strong Positive
Cloudflare	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Ergon	Neutral	Neutral	Neutral	Neutral
Fortinet	Positive	Strong Positive	Strong Positive	Positive
Forum Systems	Neutral	Neutral	Neutral	Positive
Ivanti	Neutral	Neutral	Positive	Neutral
Jamf	Positive	Neutral	Positive	Positive
Lookout	Strong Positive	Neutral	Neutral	Positive
NetFoundry	Strong Positive	Neutral	Neutral	Positive
Sophos	Positive	Strong Positive	Strong Positive	Strong Positive
Systancia	Neutral	Neutral	Neutral	Weak
TrustBuilder	Neutral	Neutral	Neutral	Positive
Zero Networks	Neutral	Neutral	Weak	Neutral

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For Zero Trust Network Access solutions covered in this report, we look at the following categories:

- **Secure Connectivity** – all communications between resources must be secured, regardless of their locations, using end-to-end encryption of any network traffic between resources. The assessment in this category examines the fundamental capabilities of the solution, including its support for secure point-to-point connections, complete cloaking of the underlying network architecture, legacy VPN solutions, and management of inbound connections. The examination also delves into the encryption standards used, explicitly questioning the support for modern transport-level security standards and the deprecation of legacy encryption protocols like TLS 1.1.
- **Access Management**—this section focuses on the solution's compatibility with external systems for authentication and authorization, emphasizing supported standards or integrations. This evaluation explores critical aspects of the solution's ability to manage and enforce access policies. It examines the user interface for creating and editing policies, policy auditing tools, access control principles, and more.
- **Strong Authentication** —must be dynamic and strictly enforced. This includes the use of strong multi-factor authentication, scanning for cyberthreats, and re-evaluating trust before each transaction. It is driven by dynamic policies that continuously evaluate the state of the resource, requester, and other contextual attributes. For example, this assessment looks at support for various authentication protocols, including FIDO 2.0, U2F, UAF, FIDO authenticators, and security keys. It examines continuous authentication capabilities, step-up authentication support, graphical visualization, and risk assessment policy configuration. Overall, this evaluation provides organizations with valuable insight into the solution's device and authentication intelligence capabilities, helping them make informed decisions for their Zero Trust strategies.
- **Client Risk Posture**—each access decision is made based on real-time risk evaluation that may include behavioral analysis, environmental conditions, history of

previous accesses, etc. performed either using the platform's own agent or by analyzing the telemetry collected through partnerships and integrations with third-party security vendors.

- **Monitoring and Analytics**—information about the current state of assets and their communications must be collected, analyzed, and used to improve the organization's security posture. The integrity and security of all assets must be continuously monitored and deviations in security posture must be mitigated promptly. This section assesses the solution's capabilities in providing comprehensive insights, real-time visibility, and analytical tools for effective management.
- **Audit and Compliance**—Security data retention and comprehensive compliance reporting are the basic capabilities here. Out-of-the-box support for regulatory frameworks like GDPR, HIPAA, or PCI is a major differentiator for many customers.
- **Performance and Scalability**—ZTNA solutions must be able to withstand massive spikes in demand and adapt to complex, distributed deployments, and, of course, provide native support for cloud and hybrid scenarios.

These spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some products may have gaps in certain areas while being strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations—for example, for powering enterprise-grade security operations centers.

Absolute Software – Absolute Software Secure Access

Absolute Software is an endpoint and network security vendor headquartered in Seattle, Washington, USA. Founded in 1993, the company is known primarily for its products spanning service management, endpoint security, secure network access, application resilience, and ransomware recovery. In 2021, the company acquired NetMotion Software, a privately held company specializing in network security, VPN, and ZTNA. Furthermore, in May 2023, Absolute Software announced that it had been acquired by Crosspoint Capital Partners.

The Absolute Edge product, part of the Absolute Secure Access offerings, extends beyond the core capabilities of Absolute Core, incorporating Absolute ZTNA for an optimal user experience within the software-defined perimeter. It provides comprehensive visibility beyond the corporate perimeter, conducting continuous risk assessments using diverse data points to inform access policies. It also includes ZTNA policy actions, malware scanning, application hiding, web access and cloud application control based on contextual risk factors, and a self-healing Secure Access client for Windows. With a focus on restricting access to enterprise resources, irrespective of their hosting location, Absolute Edge also includes Absolute Insights for Network, featuring patented proactive diagnostics on devices and networks. This includes network performance analytics spanning cellular to public Wi-Fi, real-time geolocation dashboards, and threat categorization of domains visited by remote workers. Absolute Secure Access is designed to be easy to deploy, configure, and maintain, offering rich data analysis dashboards for detailed insights into threat defense, network performance, security enforcement, and more.

In addition, the Absolute Secure Web Gateway Service add-on module, powered by Ericom, is a cloud-delivered security solution that offers comprehensive protection for organizations with highly mobile and distributed workforces. Tightly integrated with Absolute Insights for Network, it provides detailed reporting on the overall impact of security policies, data leakage prevention, browser sessions, file transfers, and user feedback. Furthermore, the solution's telemetry capabilities provide valuable insight into both network performance and security, contributing to a robust and informed decision-making process. All SaaS applications are supported natively with no additional configuration while SaaS-specific security measures and policies can be configured on a per-customer basis. Absolute Software has a customer base primarily situated in North America and Latin America, with an expanding footprint in Europe, Japan, and Asia Pacific including Australia and New Zealand, catering to small to enterprise organizations. Notably, the company appears in all of the leadership categories of this Leadership Compass. This makes the Absolute Secure Access product line a good option in the market for organizations that are increasingly adopting a Zero Trust approach and considering enhancing traditional network access security measures.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive



Table 3: Absolute Software’s rating

Strengths

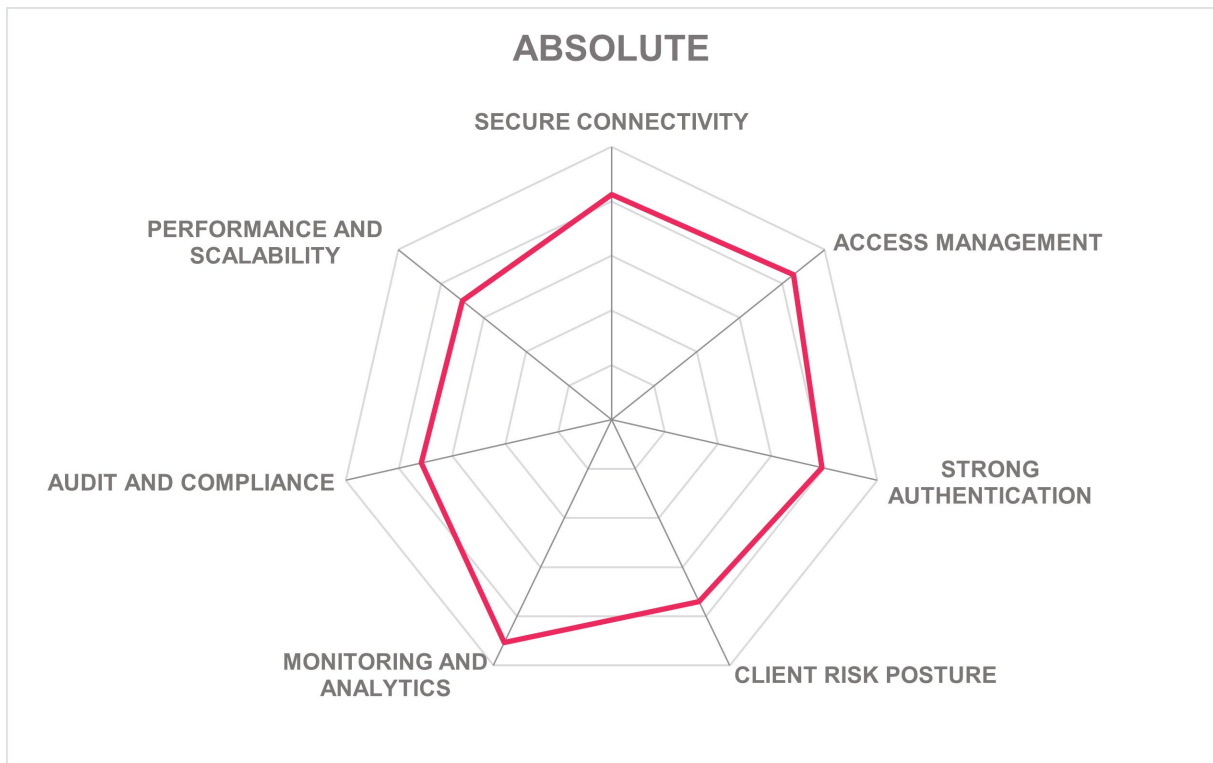
- Scalability across on-premises and mobile/remote infrastructure
- Easy to deploy and configure
- Strong telemetry capabilities
- Rich data analysis dashboard
- Seamless support for hybrid (ZTNA+VPN) scenarios
- Dynamic policies that are network and location-aware
- Specifically designed and optimized for mobile workers and devices
- Tight integration between endpoint and network security solution stacks

Challenges

- FIDO2 support would be beneficial
- Integration with third-party application catalogs is not currently supported
- Lack of graphical visualization and configuration of risk evaluation policies for customer administrators
- Small but growing presence outside of the North American and Latin American market

Leader in





Akamai Technologies – Akamai Enterprise Application Access, Akamai MFA

Akamai Technologies is headquartered in Cambridge, Massachusetts, USA. Founded in 1998, the company is one of the veteran players on the market, providing a broad range of performance-, security- and even productivity-related services through their massively distributed edge and cloud platform. Coverage is primarily focused on North America, APAC, and EMEA, but with a growing presence in Latin America as well.

Akamai's ZTNA solution is built on the Akamai Connected Cloud, which is a distributed platform for cloud computing, security, and content delivery. This allows the seamless insertion of acceleration to improve application performance and security for additional protection. The core products in Akamai's ZTNA solutions are Akamai Enterprise Application Access (EAA) and Akamai Multi-Factor Authentication (MFA). EAA facilitates secure and seamless access to applications for users, regardless of their location or device. It operates on a Zero Trust model, ensuring that access is granted based on identity and other contextual factors. EAA is deployed on the Akamai Connected Cloud. This ensures that every application is completely hidden from "trusted" public exposure regardless of where it is hosted – in a corporate LAN, on-premises datacenter, or in the public cloud. However, customer applications can be hosted anywhere—on-premises, private cloud, public cloud, or hybrid. The Akamai Connected Cloud is a significant differentiator, leveraging a robust infrastructure spread globally. This cloud infrastructure enhances the delivery of secure access services, contributing to a reliable and high-performance user experience. Furthermore, Akamai MFA is an advanced FIDO2 solution designed to enhance security by incorporating a phish-proof authentication factor secured through cryptography. It uses a smartphone app, eliminating the need for physical security keys and providing an easy-to-use experience. Akamai MFA effectively mitigates the risk of phishing attacks and aligns with the trajectory towards a passwordless future of authentication.

In addition, Akamai Enterprise Defender is a bundled solution that consists of Akamai EAA and Akamai Secure Internet Access (Secure Web Gateway/CASB). Nevertheless, additional application security and acceleration can be added. For example, Akamai WAAP for application security, Akamai API & Application Protector, Akamai API security, Akamai Prolexic for DDoS protection, and Akamai ION/IPA for acceleration. As a result, Akamai's cloud security services can be combined to create a Zero Trust solution tailored to your business needs. With its massive global edge infrastructure, integrations with all notable identity providers, and a strong focus on strong authentication, Akamai Enterprise Application Access is uniquely suited for large enterprises with hundreds of business applications and complex business requirements. Akamai appears in all leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive



Table 4: Akamai's rating

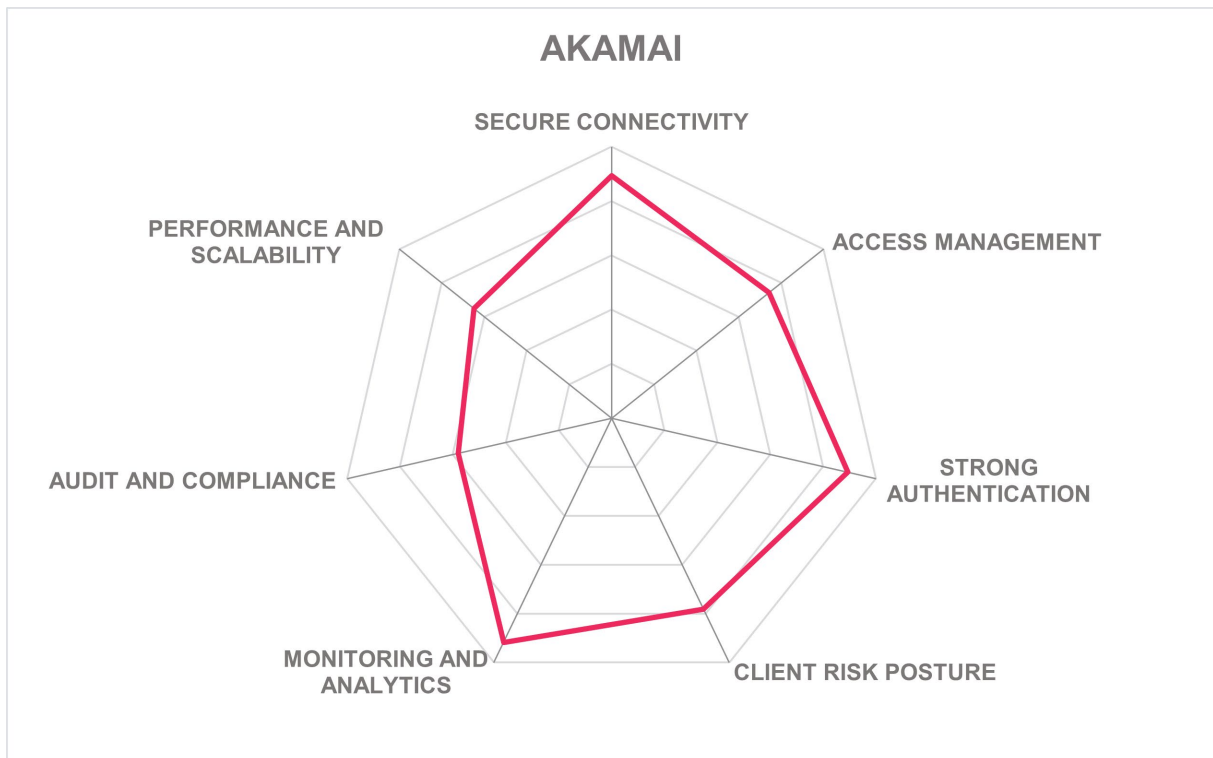
Strengths

- Native FIDO2 MFA support
- Cloud-native approach
- Strong authentication
- Global market presence
- Strong partner ecosystem
- Consistent enforcement of secure access policies
- Massive scale and availability of infrastructure in every region of the world
- Extends Zero Trust with threat protection, application performance, API security, and other security services

Challenges

- Dashboards do not support corporate look and feel customization
- More security certifications and compliance standards would be beneficial
- Deployment could be perceived as complex considering the diverse combination of solutions Akamai supports. However, Akamai offers professional services to help customers accelerate deployment from the initial pilot to full production.





Barracuda Networks – Barracuda CloudGen Access

Founded in 2003, Barracuda Networks is a company dedicated to creating a more secure digital environment for businesses worldwide. The company focuses on delivering security, networking, and storage products based on network appliances and cloud services. These include solutions specializing in data protection, email security, application security, remote connectivity, Zero Trust, and more. Barracuda Networks is headquartered in Campbell, California, USA. Coverage is primarily focused on North America and EMEA. In April 2022, the company announced that it had been acquired by Kohlberg Kravis Roberts & Co.

Barracuda CloudGen Access is a ZTNA solution that provides secure access to applications and workloads from any device and location while avoiding the performance limitations associated with traditional VPNs. CloudGen Access continuously verifies that only the right person, with the right device, and the right permissions can access company data or apps. It ensures that devices meet baseline security and compliance requirements before getting access. The solution delivers remote, conditional, and contextual access to resources, reducing over-privileged access and mitigating third-party risks. With CloudGen Access, employees and partners can securely access corporate applications and cloud workloads without introducing additional attack surfaces. The platform excels in securing contractor access, providing enhanced visibility into device and user activity, enabling role-based access, and safeguarding against risks associated with third-party network entry. Additionally, CloudGen Access facilitates agile DevOps and Kubernetes deployments, offering authorization, access management, and workflow management in multi-cloud or hybrid IT environments. Furthermore, by integrating with Identity Providers and employing advanced authentication methods like Certificate-Based Authentication and device posture analysis, CloudGen Access prevents MFA bypass attacks and safeguards against evolving risks. Notably, the platform now includes web security to protect users from malicious web content, ensuring a safe and productive work environment regardless of location.

In addition, Barracuda stands out from some of its counterparts by avoiding the practice of directing all application traffic through its cloud service. Instead, it offers selective backhauling, allowing IT professionals within enterprises to make informed decisions on where security inspections occur. Barracuda CloudGen Access is well-suited for enterprises modernizing their infrastructure while still needing to support mission-critical legacy applications.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



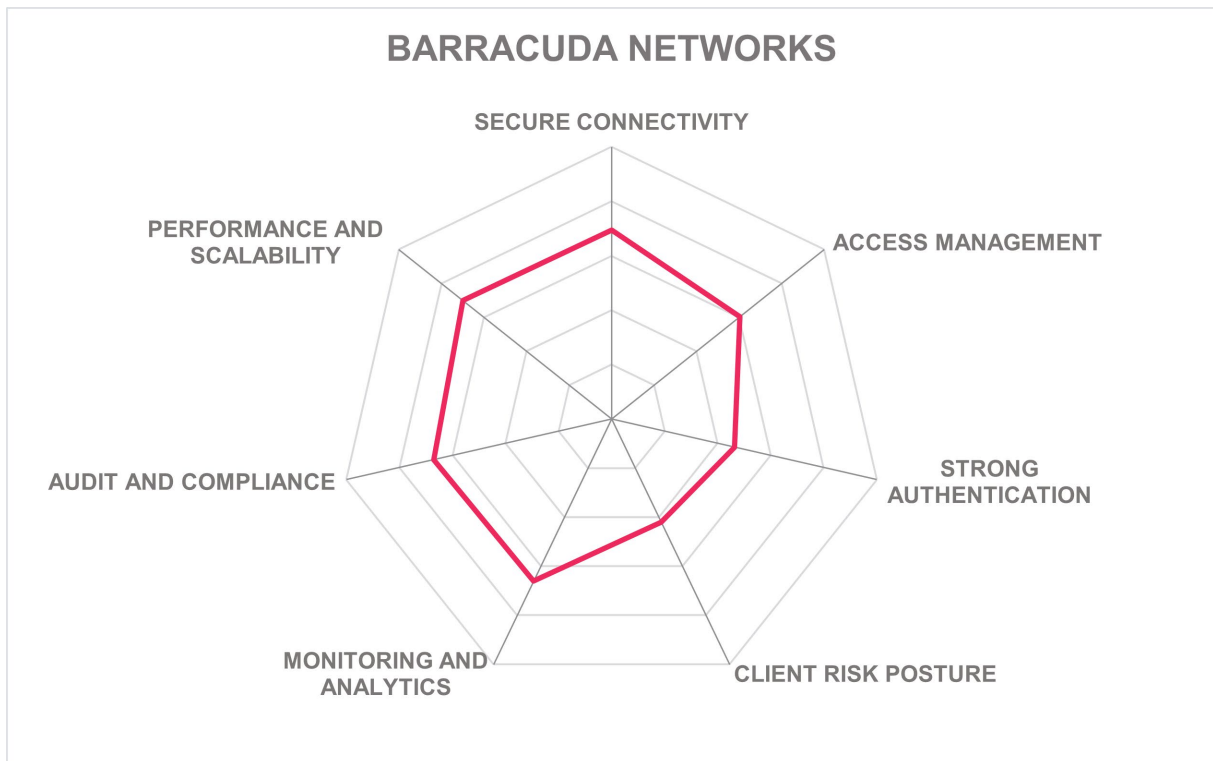
Table 5: Barracuda Networks' rating

Strengths

- Flexible deployments
- Selective backhauling
- Data confidentiality
- User friendly solution
- Self-hosted solution with low latency
- Passwordless SSO to SaaS applications
- Web security features in a single solution
- End-to-end solution designed to manage the entire lifecycle of user access

Challenges

- Limited market presence outside of EMEA and North America
- Step-up authentication is currently not supported
- More security certifications and support for compliance standards would be beneficial



Broadcom – Symantec Zero Trust Network Access (ZTNA)

Broadcom is a large US-based manufacturer of semiconductor products and supplier of infrastructure software solutions founded in 1961 and currently headquartered in San Jose, California. The company acquired CA Technologies in 2018, and the Symantec Enterprise business in November of 2019. Today, the company offers a broad portfolio of security solutions under the Symantec brand.

Symantec ZTNA is a SaaS solution that provides a secure and granular access control mechanism for all enterprise resources, whether on-premises or in the cloud. The product focuses on application security, removing the surface network as an attack surface and providing privileged conditional access with continuous evaluation. It caters to both managed and unmanaged devices, including contractors and suppliers. Using Zero Trust Access principles, it provides direct point-to-point connectivity without the need for agents or appliances, effectively mitigating network-level threats. The solution is sold individually or included in Symantec Network Protection. Symantec ZTNA ensures rapid support for remote workers by enabling deployment without requiring any agents, allowing users to access resources from any device. It ensures data compliance and protection by governing internal resources through existing DLP compliance rules. The Secure Access Cloud (SAC) Policy includes a built-in Threat Prevention Service (TIS) to prevent the upload of malware files to applications. With Role-Based Access Control (RBAC), administrative tasks can be efficiently distributed across teams, individuals, or machines, minimizing maintenance efforts. As part of the Broadcom SASE solution, Symantec ZTNA implements SASE controls on corporate workloads, addressing issues associated with multi-vendor hybrid environments. Furthermore, Symantec ZTNA is agnostic to the secondary MFA methods supported by IdPs, which can include smart cards, hardware keys, tokens, and biometric authentication.

Broadcom positions itself as a provider of enterprise solutions for large global multinational organizations. In that context, Symantec ZTNA is suitable for a variety of organizations, particularly those that prioritize advanced security measures and seek to enhance their access control infrastructure. The largest proportion of customers are primarily focused on North America, EMEA, and the APAC. Broadcom appears in the overall product, market, and innovation leadership categories.

Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Positive	
Usability	Positive	

Table 6: Broadcom's rating

Strengths

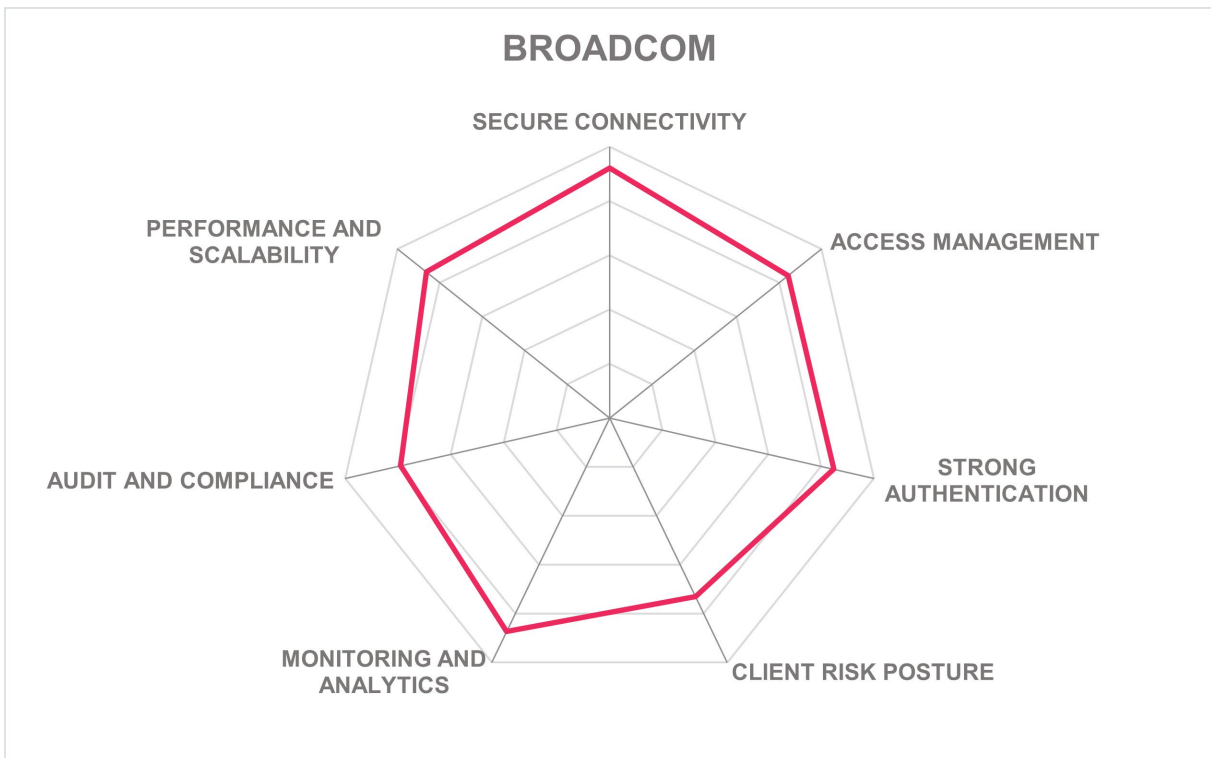
- Secure Access Cloud
- Global partner ecosystem
- Wide range of authentication methods
- Easy to deploy and configure
- Data compliance and protection
- Most capabilities do not require the deployment of an agent
- Massive global market presence and brand recognition
- An integral part of a larger cloud-based security product portfolio (including SASE)

Challenges

- The process of portfolio consolidation is still underway
- Only offered as a SaaS solution; fully on-premises deployment is not supported
- Customer configurable weighting of risk factors within policies is not supported, but improvements are on the roadmap
- Ensuring Symantec ZTNA is recognized as an offering beyond the broader suite of Broadcom products

Leader in





Cato Networks – Cato SASE Cloud

Cato Networks is a network security company founded in 2015 in Tel Aviv, Israel. Cato operates a global private backbone infrastructure, which combines SD-WAN, secure access, and managed security services in a single global security cloud. One of the pioneers of secure edge technology, the company's vision extends beyond ZTNA or SASE, striving to consolidate all network and security functions in its platform.

Predating the term itself, Cato claims to be the world's first SASE platform to converge SD-WAN and SSE functions, including Firewall-as-a-service (FWaaS), Cloud Access Security Broker (CASB), Data Leakage Prevention (DLP), Secure Web Gateway (SWG), and ZTNA, into a unified, cloud-native service. The company's cloud is built to handle a large amount of traffic seamlessly and elastically. The solution efficiently connects all enterprise network resources, including branch locations, the hybrid workforce, and physical and cloud data centers. Flexible management options are also available. Unlike legacy managed network services, customers can manage the network themselves or use expert managed services from Cato or its partners. Cato's customer admin dashboard includes many out-of-the-box reports covering a wide variety of common regulatory compliance metrics. In addition, Cato offers a unique set of features in addition to its SASE capabilities. Notably, Cato boasts a global and optimized backbone that is monitored for zero packet loss. This backbone utilizes various tiers of optimization to enhance throughput over both the Internet and MPLS. Furthermore, the solution provides Managed Detection and Response (MDR) services. This service aids users in identifying threats within their network by seamlessly extending internal threat detection capabilities. Cato MDR continuously monitors the network for compromised and malware-infected endpoints without the need for additional agents or appliances, as the network traffic flows through Cato. Cato utilizes UBA to identify potential threats, such as periodic connections to low-popularity domains, using a proprietary algorithm to measure domain popularity. Anomalous usage patterns, among other factors, contribute to the overall threat identification process within Cato's security framework.

Cato SASE Cloud aims to provide organizations with a unified, cloud-native solution that integrates networking and security, offering flexibility, scalability, and robust protection against evolving cyber threats. The Cato platform can serve both small and large enterprises. Therefore, organizations looking for the networking enhancement side of SASE, and that have other security tools in place to provide endpoint security and management, will want to consider Cato Networks. The company appears in the overall, product, market, and innovation leadership categories.

Security	Strong Positive	
Functionality	Positive	
Deployment	Strong Positive	
Interoperability	Neutral	
Usability	Positive	

Table 7: Cato Networks' rating

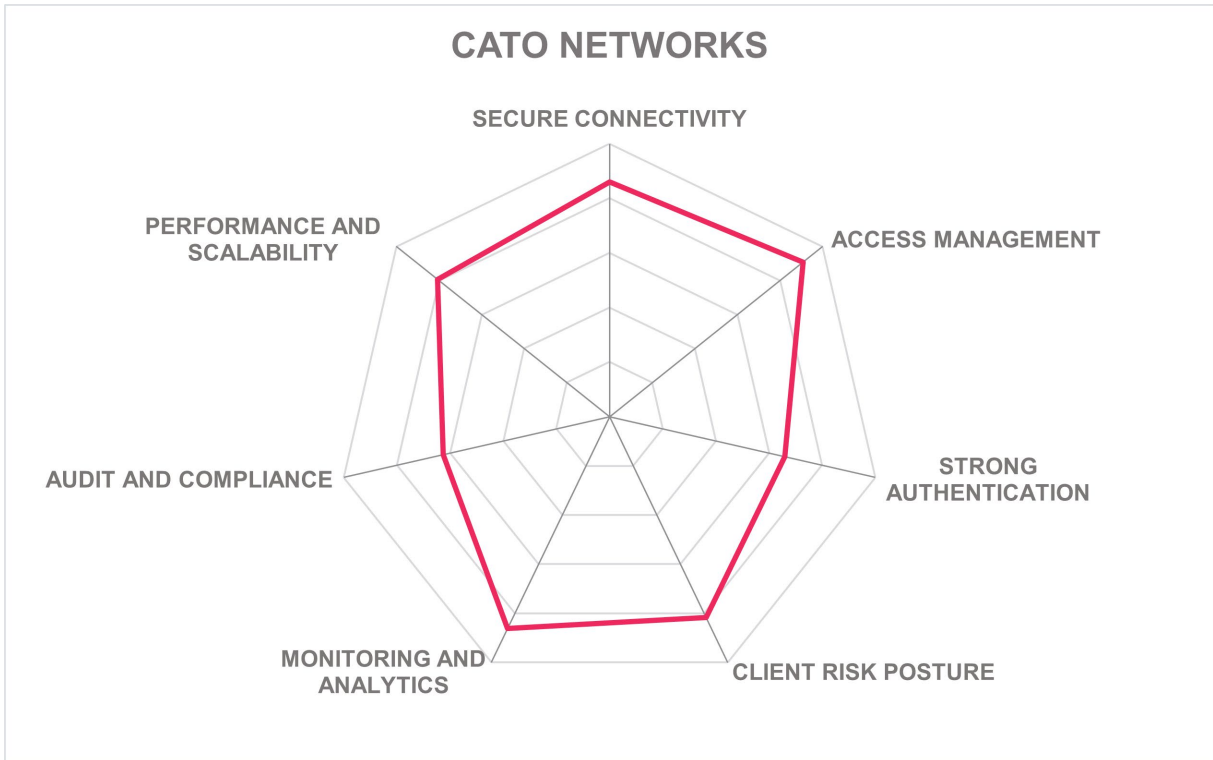
Strengths

- Strong UBA features
- Strong MDR capabilities
- High availability SLA: 99.999%
- Broad portfolio of managed services
- Rich built-in network and security analytics tools
- Admin dashboard with many reports available, including regulatory and security policy compliance
- Fully integrated cloud security and access platform (predating the notion of SASE)

Challenges

- FIDO2 support would be beneficial
- Does not support SAML for IdP interoperability
- Only GraphQL is supported for API
- The selection of strong authentication options is somewhat limited
- The number of third-party technical integration is low





Check Point – Quantum SASE

Check Point is a global leader in cybersecurity, founded in Tel Aviv in 1993. The company also offers next-generation firewalls, edge security solutions, IoT security gateways, VPNs, cloud security solutions, and complete SOC management solutions. In 2023, the company announced the acquisition of Perimeter 81, a cloud and network security company specializing in secure remote access and internet security solutions based on a Zero Trust architecture.

Quantum SASE is Check Point's new SASE solution (replacing Check Point's Harmony Connect product suite) designed to provide enhanced security and connectivity for hybrid work and cloud networks. It enables secure remote access for employees, partners and customers ensuring that only authorized users and devices can access sensitive data and applications. The solution offers on-device and cloud network protections to achieve faster and more secure browsing. It implements full mesh secure connectivity between users, branches, and applications, following a Zero Trust Access model. Furthermore, the SD-WAN component of Quantum SASE is optimized for connectivity while utilizing ThreatCloud AI for effective threat prevention. Quantum SASE applies an identity centric Zero Trust access policy, accommodating employees and partners. It ensures performance through a full mesh global private backbone. The solution addresses the evolving security landscape by expanding beyond traditional perimeters, catering to the new standard of hybrid work. It aligns with the continuous digital transformation of organizations, providing security and convenience. The admin interface is intuitive, allowing customers to easily manage access rules and check status and security of connections. Many administrative reports are available. Check Point provides support for both customer admins and end users over phone, web, and email.

Check Point's recent acquisitions and innovative solutions demonstrate its commitment to effectively addressing evolving security challenges. Organizations looking for rigorous security in a ZTNA solution should put Check Point on their evaluation list. The company appears in all leadership categories.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 8: Check Point's rating

Strengths

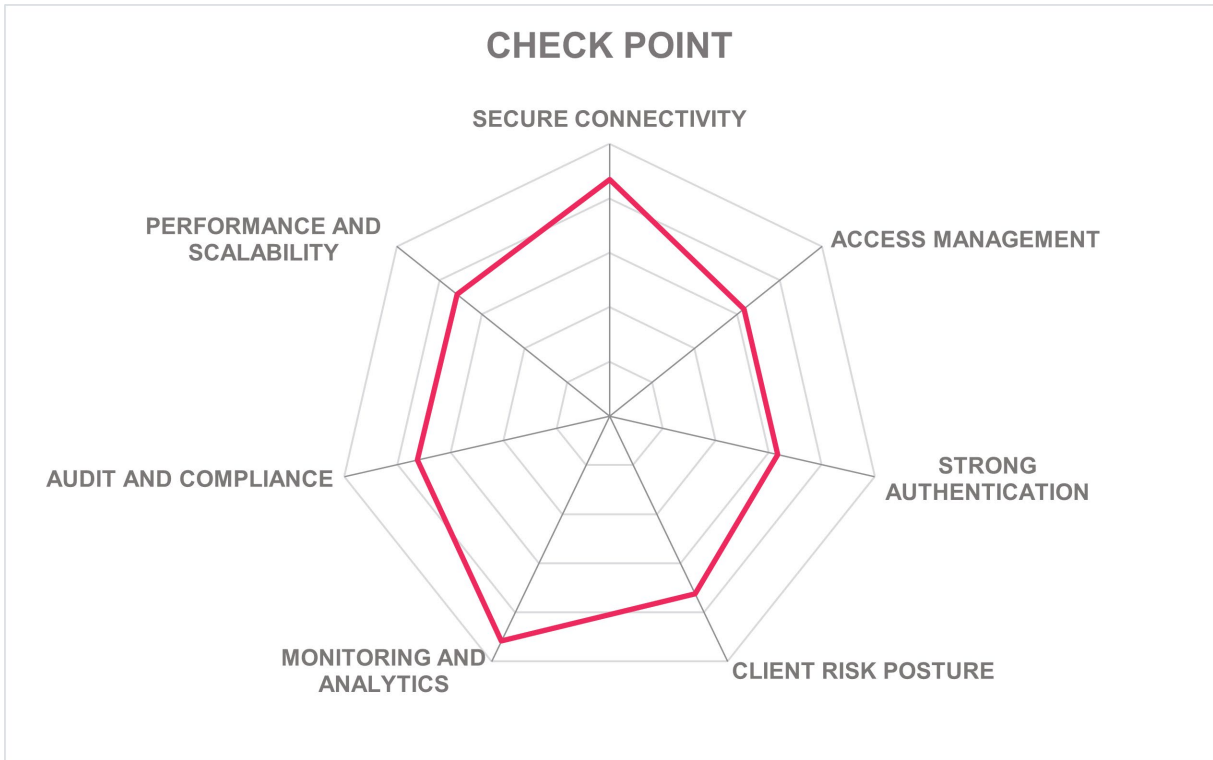
- TLS 1.3 support
- User friendly solution
- Good customer admin interface
- Threat prevention features
- Good auditing and forensic analysis capabilities
- High performance global private backbone

Challenges

- ABAC model is not supported
- OIDC not supported for ZTNA
- Step-up authentication is currently not supported
- Delegated administration is not supported

Leader in





Cisco – Secure Access

Cisco is a multinational technology company based in San Jose, California. Founded in 1984 by the pioneers of the multiprotocol network router concept, the company quickly grew to become one of the world's largest manufacturers of networking hardware and telecommunications equipment. Over the last decade Cisco has also built a large and growing security business that exceeds 3.6 billion in annual revenue. With a presence in more than 100 countries, the company serves customers in a wide range of industries.

Cisco Secure Access is the company's Security Service Edge (SSE) solution that radically simplifies the way companies can securely access the internet, SaaS apps as well as private applications and resources hosted anywhere. It provides customers with a flexible choice of both client and clientless secure remote access capabilities to meet their needs and use cases.

Any Cisco networking device that supports IPsec termination can serve as a gateway to provide backhaul connectivity. Additionally, Cisco Secure Access offers resource connectors for ZTNA, which can be delivered as containers or VMs. As part of a larger user protection approach, Cisco enables customers to tailor their deployment with a range of components such as SSO, passwordless authentication, MFA, anomalous user behavior detection, and device posture assessments for diverse applications. It integrates with most major EPDR and MDM/UEM solutions to verify the device trustworthiness at the time of access. Additionally, with the Cisco Secure Endpoint solution, administrators can automatically block malware infected devices. This approach allows organizations to align their configurations with specific needs, use cases, and threat models, making Cisco's Secure Access a flexible and customizable choice in the Zero Trust landscape. Cisco's included DLP and CASB capabilities do data and application discovery. They can classify hundreds of pre-defined data types, and customers can create their own. Experience insights are provided within the dashboard to help diagnose and remediate the source of remote user performance issues. The optional use of MASQUE and QUIC protocols provides additional efficiency and protection.

Cisco has collaborated with Apple (iOS) and Samsung (Galaxy devices) to enable Zero Trust access through Cisco Secure Access. Additionally, the solution supports various integrations like ISE SD-WAN and Duo that provide additional layers of protection and strengthen the security posture. Cisco Secure Access is a compelling case for workforce access, remote work, and hybrid scenarios. It stands out as a leading solution in the realm of Zero Trust for workforce security. Overall, Cisco can deliver remote access security in on-premises, hybrid, and cloud formats. ZTNA capabilities are also available in Cisco Secure Connect, their unified SASE solution which provides the combination of both security and networking functionality. Cisco appears in the overall product, market, and innovation leadership categories.

Security	Strong Positive	 CISCO Cisco Security
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 9: Cisco's rating

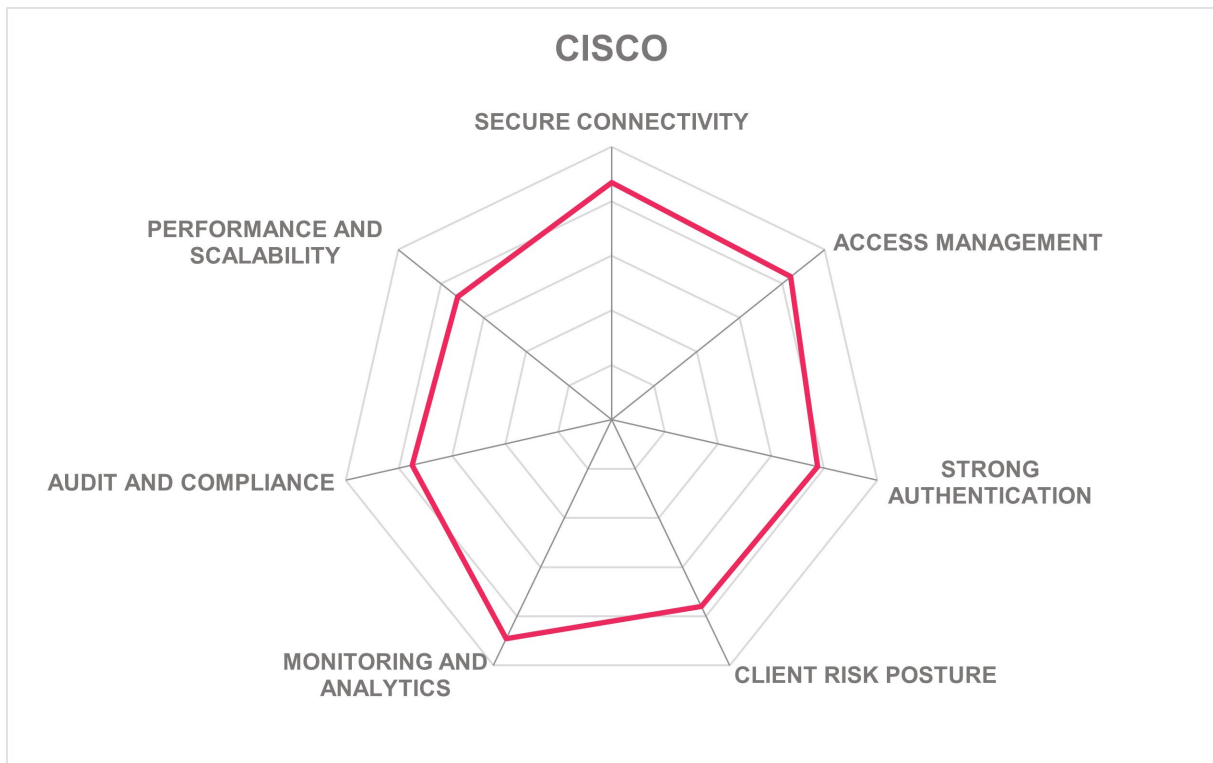
Strengths

- Single client for a full range of SSE capabilities (including ZTNA)
- Global partner ecosystem
- Flexible deployment options
- Multiple security certifications
- Strong market presence and global brand recognition
- Unified remote access and cloud security offering
- Adaptability as stand-alone or integrated solution
- Complete IDaaS with wide range of MFA options available in Duo, packaged with Secure Connect

Challenges

- Support for creation of unified access policies for hybrid access is in development
- With clientless access, endpoint posture evaluation is limited to basic checks like browser, OS version, or geolocation
- Ensure that Secure Access is recognized as a ZTNA offering beyond the broader Cisco product suite





Cloudflare – Cloudflare Access

Cloudflare is headquartered in San Francisco, CA. The company is a leading Content Delivery Network (CDN) and provider of network security services such as API gateway, WAF, DDoS protection, and bot management. Founded in 2009, Cloudflare has quickly grown from a simple “firewall in the cloud” to one of the leading providers of website performance and security services, focusing its vision on accelerating and protecting internet, SaaS, and self-hosted applications through an intelligent global security cloud without adding hardware or installing software.

Cloudflare Access, part of the company's SASE platform Cloudflare One, operates exclusively as a SaaS solution within Cloudflare's global cloud network and is not deployable as virtual appliances on-premises or in public clouds. However, it effectively safeguards on-premises, public, and private cloud applications. The platform seamlessly integrates with Cloudflare Gateway, providing a client for end-user devices. Furthermore, customers can quickly migrate internal applications to ZTNA using Cloudflare's lightweight connector, "cloudflared." This daemon operates on various operating systems and Docker containers, eliminating the necessity for incoming traffic or publicly reachable IP addresses for cloud platform applications. This approach enhances security by eliminating the need to create openings in the perimeter firewall. The solution offers a superior alternative to traditional VPNs. It ensures swift, secure, and convenient user-to-application connections by implementing identity- and context-driven rules, reducing lateral movement risks. The platform supports in-browser terminal functionality for secure remote access through SSH and VNC protocols over HTTPS. Robust security measures include end-to-end encrypted tunnels for L4-7 connections, optional mutual TLS authentication, and integration with identity providers for granular authentication.

In the context of ZTNA, Cloudflare acts as an identity proxy and relying party. Any OIDC or SAML issuing IdP can be used. Authentication policies can leverage any authenticator supported by these IdPs. As an identity proxy, Cloudflare supports secure token exchange. Cloudflare performs basic UBA, evaluating many risk factors surrounding each session, and can optionally consider some third-party intelligence sources. In addition, device posture verification and micro segmented access authorization are consistently enforced based on dynamic contextual signals. Cloudflare is a versatile platform that can be tailored to meet the needs of organizations with diverse requirements, making it a compelling choice for a broad range of industries and use cases. The company appears in all leadership categories.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive



Table 10: Cloudflare's rating

Strengths

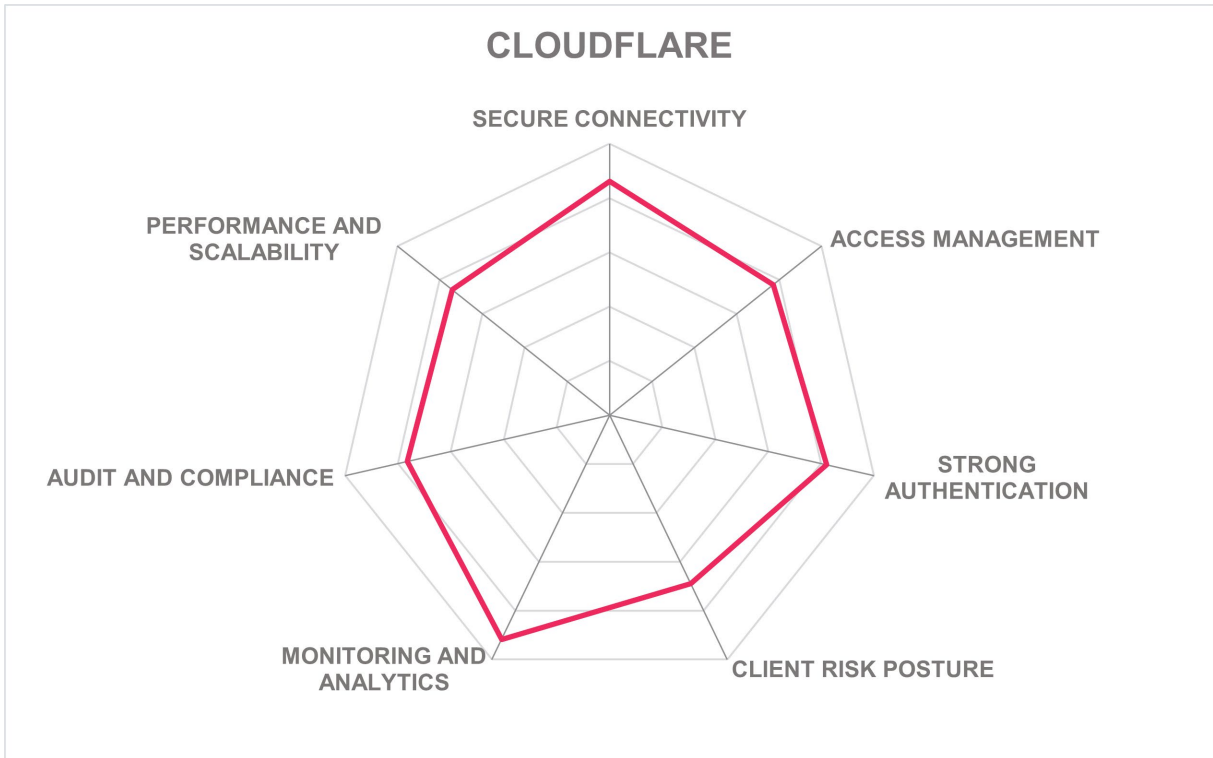
- Highly scalable
- User friendly solution
- Easy to deploy and configure
- HIPAA/HITRUST certification
- Strong market presence and global brand recognition
- Global cloud infrastructure with low latency
- Innovative Remote Browser Isolation built on Network Vector Rendering technology

Challenges

- Only offered as a SaaS solution; full on-premises deployment is not supported
- Policy testing tools are currently not available
- Integration complexity, particularly with other security agents
- Endpoint posture checks rely largely on third party integrations

Leader in





Ergon – Airlock Secure Access Hub

Ergon Informatik is on the verge of its 40th anniversary and currently has over 400 employees in Switzerland and a small sales office in Germany. The product has a strong presence in the DACH region (Germany, Austria, and Switzerland) and serves customers in the financial industry as well as banking software vendors. They also have a small but growing number of customers in the Middle East, North America, and the APAC region.

Airlock Secure Access Hub is a versatile solution that integrates Web Application, API protection, and IAM functionalities, offering deployment options on-premises or in the cloud using hypervisor or container technology. This integration supports features such as step-up authentication and risk-based authentication. It strengthens access control, simplifies management, and enhances security for web application, helping organizations protect their sensitive data and resources. The solution can support on-premises, full multi-tenancy for cloud, and hybrid deployment models. Airlock Gateway is available as a virtual appliance while Airlock IAM is delivered as a self-contained application. Airlock Gateway is configured using a management UI or a REST-based API. Airlock Microgateway is fully Kubernetes-native and is therefore configured using Custom Resource Definitions (CRDs) via Kubernetes API or using .yaml files. Both products offer their security protection functionality by being placed as a reverse proxy between client and server. Strong API security is given and derived from its long history in the Web Application Firewall (WAF) market, focusing on content security. In addition, Airlock's Continuous Adaptive Trust is an innovative feature which focuses on providing dynamic and context-aware security measures to protect digital assets and ensure secure access to resources based on the continuously evolving risk landscape.

Airlock IAM supports many authentication methods that may be combined into authentication flows. Passwordless authentication is accomplished using FIDO2 and Airlock 2FA support. Furthermore, the solution provides a portal page, where the customer configures which applications an end user can view. The login screen supports multiple languages and dynamic step activation through checkboxes, enabling users to customize their flow experience. Ergon's Airlock has a well-established set of Zero Trust capabilities with a strong focus on WAF, API Security, CIAM, and strong authentication in one solution. Its customers and their partner ecosystem are primarily focused on DACH, although growing across the EMEA and the APAC regions. Ergon Airlock Secure Access Hub continues to grow its feature set and remains a competitive alternative to other solutions within the DACH EMEA region.

Security	Strong Positive	 <p>AIRLOCK®</p> <p>SECURE ACCESS HUB</p>
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

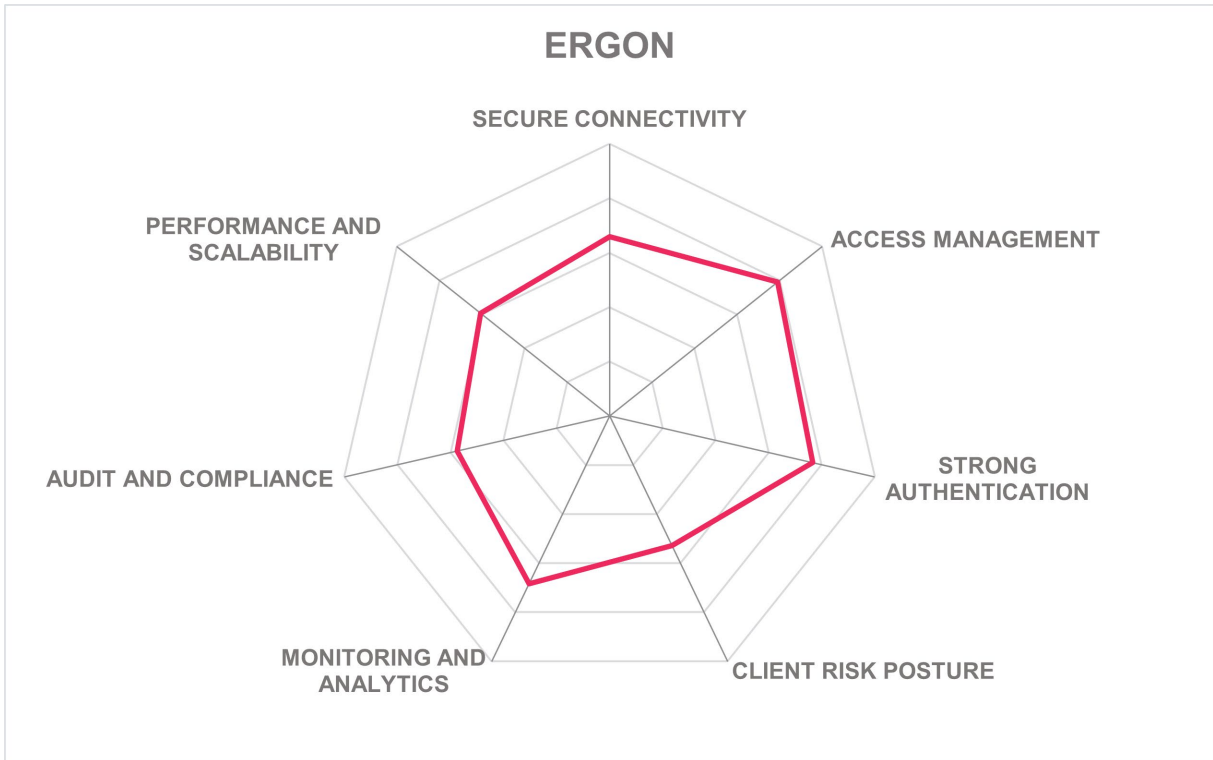
Table 11: Ergon's rating

Strengths

- Good MFA support
- Strong API security
- Developer-friendly solution
- UBA capabilities
- Excellent admin dashboard
- Combination of Filtering and Access Control
- Continuous Adaptive Trust feature
- Innovative list of capabilities on roadmap

Challenges

- Small partner ecosystem & limited global reach
- Feature requests and roadmap alignment
- No support for integration with UEM solutions



Fortinet – Fortinet Universal ZTNA

Fortinet is an American cybersecurity company with headquarters in Sunnyvale, California, USA. Established in 2000, it provides a wide range of network security and SD-WAN, switching and wireless access, network access control, authentication, public and private cloud security, endpoint security, and AI-driven advanced threat protection solutions for carriers, data centers, enterprises, and distributed offices. Its solutions are integrated into the Fortinet Security Fabric.

Fortinet Universal ZTNA is built into the Fortinet operating system, providing scalability and flexibility for both cloud and on-premises deployments. This approach allows for a low-latency architecture and easy implementation for existing Fortinet customers, as ZTNA capabilities are built into the operating system and do not require separate licensing. Universal ZTNA ensures secure and straightforward access to applications from any location, accommodating the needs of the evolving hybrid workforce. This solution enables users, whether working remotely or in the office, to securely access applications hosted anywhere. It provides granular access control, allowing access to specific applications for the duration of a session. Ongoing verification ensures the user's identity, device identity, and posture are verified before granting access. The unified FortiClient Agent manages the transition from VPN to ZTNA seamlessly. It checks in with the policy, performs security checks, and establishes an encrypted tunnel to the appropriate application gateway. Furthermore, like many Fortinet products, it is delivered in an appliance form factor, either as a hardware appliance or as a virtual machine for on-premises or public cloud deployment. To extend its capabilities, the solution supports multiple integrations with other Fortinet products, including Fortinet IAM, FortiTrust, FortiSASE, FortiClient, FortiToken and FortiAuthenticator, as well as external security platforms, threat intelligence feeds, identity providers, and even data lakes.

Overall, Fortinet's ZTNA solution is positioned as a flexible, comprehensive, and user-friendly approach to enforcing zero trust principles in network access, with a focus on scalability, integration, and ease of deployment. Fortinet's product strategy is based on the concept of Security Fabric, an integrated, automated platform that unifies networking, security, and access capabilities in a mesh-like architecture. The solution should be near the top of any organization's ZTNA RFP list. Fortinet appears in the overall, product, innovation, and market leadership categories.

Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Positive	

Table 12: Fortinet's rating

Strengths

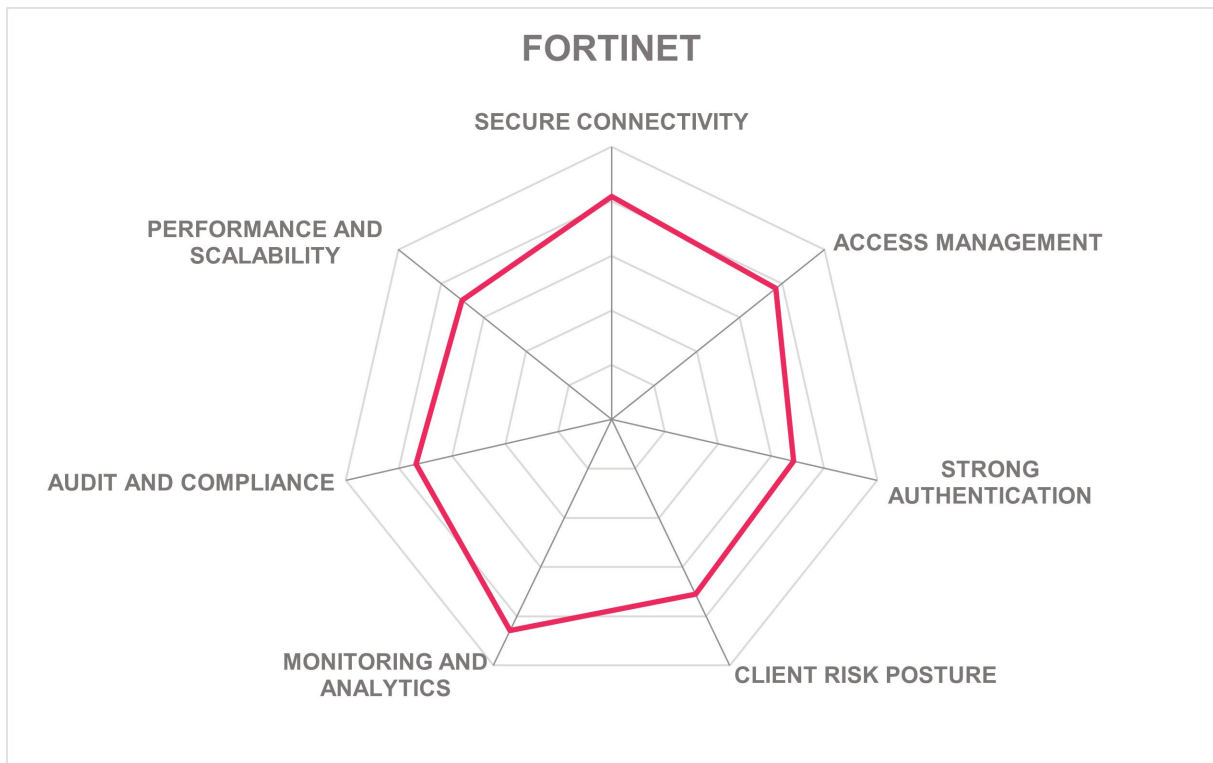
- SD-WAN integration
- Strong partner ecosystem
- Comprehensive security fabric
- Flexible for both cloud-delivered or on-prem deployments
- FortiClient Agent manages the transition from VPN to ZTNA
- Unified agent for endpoint remote access and control
- Direct integrations with other Fortinet security tools
- Numerous built-in content to reduce time to value

Challenges

- Ensuring Universal ZTNA is recognized as an offering beyond Fortinet's broader suite of products
- Aligning ZTNA with organizational goals and overcoming the perceived daunting nature of the implementation process

Leader in





Forum Systems – Forum Sentry

Forum Systems is a privately held independent engineering company based in Needham, MA. Founded in 2001, the company provides gateway-based solutions for API and cloud security. Since its very beginning, the company has offered mission-critical, large-scale solutions with a heavy emphasis on “security by design.” Forum Systems addresses the Zero Trust cybersecurity challenge through its scalable Forum Sentry solution. In recent years, the company has significantly expanded the choice of deployment and integration scenarios to support highly regulated and government customers.

Forum Sentry serves as an enterprise Policy Enforcement Point (PEP), offering federal and commercial organizations a secure, agile, and high-performance solution for implementing a Zero Trust network model. It facilitates data transformation, mapping, and validation, allowing for secure PEP enablement without the need for coding or causing disruptions in the environment. The solution is unique in its approach towards security by not allowing any third-party extensions or libraries, which ensures resilience against known and not yet discovered vulnerabilities. Furthermore, the solution supports fast and easy authentication with SSO and MFA from multiple IDPs. It accommodates a range of identity token formats, including username/password, PKI, SAML, OAuth, and JWT. Forum Sentry ensures data privacy for both data in motion and at rest by providing accelerated FIPS 140-2 encryption. The solution also offers integrated hashing and digital signatures to ensure that communications can be signed and verified, maintaining the integrity of data.

The Forum Sentry solution offers Flex Instance-Based licensing, eliminating per-user, per-API, per-CPU, or per-transaction fees. Additionally, the solution offers advanced content based DLP, incorporating Base64 extraction and supporting Internet Content Adaptation Protocol (ICAP) scanning or custom API analysis for enhanced security measures such as Zero Day Threat detection and AI engine inspection. While maintaining a strong focus on API security, the company has significantly updated and expanded its product portfolio. Overall, Forum Sentry provides a modern and versatile solution for organizations to implement Zero Trust cybersecurity measures, offering a range of capabilities to secure data communications, ensure integrity, and leverage advanced technologies such as machine learning and AI.


Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Strong Positive	
Usability	Positive	

Table 13: Forum Systems' rating

Strengths

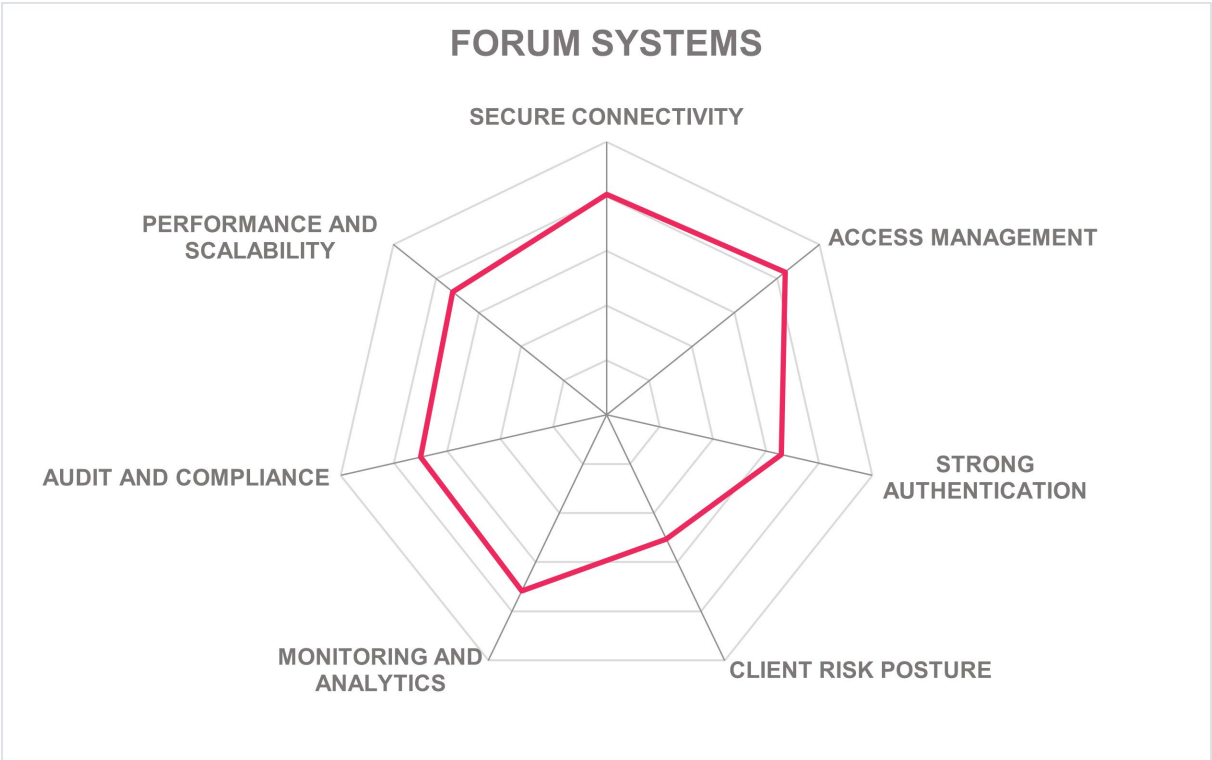
- Strong API security
- Cost-effective licensing model
- Innovative list of capabilities on the roadmap
- “Security by design” architecture for maximum reliability
- FIPS 140-2 and NIAP NDPP-certified
- Supports a broad range of identity and access control standards, tokens, and credentials.

Challenges

- Ad-hoc reporting is not currently supported
- North American customers are their prime focus
- Lack of graphical visualization and configuration of risk evaluation policies for customer admins
- Sentry does not integrate with legacy VPNs, however, it can coexist with a legacy VPN

Leader in





Ivanti – Ivanti Neurons for Zero Trust Access

Ivanti is a software company specializing in IT asset and service management, supply chain management, and IT security headquartered in South Jordan, Utah. Although established in 2017, the company's history can be traced back to the 1980s under the name LANDESK. Through a substantial number of recent acquisitions, the company has created a broad portfolio of solutions for discovering, managing, and securing IT assets. All these technologies are now offered as parts of Ivanti Neurons, a unified workspace hyper automation platform powered by machine learning.

In 2020, Ivanti acquired Pulse Secure, a provider of secure access solutions ranging from VPN to ZTNA. Today, this technology forms the basis of Ivanti Neurons for Zero Trust Access, part of the company's network security offering that is integrated with Ivanti's unified endpoint management offering, which includes a full range of secure access options as well as mobile device management, secure productivity, and other capabilities. Ivanti Neurons for Zero Trust Access is designed for the modern cloud-first world, delivering secure and seamless access to corporate applications. The solution follows a distributed Software Defined Perimeter (SDP) architecture, directing user application traffic from the endpoint to specific ZTA Gateways for each application. In the event of a controller outage, users with established tunnels will continue to access applications without any impact. This design enhances robustness and uninterrupted access for users even in the face of infrastructure challenges. In addition, the solution dynamically assesses user identities, device posture, and application access to enforce granular access controls, allowing authorized users to access only the resources they need.

One of the most differentiating features about Ivanti's solution is its tight integration with VPN products. With the help of a cloud-based console that manages both VPN and ZTA networks, customers can perform "in service" migration of an application from VPN to ZTA in real time. Other key features include continuous assessment of device risk based on running processes and applications, automatic quarantine of unpatched devices running high-risk applications, least-privilege connectivity for secure access to private applications from anywhere, actionable insights for automated remediation based on user risk scoring, and more. For dashboards, the solution allows admins to customize some of the insights and analytics-related views based on what they want to keep or remove. It also offers flexible reporting capabilities, allowing users to generate ad hoc reports or schedule them for regular intervals. Moreover, Neurons for ZTA integrates with other Ivanti products, including Neurons MDM, EPMM, and RiskSense VULN KB. This integration enhances the overall functionality and collaboration between different Ivanti security and management solutions.

Organizations in a variety of industries, especially those prioritizing device management, complex and hybrid deployments, and secure user-centric access, should consider deploying Ivanti Neurons for ZTA. Its integration with other Ivanti products enhances its appeal and makes it a good fit for organizations already using Ivanti products. Ivanti is listed in the product leadership category.

Security	Positive	
Functionality	Strong Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 14: Ivanti's rating

Strengths

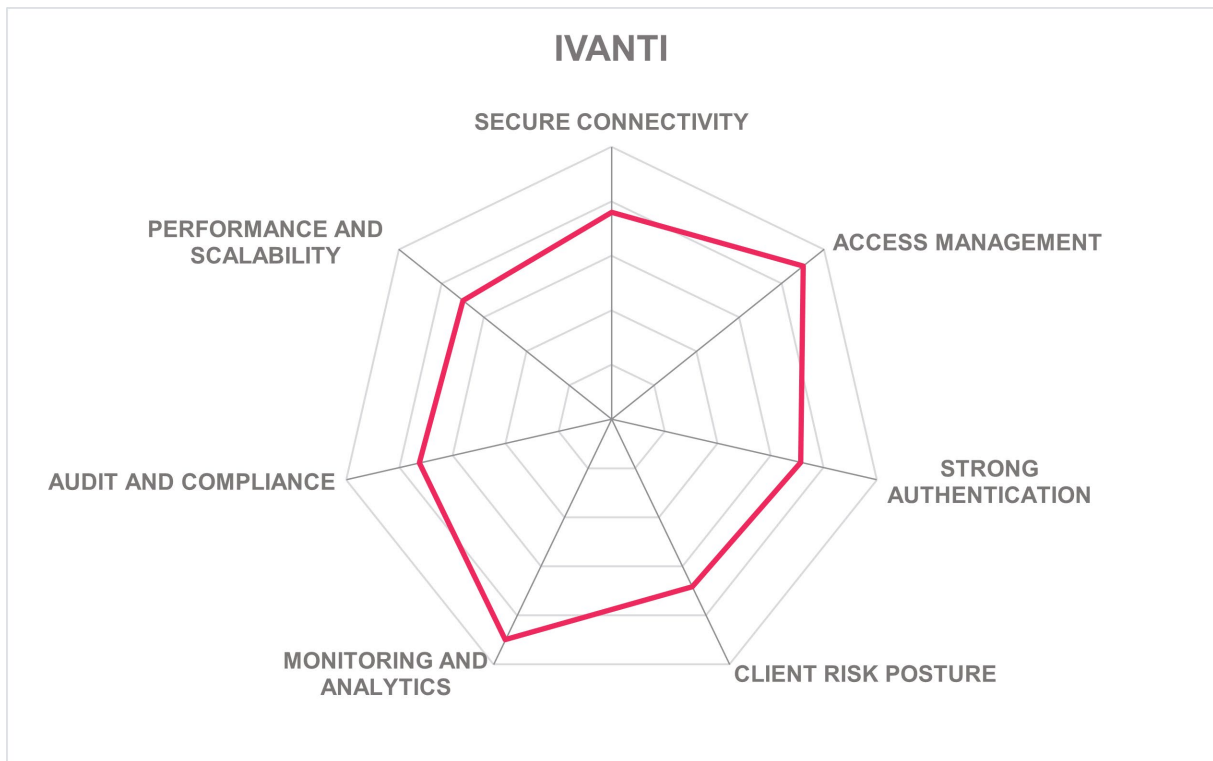
- Brand recognition
- Good UBA capabilities
- Based on an SDP architecture
- Customer admin interface is comprehensive and easy to navigate
- Single client and unified policies for all platforms and types of connectivity
- Integral part of a large, end-to-end IT management, device management, automation, and security platform
- Primary focus on complex, hybrid deployments, seamless migration from legacy VPN access

Challenges

- Small, but growing global partner ecosystem
- On-premises controller deployment currently not supported by vendor, but is planned
- Agentless operation is supported with L7 proxy that grants access to specific applications on VPN. However, supporting those applications on ZTA Gateways is currently in progress.

Leader in





Jamf – Jamf Connect

Jamf is a software vendor primarily known for device management and security solutions for Apple devices. Established in 2002, Jamf is headquartered in Minneapolis, Minnesota, USA, serving over 70 thousand customers around the globe and running on over 32 million devices. In 2021, Jamf acquired Wandera, a Zero Trust cloud security company, bringing its technology to a much wider customer base. Jamf's ZTNA for remote access provides real-time risk assessment, cloud-based integration, intelligent split-tunnelling, and seamless reconnections, ensuring device health evaluation and secure business connections.

The solution's ZTNA capability can operate as a standalone service or as a feature **integrated into Jamf's device management and security platform**. It provides provisioning, authentication, and remote access to applications, adhering to Zero Trust principles. Jamf Connect is a fully cloud-hosted solution that integrates with a customer's existing IdP and firewall infrastructure. The solution streamlines end-user identity workflows, improving the security of both devices and accessed applications, whether hosted in a data center or the cloud. This results in rapid, simplified, and highly secure user access, offering a consistent experience across different application hosts and connected devices.

All configurations are managed online through the Jamf Security Cloud Portal, ensuring a quick and straightforward process that can be completed quickly. The solution can be remotely deployed to devices UEM or MDM, allowing for rapid rollouts. Moreover, the solution eliminates the necessity for configuring internal routes between clouds and data centers. Instead, Jamf Connect directly connects to the edge of each cloud or data center where applications reside. This approach significantly reduces the complexity of maintaining network interconnects and security rules. Jamf Connect's dynamic split-tunnel functionality enables routing using hostnames, not IP addresses, which is important for modern cloud applications. In addition, when combined with Jamf's cloud-based Web Gateway service, customers can achieve remote access, network security, content filtering, and data optimizations through a unified platform.

The platform offers a broad range of real-time statistics that provide insight into unusual activity, session duration, or bandwidth requirements. Comprehensive visibility allows administrators to monitor inappropriate content, detect malware and identify data leaks. Jamf's notable differentiator has always been its long-term strategic focus on mobile platforms and specifically, the Apple device ecosystem. However, the ZTNA platform extends support to all major desktop and mobile operating systems, including Android, Windows, and MacOS. Jamf appears in the overall, product, and innovation leadership categories.

Security	Positive	
Functionality	Strong Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 15: Jamf's rating

Strengths

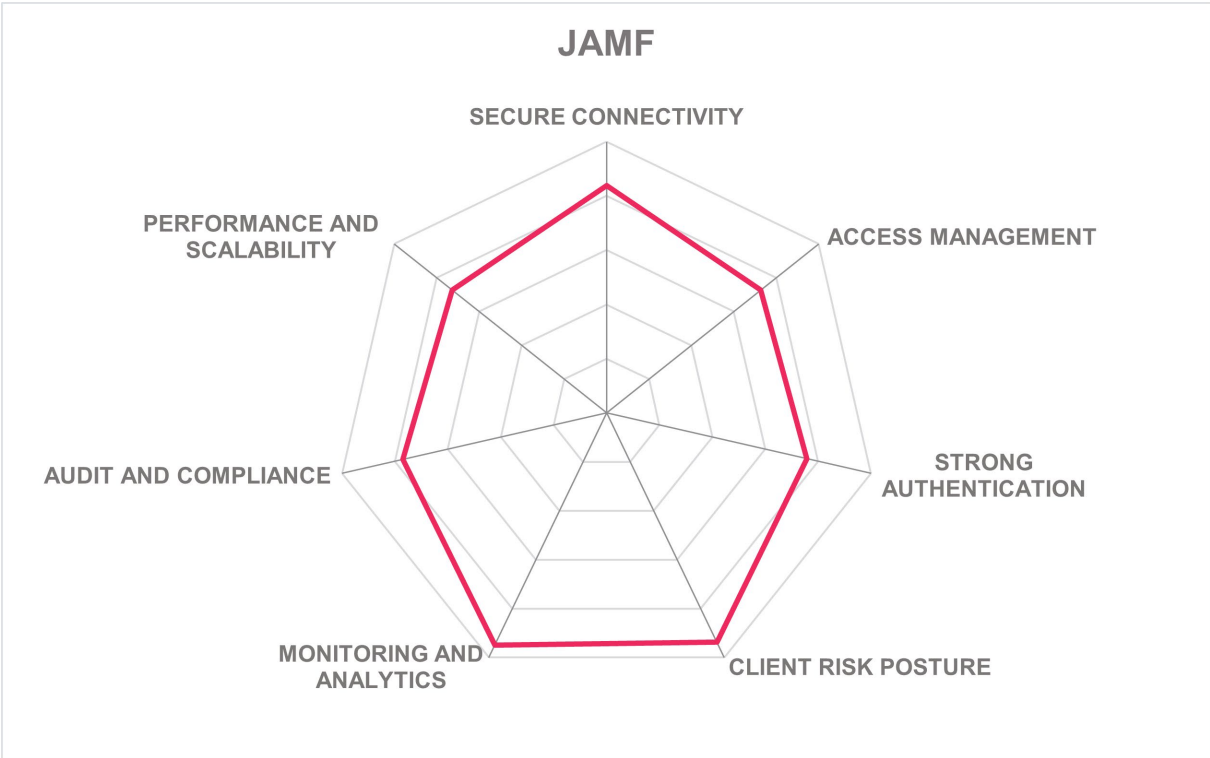
- User friendly solution
- Strong device management features
- Real-time statistics and reporting capabilities
- Risk-engine can evaluate multiple attributes
- Easy and streamlined rollout and management even at large scale
- Broad partner ecosystem with leading IdPs and UEM vendors

Challenges

- More security certifications would be beneficial
- Entirely on-premises deployments are not supported
- No support for delegated administration

Leader in





Lookout – Lookout Secure Private Access

Lookout is a cybersecurity provider of endpoint and cloud security solutions based in San Francisco, California, USA. Originally one of the pioneers in mobile security (established in 2002), over the years, Lookout has grown into an integrated data-centric security company. The acquisition of CipherCloud in 2021 made the company expand into the market for ZTNA solutions. Today, Lookout provides a unified security platform that enables secure and protected access to sensitive applications from any device.

Lookout Secure Private Access is a data centric ZTNA solution designed for secure access and data protection of enterprise private applications. Secure Private Access is an integral component of Lookout's unified data-centric platform, the Lookout Cloud Security Platform. This solution offers adaptive access control based on user, device, and location, intelligently enforcing granular data protection controls. It continuously monitors the security posture of both managed and unmanaged user devices, and in the event of anomalies, it re-verifies the security posture, allowing for access revocation or the enforcement of stricter actions such as data masking, redaction, or watermarking. The solution has the ability to operate alongside a customer's existing legacy VPN solution, all the while delivering Zero Trust access to designated private applications. This is particularly valuable during the customer's transition from their current remote access system to Secure Private Access. In addition, Lookout Secure Private Access combines DLP content inspection, threat prevention, and advanced UEBA with popular access controls to private applications. The platform's unique risk-based Continuous Conditional Access enables customers to protect sensitive data, especially against leaks on unmanaged devices. Furthermore, the platform provides a single pane of glass to manage all access policies through the management console.

Lookout Secure Private Access addresses a variety of user scenarios, including secure remote access for external partners and contractors using non-managed devices. Overall, Lookout's Secure Private Access proves to be a versatile and effective solution for organizations seeking intelligent, adaptive, and easy-to-use security measures. Organizations looking for a ZTNA solution with these capabilities should take a close look at Lookout's platform. Lookout appears in the overall, product, and innovation leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 16: Lookout's rating

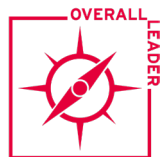
Strengths

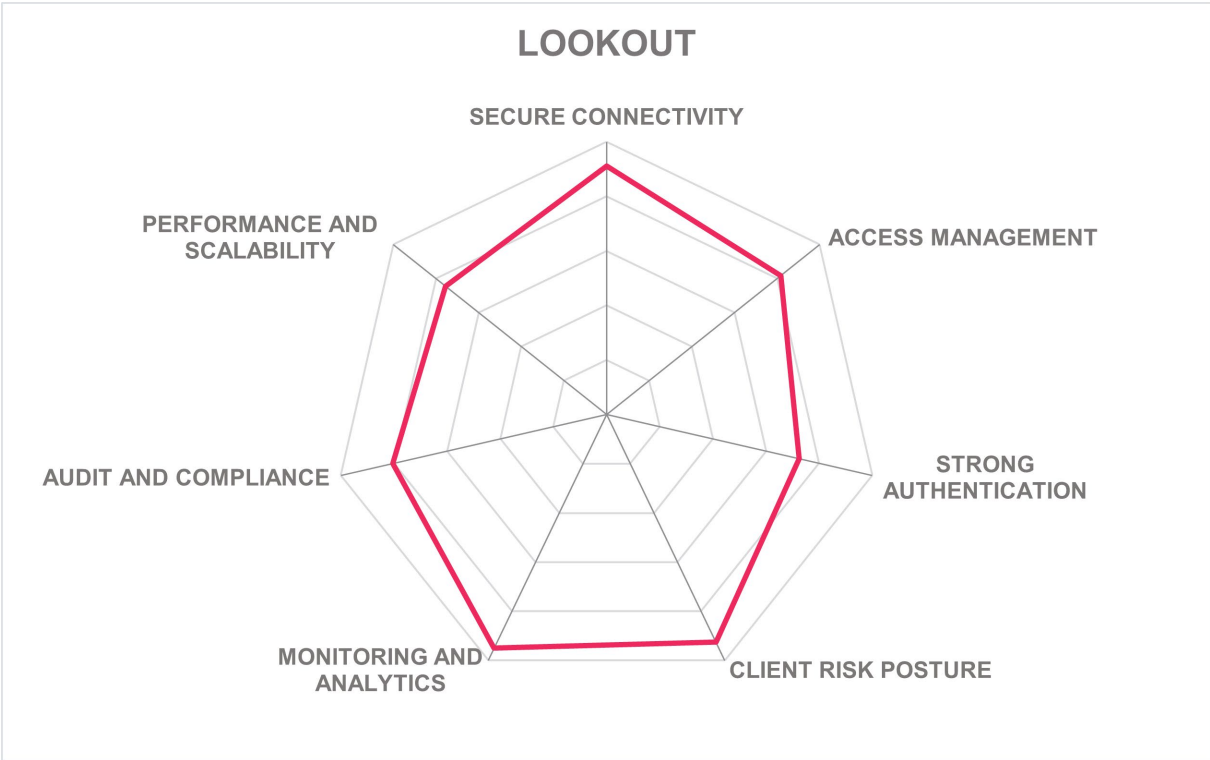
- Advanced UBA features
- Customer admin interface is comprehensive
- Multiple security certifications
- Continuous conditional access feature
- Mobile endpoint data protection
- Strong global market presence and brand recognition
- Part of a complete security platform with CASB and DLP functions combined with a strong endpoint security portfolio

Challenges

- OIDC is not supported for ZTNA
- Entirely on-premises deployments are not supported
- No support for virtual appliances, but enhancements are on the roadmap
- No integration with third-party application catalogs

Leader in





NetFoundry – CloudZiti and OpenZiti

NetFoundry is a network security vendor based in Charlotte, North Carolina, USA. The company was founded in 2016 to address a major shortcoming of existing Zero Trust solutions. At the core of NetFoundry's solution is OpenZiti – an open-source programmable Zero Trust networking stack which can be applied to any use case. NetFoundry's platform is accessed via APIs, SDKs, and DevOps tools integrations, enabling users to benefit from connectivity-as-code. Regional coverage includes North America, EMEA, and APAC.

CloudZiti is a comprehensive and flexible networking solution that simplifies the delivery of secure applications, APIs, proxies, IoT, and browsers by embedding Zero Trust principles. The solution caters to various use cases, including IoT management, API security, and agentless networking. The CloudZiti SaaS solution is built on the OpenZiti open-source platform. OpenZiti is a project designed to incorporate Zero Trust networking principles into any application. It provides the essential components and tools needed to build a Zero Trust overlay network, making it easy to integrate Zero Trust directly into existing solutions. The solution extends the principles of Zero Trust beyond traditional network boundaries, asserting that these principles should not be confined to the network alone, but should be an integral part of the application architecture. Through an SDK, the solution eliminates the exposure of open ports and strengthens security. In addition, OpenZiti requires authentication and authorization prior to connection, ensuring micro-segmentation with least privilege access. It also trusts endpoints based on access control compliance, performs posture checks, and implements end-to-end encryption for robust data security. The platform offers flexible identity management, private authenticated DNS, and prevents port inference and source/destination information exposure, bolstering overall security. Furthermore, the OpenZiti Controller serves as the central configuration and management entity within the OpenZiti Network, playing a pivotal role in configuring services, managing user and device identities, and overseeing authentication and authorization for all network connections. To establish secure connections, the controller requires configuration with a PKI, facilitating mutually authenticated TLS (mTLS) connections throughout the network. The solution's application portability, easy integration, and multiple deployment options make it a versatile and efficient alternative for developers and users.

OpenZiti offers an innovative solution for organizations seeking to implement Zero Trust principles. It is ideal for organizations of varying sizes and industries, particularly those prioritizing security and performance in their infrastructure. NetFoundry appears in the overall, product, and innovation leadership categories.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 17: NetFoundry's rating

Strengths

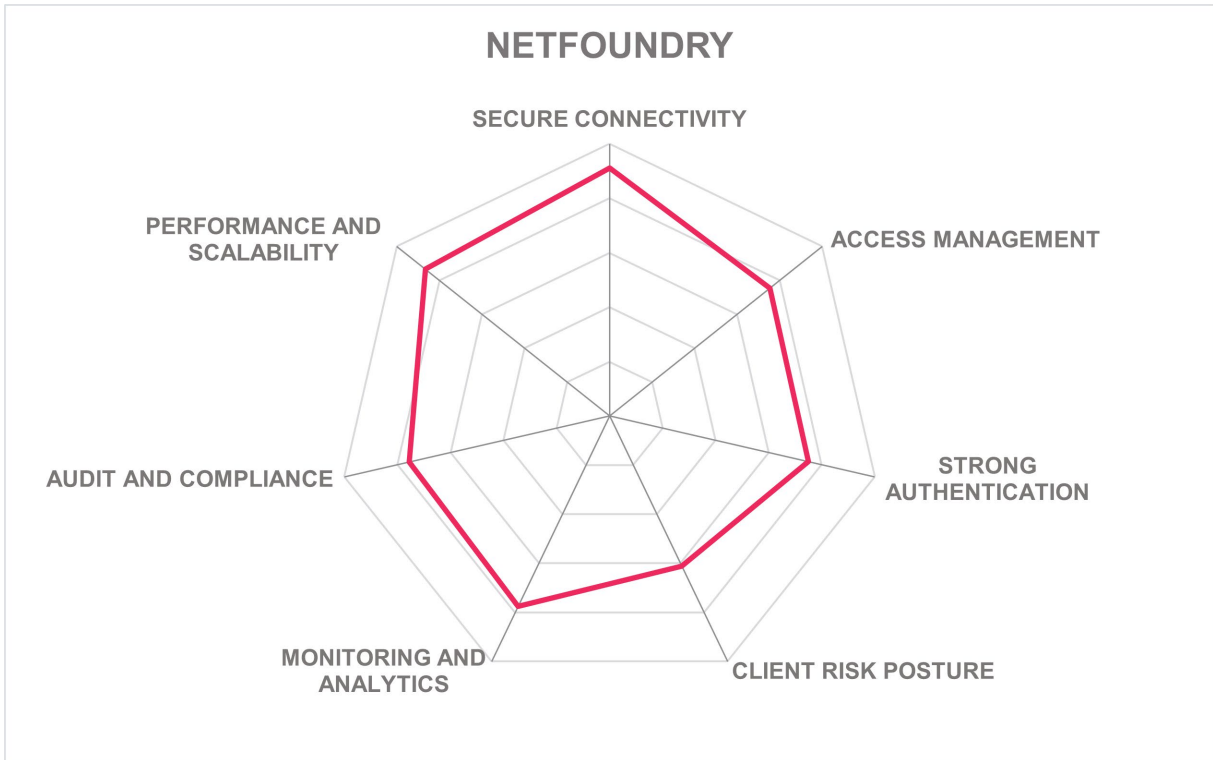
- Developer friendly
- Adherence to NIST 800-207
- Support for any use case across cloud, IoT, even VoIP
- A collection of SDKs in popular development languages
- A massive open-source ecosystem with the OpenZiti project
- Unique approach by embedding ZT enforcement directly into applications

Challenges

- Small, but growing partner ecosystem
- Training and documentation might be necessary for smooth implementation
- No support for UEM solutions, but improvements are on the roadmap
- The commercial platform is only available as a SaaS solution (unmanaged on-premises deployments are still possible)

Leader in





Sophos – Sophos ZTNA

Sophos was founded in 1985 in the UK. The company was acquired by Thoma Bravo in 2020. Sophos is a pureplay cybersecurity vendor, with a strong focus on the endpoint. The company provides solutions for endpoint security, managed detection and response, encryption, unified threat management, cloud security, firewalls, ZTNA, and email and web security gateways. However, to address the complexity often associated with ZTNA, Sophos offers a single vendor, single console, single agent solution for ZTNA, providing a unified solution.

Sophos ZTNA is a cloud-managed, as-a-service solution designed to provide secure access to corporate applications and data. Operating on and off the corporate network, it delivers a friendly user experience and enhanced security through Zero Trust principles. The solution prioritizes device health in policy-based access, rendering applications invisible to external entities. Moreover, it offers management and access for remote and hybrid environments, providing enhanced security and threat protection compared to traditional VPNs. Sophos Central provides a comprehensive management, monitoring and reporting platform for the ZTNA environment. It covers gateways, applications, and endpoint software, and includes both ZTNA and Sophos Intercept X. Deployment and management processes are streamlined through a single console in Sophos Central, which offers easy integration with existing Sophos cybersecurity products. Sophos ZTNA integrates with Azure and Okta identity providers. All integrations supported by them work with Sophos ZTNA. In addition, Active Threat Response (ATR) enables automated responses and ensures that the platform is in constant communication with other Sophos products when a potential threat is identified. Sophos also delivers part of SASE with NGFW, web gateway, in-line CASB controls and SD-WAN orchestration. This integrated approach increases efficiency and eliminates the need for additional management consoles. As a result, with Sophos as a single vendor, licensing becomes simpler with transparent costs and easier support processes.

Sophos ZTNA stands out as a flexible and streamlined solution for organizations seeking a unified, secure, and easy-to-manage approach to network access. With its emphasis on device health, user experience, and integration across the Sophos cybersecurity portfolio, it addresses the challenges associated with traditional network security products. This solution is well-suited for organizations prioritizing simplicity, scalability, and enhanced security, making it an ideal choice for those looking to consolidate their security tools under the same umbrella. Sophos appears in the overall, product, and market leadership categories.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 18: Sophos's rating

Strengths

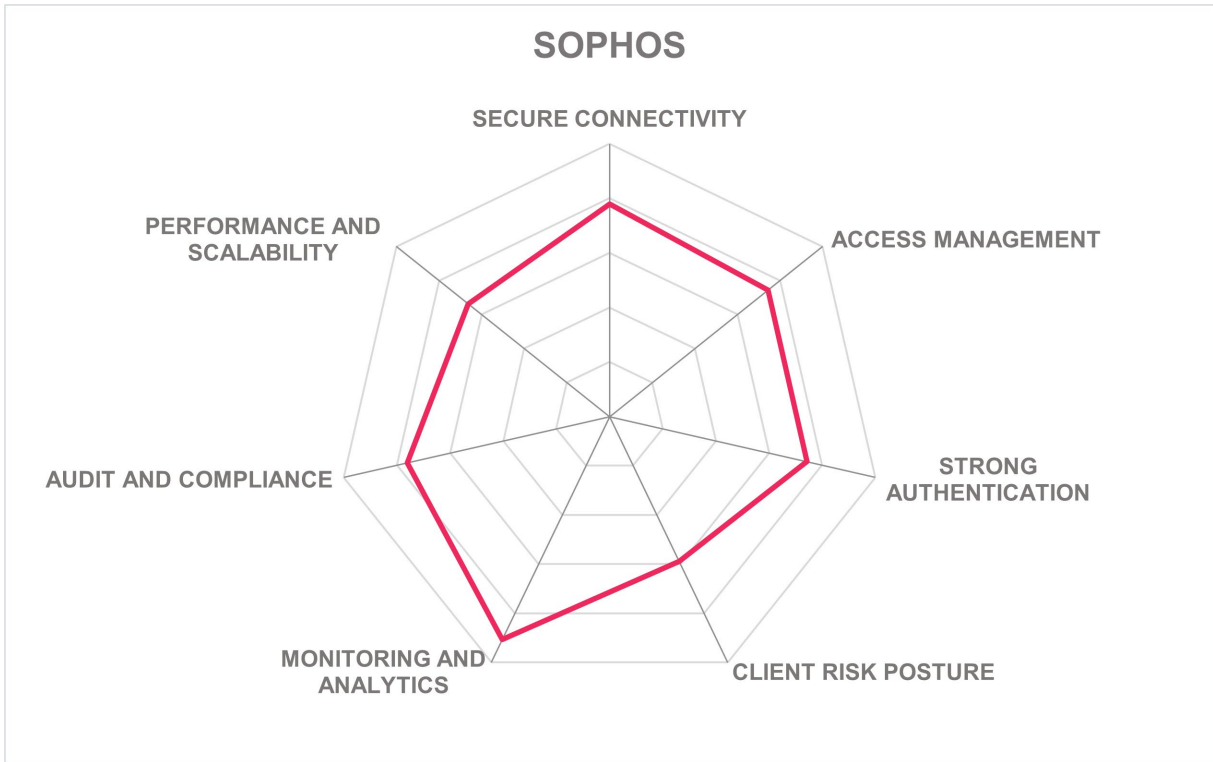
- Strong market presence
- Global partner ecosystem
- Active Threat Response
- User friendly solution
- Direct integrations with other Sophos security tools
- Unified management experience through Sophos Central
- Per-user/multiple devices licensing available as well as standard per-endpoint options

Challenges

- SAML not currently supported
- Entirely on-premises deployments are not supported
- No support for contextual risk-based authentication
- No support for policy testing tools, but troubleshooting tools are available for the endpoint and the gateways

Leader in





Systancia – Systancia Gate

Systancia is a software vendor specializing in secure remote access and workspace solutions based in Sausheim, France. Founded in 1998 and originally focusing on virtual desktop infrastructure (VDI), the company has expanded into identity management and Zero Trust Access solutions through later acquisitions. Systancia is the only software vendor combining ZTNA and PAM within the same platform, as an extension to each other.

Systancia Gate, formerly known as IPdiva Secure, is designed to provide secure access to corporate resources and applications for various remote user scenarios, including roaming users, teleworkers, and third-party service providers. Systancia Gate prioritizes access security, especially for external access points, acknowledging the heightened risk they pose for attacks. By providing access without compromising the integrity of the information system, the solution reduces the risk of data leakage and minimizes downtime in the event of an attack. In addition, the solution offers a single access window through a web portal, ensuring a friendly user experience with additional security measures such as one-time passwords (OTPs) and compliance checks. Systancia Gate's architecture accommodates multi-site and multi-VLAN configurations, catering to diverse access scenarios while adhering to the principle of least privilege. The solution is suitable for various use cases, including telework, VPN replacement, traceability of access, regulatory compliance, cloud migration, and service provider access. It supports multiple authentication methods, including FIDO2. Additionally, Systancia Gate's functionalities extend to operational traceability, providing quick access to audit trails, and its flexibility aligns with regulatory requirements, making it a good choice for Operators of Vital Importance (OVI) and Operators of Essential Services (OES). Having secured the ANSSI first-level security certification (CSPN) and achieving the ANSSI Qualification-Elementary level for identification, authentication, and access control, Systancia Gate is distinguished as a trusted cybersecurity solution for administrations.

Recently, the company has invested a lot of effort into AI-powered behavioral analytics and threat detection that serves as the feedback loop for continuous authentication within the platform. Systancia Gate is a full-featured private network access solution with a unique double barrier architecture and a strong emphasis on regulatory compliance. Systancia delivers its offering as software products or as a cloud service platform (cyberelements.io), often in hybrid deployment models. Systancia appears in the product leadership category.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Neutral
Usability	Strong Positive



Table 19: Systancia’s rating

Strengths

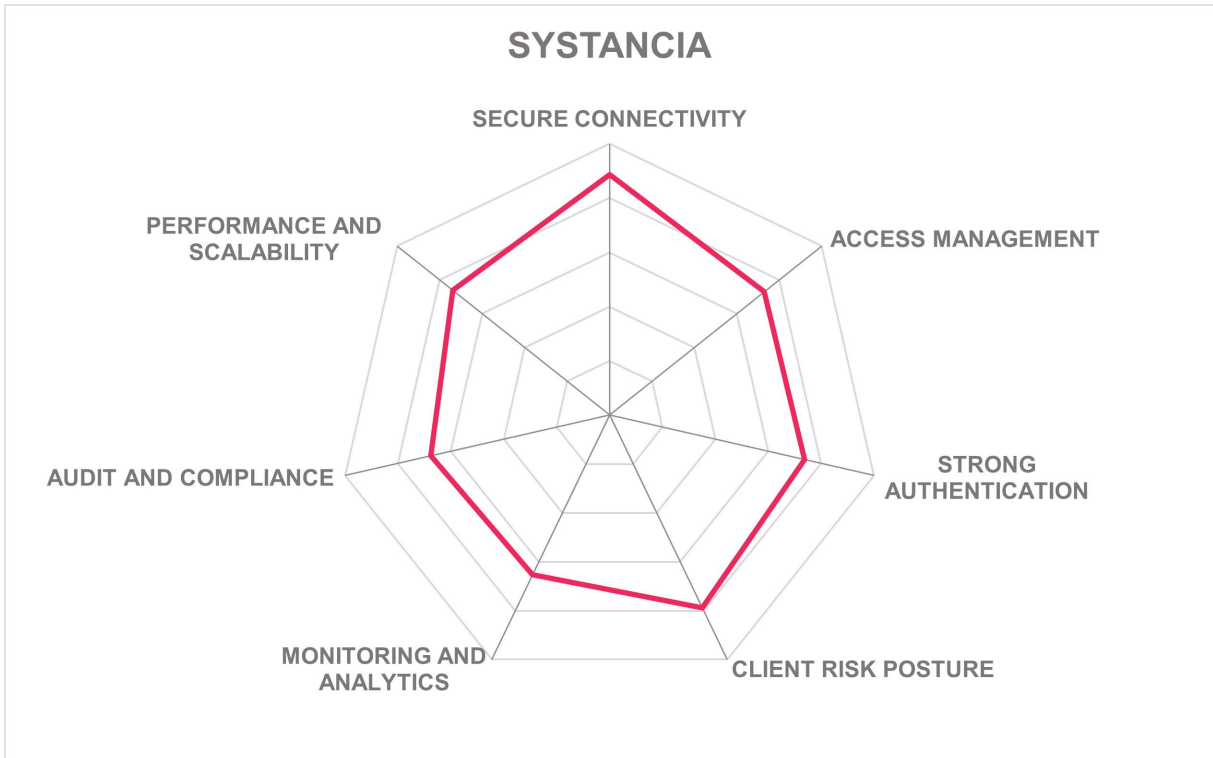
- Breadth of MFA capabilities, including FIDO2 support
- UBA capabilities
- “Single pane of glass” interface
- Supports migration from VPN through gradual policy refinement
- Strong focus on regulatory compliance, government-level certification
- Double-barrier architecture that aims to simplify deployment while maintaining high security and availability
- Advanced security features, such as dynamic random and volatile ports; URL rewriting; and clientless web isolation

Challenges

- Small, but growing partner ecosystem
- Limited market presence outside of Europe
- No support for OIDC, but it’s on their roadmap
- No support for auditing/forensic capabilities

Leader in





TrustBuilder – TrustBuilder.io

TrustBuilder is based in Gent, Belgium and was founded in 2017 with development beginning in 2016. The company delivers a cutting-edge SaaS CIAM solution that is specifically tailored for the European market. It provides a full-service identity solution consisting of onboarding, verification, authentication, and authorization. TrustBuilder.io Suite currently consists of three products: TrustBuilder.io, TrustBuilder Connect, and TrustBuilder Mobile Authenticator. The company has other offices in Netherlands, Germany, the UK, and US. Today, TrustBuilder has joined the inWebo Group, an independent vendor of MFA solutions.

TrustBuilder provides a flexible and user friendly IAM solution that caters to the needs of organizations seeking to implement a Zero Trust security model. The IAM solution is targeted at B2B, B2C, and B2E use-cases. It provides a full-service identity solution that includes onboarding, verification, authentication, and authorization capabilities. The solution is delivered as a SaaS solution for MFA and CIAM, with a local component called TrustBuilder Connect which connects the SaaS solution with customers' applications and sensitive data that can remain in their dedicated environments. The product can be delivered as a virtual appliance, container-based solution, or a managed service by third-party service providers. Docker, Rancher Labs, and Red Hat container-based platforms are supported. TrustBuilder's authentication policies allow customers to define and ease the user's journey by providing low-friction authentication methods based on dynamically driven contexts. The solution analyzes various factors such as user behavior, device information, location, and contextual data to determine the risk level of each authentication attempt. Based on this risk assessment, TrustBuilder can dynamically adapt the authentication process, requiring additional factors or steps for higher-risk access attempts, while allowing smoother access for lower-risk situations. User access principles such as attribute-based access control (ABAC), role-based access control (RBAC), policy-based access control (PBAC), and user-group are possible. Additionally, TrustBuilder works with the concept of policy-driven access control based on personas. A persona refers to a person's role or relationship to an organization with sub-attributes, allowing rules to be centered on personas rather than individual attributes.

With fine-grained access control and flexible authentication methods, TrustBuilder provides a scalable solution that continuously evolves to meet the changing needs of organizations adopting the Zero Trust security model. TrustBuilder positions itself as a good alternative to the established offerings supporting mid-market to enterprise organizations in the European market. Their solution appears in the product leadership category.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



Table 20: TrustBuilder’s rating

Strengths

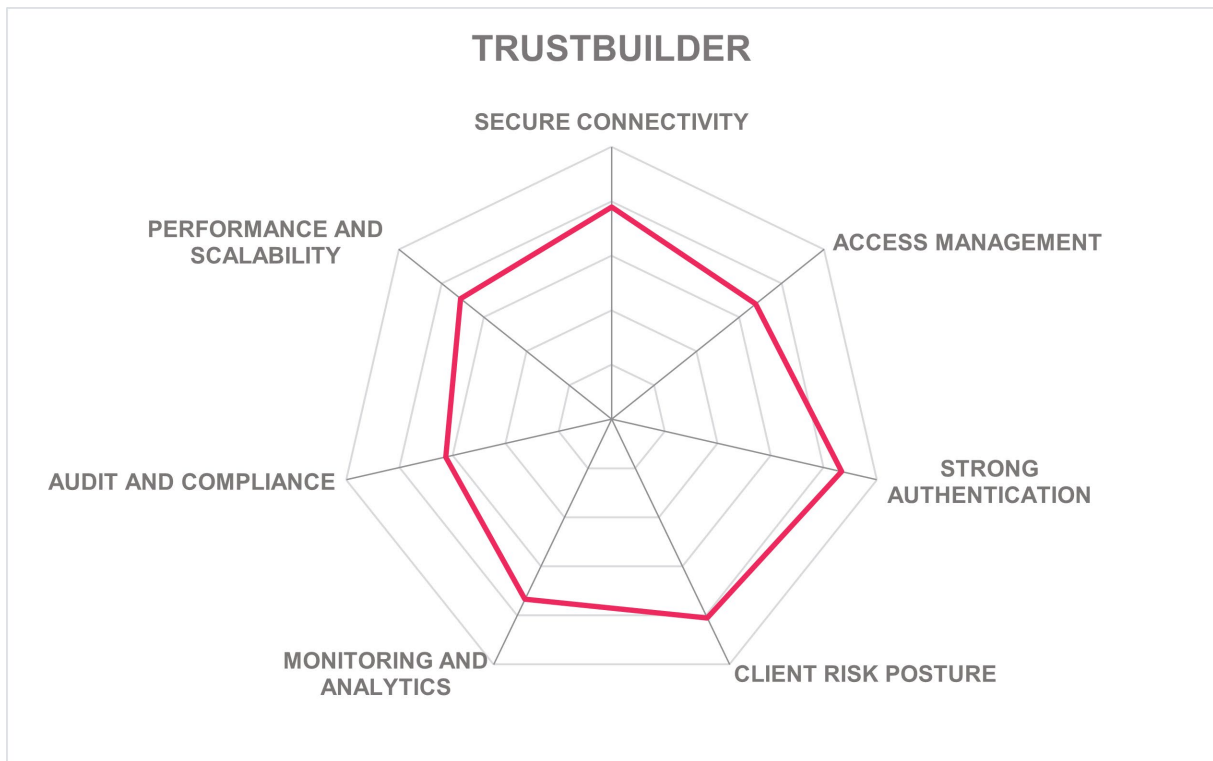
- UBA capabilities
- User friendly solution
- Lots of connectors
- Flexible and scalable solution
- Compelling use of persona-based access control
- Fine-grained access control and flexible authentication methods
- Good support for basic, popular authentication apps and hardware token authenticators

Challenges

- Currently focuses on the EU market only
- Smaller and regionally constrained partner eco-system
- No support for policy testing tools, but improvements are on the roadmap
- VPN and UEM functions are only available via partnerships

Leader in





Zero Networks – Zero Networks Connect

Zero Networks is a network security provider headquartered in Tel Aviv, Israel. Founded in 2019, the company focuses on securing existing enterprise networks with a combination of MFA-based segmentation and ZTNA capabilities. The solution allows vendor access segmentation based on user access configuration, ensuring that vendors can only access the resources they need within the network. It also avoids obfuscating all connections behind a single Network Address Translation (NAT) IP address, improving the overall security posture. Coverage is mainly focused on North America and the EMEA region.

Zero Networks Connect offers a distinctive integration of VPN and ZTNA capabilities, addressing the limitations of both. It ensures maximum network performance with WireGuard for direct, peer-to-peer connectivity, while maintaining the security benefits of Zero Trust by eliminating open ports for attackers and configure policies for user or group based granular access to internal resources. Zero Networks' approach involves separating the authentication and data transport layers, leading to enhanced point-to-point performance while still maintaining a zero-trust architecture. Notably, the VPN server remains unexposed to the internet, except for the public IP utilized by the connecting client post-successful MFA authentication through either Zero Networks or a third-party Identity Provider (IdP) and certificate validation of the client. Furthermore, the solution allows for custom policies, accommodating both employee and vendor access without compromising security. Unlike traditional VPNs or ZTNA, it provides a seamless user experience with no additional bandwidth overhead and offers maximum visibility into connected users. The architecture involves closing VPN ports, verifying users through cloud-based MFA, and dynamically opening ports only for validated users, minimizing the risk of unauthorized access. This approach combines the strengths of VPN and ZTNA while mitigating their respective weaknesses, providing a secure and high-performance solution. Zero Networks Connect runs as a virtual appliance based on Linux and can operate on any location, including cloud, that supports Linux VMs. The initial authentication is done through Zero Network's SaaS authentication, augmented by the customer's own IDP of choice.

Zero Networks Connect introduces a robust solution that effectively bridges the gap between VPN and ZTNA, offering an amalgamation of performance and security. Despite being a relatively young vendor, the company has demonstrated its ability to win and serve high-demand customers with a broad set of advanced requirements and needs in different geographies and at different scale. Organizations seeking a comprehensive network access solution, especially those prioritizing both security and performance, should consider Zero Networks Connect.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive



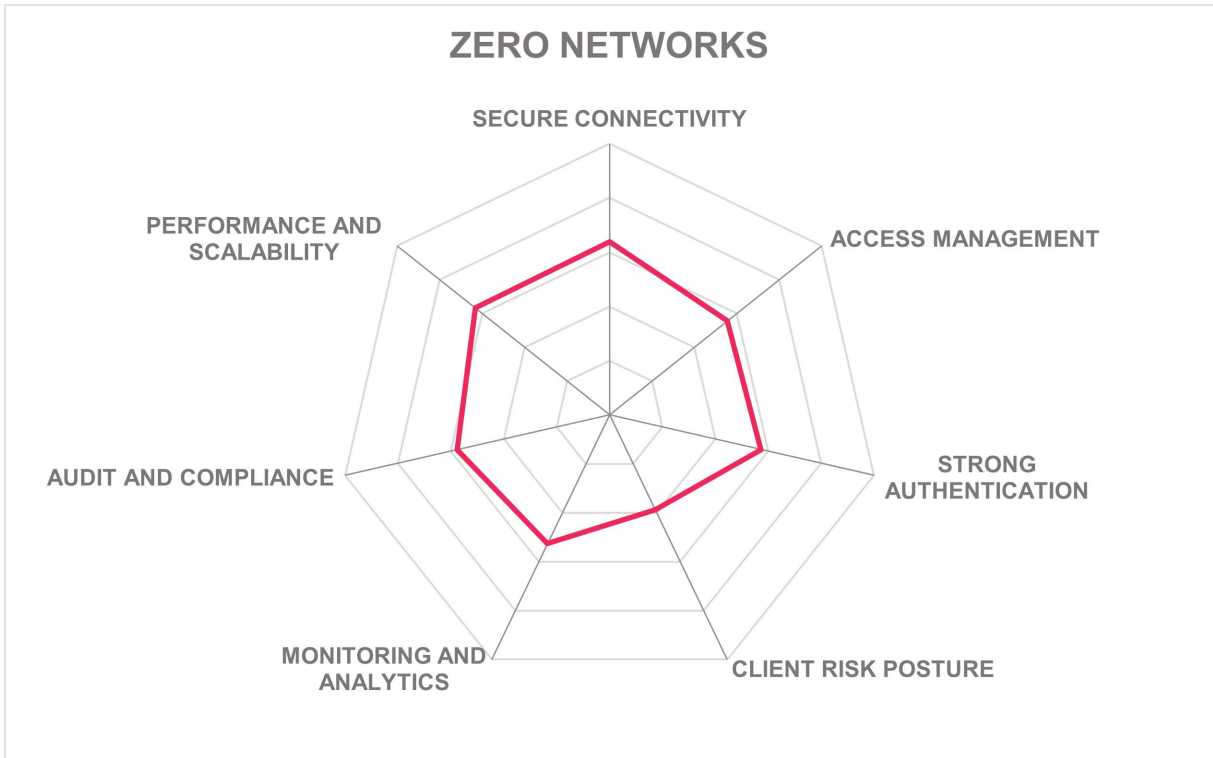
Table 21: Zero Networks' rating

Strengths

- Low latency
- Developer friendly solution
- Effective secure remote access
- MFA-enabled micro segmentation
- Flexible out-of-band monitoring and automation
- Distinctive integration of VPN and ZTNA capabilities
- Data isn't tunneled over a 3rd-party network
- Clients aren't obfuscated behind NAT
- VPN appliance only visible/open to successful MFA authenticated clients

Challenges

- No support for OIDC
- Small, but growing partner ecosystem
- Entirely on-premises deployments are not supported
- No support for delegated administration



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or could be a fast-growing startup that may be a strong competitor in the future.

Amazon

Amazon Web Services, Inc. (AWS) is a multinational cloud service provider headquartered in Seattle, USA. A subsidiary of the American retail giant Amazon.com, AWS was initially formed to consolidate and standardize the computing infrastructure powering Amazon's online business.

Why worth watching: AWS Zero Trust is a security model emphasizing identity-centric access controls and fine-grained authorization, where users and systems must continually authenticate and validate their trustworthiness before accessing applications and data. It involves leveraging AWS services to minimize attack surfaces, enforce least privilege, and enhance overall security posture by eliminating implicit trust based on network location.

Appgate

Appgate is an American software company developing cloud-ready security and analytics solutions based in Coral Gables, Florida, USA. Previously a part of Cyxtera Technologies, Appgate became an independent company in 2020.

Why worth watching: Appgate SDP, the company's flagship product, is a comprehensive, flexible, and versatile software-defined perimeter platform with a people-centric focus, powered by an innovative and efficient networking technology

Banyan Security

Banyan Security is a US-based cybersecurity company providing secure and seamless solutions for remote and on-premises access to corporate resources. Founded in 2015, it is headquartered in San Francisco, California, USA. With a strong focus on hybrid and multi-cloud deployment scenarios, Banyan's solution can adapt to the requirements of customers of any size or vertical. Although North America is the primary focus of coverage, there is also a growing presence in the EMEA and APAC regions.

Why worth watching: Banyan Security Platform stands out as a comprehensive Security Service Edge (SSE) solution designed to cater to the access and security needs of the modern workforce. With a focus on four key capabilities—VPN as a Service (VPNaaS), Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), and Cloud Access Security Broker (CASB)—this cloud-native solution ensures groundbreaking device-centric SSE capabilities.

Cradlepoint

Cradlepoint is an Idaho-based technology company that develops cloud-managed wireless edge networking equipment. The company was founded in 2006. Swedish telecommunications company Ericsson completed its acquisition in November 2020.

Why worth watching: Cradlepoint's NetCloud Exchange (NCX) offers a 5G Secure Access Service Edge (SASE) solution that integrates the high performance of 5G, the efficiency of SD-WAN, and the security of zero trust networking and Secure Internet Access.

Forcepoint

Forcepoint is a cybersecurity corporation headquartered in Austin, Texas. Although established in 2016, the company traces its roots back to Websense, a major provider of network security solutions since the late 1990s. In 2015, the company became a subsidiary of Raytheon, a major US defense contractor, but became private again in October 2020. Forcepoint offers a range of "human-centric" data protection, network, and cloud security products.

Why worth watching: Forcepoint ONE is an all-in-one cloud-native security platform that consolidates threat protection and data security, access policy management, and enforcement, and a range of cloud-delivered security solutions like SWG, CASB and ZTNA built on the common foundation.

Google

Google LLC is a multinational company specializing in internet-related products and services, known primarily for its search engine, online advertising technologies, and cloud computing services. Launched in 2008, Google Cloud is the company's suite of cloud computing infrastructure services, which also powers Google's own SaaS offerings.

Why worth watching: Google Cloud's BeyondCorp Enterprise solution, based on the BeyondCorp framework introduced over a decade ago, is essentially the first practical implementation of Zero Trust, that has been successfully deployed and operated at a large scale by Google itself, securing access for over 150 thousand full-time employees, not including the vendors/contractors Google works with.

NextLabs

NextLabs provides data-centric security software to protect business-critical data and applications. NextLabs was founded in 2004, and is a privately held company headquartered in San Mateo, California.

Why worth watching: With NextLabs Zero Trust Data Security Suite, organizations can improve security and streamline regulatory compliance, ensuring business scalability. The suite implements Zero Trust and Data Centric security principles using dynamic authorization and Attribute-Based Access Control (ABAC).

Palo Alto Networks

Palo Alto Networks is a multi-national cybersecurity company, a leading provider of both traditional network security tools and modern cloud-native security solutions. Founded in 2005, the company is headquartered in Santa Clara, California, USA.

Why worth watching: Among the company's products, Prisma Access solution is an integrated cloud-native security platform that combines advanced "ZTNA 2.0" with a full range of secure service edge capabilities. Prisma Access is a single converged cloud-delivered platform transforming network security and allowing organizations to enable secure hybrid workforces quickly and easily.

VMware

VMware is an international cloud computing, virtualization, endpoint security, and software-defined network vendor headquartered in Palo Alto, California. Founded in 1998, the company was an early pioneer in hardware virtualization technology. VMware offers a broad portfolio of security tools.

Why worth watching: VMware Secure Access, the company's ZTNA solution, is a part of a unified Anywhere Workspace platform that combines distributed workforce management, secure remote access, and comprehensive security capabilities – all delivered from the cloud.

Zscaler

Zscaler is a global information security company that provides an integrated cloud-based platform for Internet security, compliance, advanced threat protection, and other information security services. Founded in 2008, the company is headquartered in San Jose, California.

Why worth watching: Zscaler was one of the first vendors to introduce the notion of "security cloud", currently operating one of the largest specialized cloud security platforms. As one of the most deployed ZTNA solutions, Zscaler offers a combination of multilayered application protection capabilities (even including deception) with seamless user experience and performance.

Related Research

[Leadership Compass Zero Trust Network Access 2022](#)

[Whitepaper The Role of Identity for Zero Trust](#)

[Whitepaper Speeding up Zero Trust Delivery Using Managed Services](#)

Copyright

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.