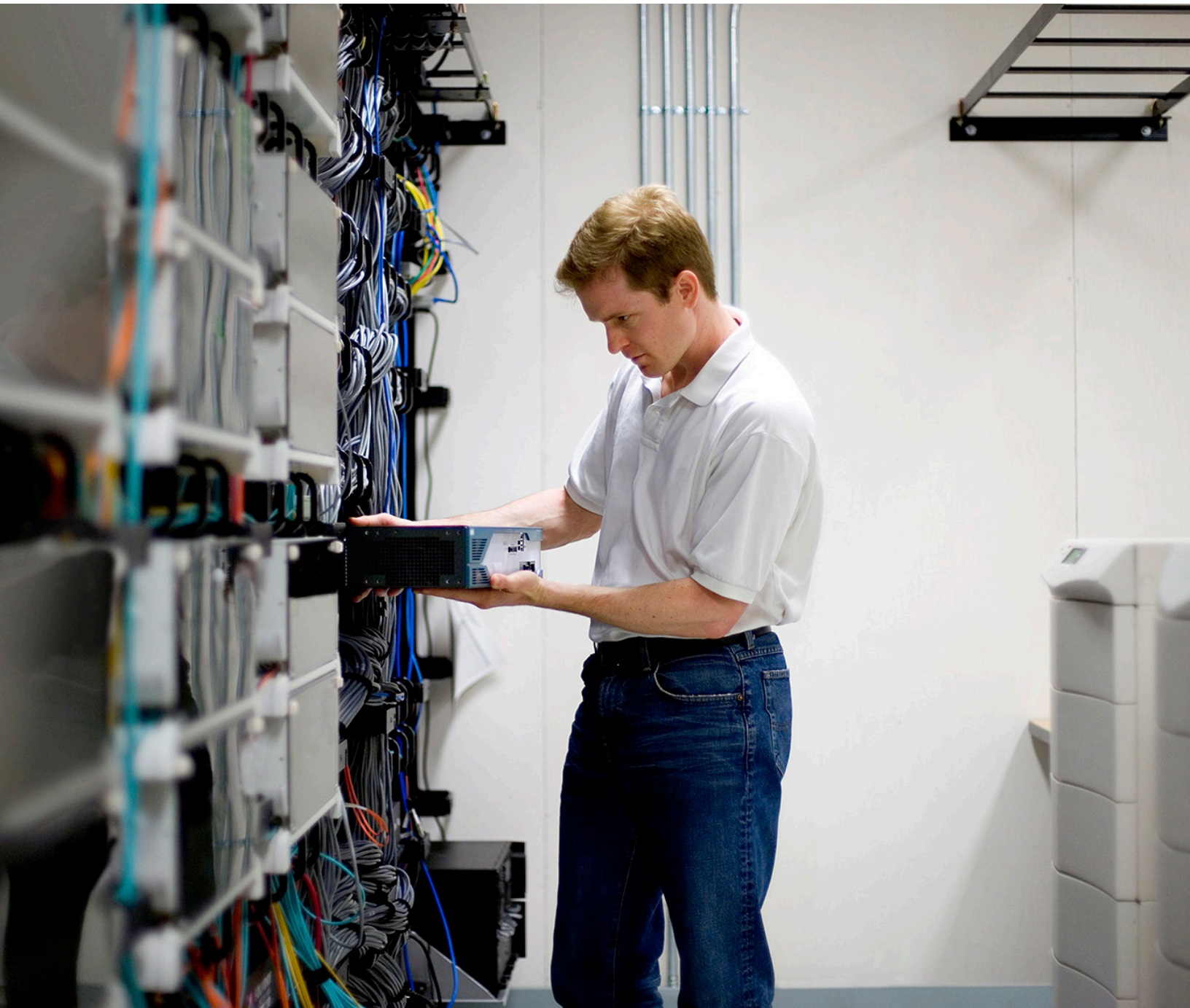# Make Your Network Edge Intelligent and Meet Tomorrow's Needs Today

Executive Summary

In the new digital business reality, the network edge has never been more important. Often overlooked, the network edge is the cornerstone that determines whether digital success is realized or lost. Consider everything that occurs at the network edge:

- It's the first line of defense against infiltration of untrusted or malicious devices.
- It's the conduit that delivers—often highly invested—applications and services to target audiences.
- It's the strategic gateway to connect widely distributed organizations.
- It's the bridge between your organization and your customers.
- It's the spot where new Internet of Things (IoT) devices are connected and managed.
- It's the optimal place to really understand what's happening with your business.

The network edge is sometimes deployed with the belief that all network solutions are essentially the same. This isn't true, because new digital business requires vast intelligence at the edge. Cisco delivers solutions and strategic functionality to achieve business success. We deliver a new network architecture that starts with the end user and continues to where applications are hosted, with a focus on:

- **Enabling faster innovation** through better experiences and highly granular insights across users, devices, applications and threats.
- **Lowering cost and complexity** to simply establish policy and manage change at scale while reducing hardware and software churn across wired, wireless, and WAN.
- **Reducing risk** with complete threat visibility and protection for internal and external risks across wired, wireless, and WAN.

Today the network is critical in enabling change in virtually all organizations as they take their digital transformation journey. This journey will help organizations innovate faster, reduce cost and complexity, and lower risk. It translates into the ability to increase agility, improve employee productivity, better engage with customers, and protect key intellectual property and assets.
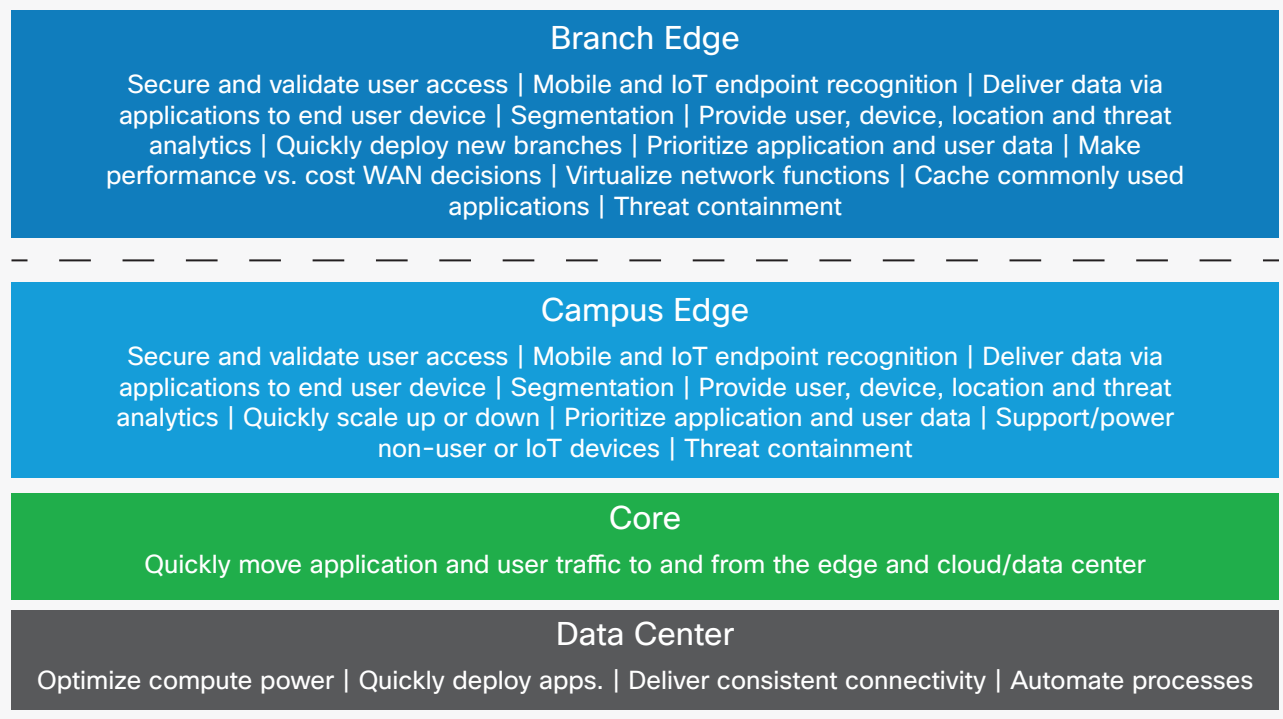
The network edge has a pivotal role to play in this transformation and carries perhaps the broadest set of responsibilities when compared to the core and to data center networks. As shown in Figure 1, when comparing the various layers of the network, the network edge has a broad responsibility in the campus. This is also true for the branch.

The Role of the Network Edge

Digital transformation makes the network edge more important than ever before. Consider everything that happens at the edge of the network:

- **It's the first line of defense.** The edge is where policy is applied and validated, without limiting your ability to access the things you need. If access is not properly managed, then your business can be susceptible to infiltration or threat proliferation, and the criticality grows as the threat landscape increases. The device, firmware, and even the operating system are all points of compromise.

Figure 1.   Network Layers and Their Functions

Branch Edge

Secure and validate user access | Mobile and IoT endpoint recognition | Deliver data via applications to end user device | Segmentation | Provide user, device, location and threat analytics | Quickly deploy new branches | Prioritize application and user data | Make performance vs. cost WAN decisions | Virtualize network functions | Cache commonly used applications | Threat containment

Campus Edge

Secure and validate user access | Mobile and IoT endpoint recognition | Deliver data via applications to end user device | Segmentation | Provide user, device, location and threat analytics | Quickly scale up or down | Prioritize application and user data | Support/power non-user or IoT devices | Threat containment

Core

Quickly move application and user traffic to and from the edge and cloud/data center

Data Center

Optimize compute power | Quickly deploy apps. | Deliver consistent connectivity | Automate processes

- **It's the conduit that delivers heavily invested applications.** The network edge is where prioritization occurs. A poor experience at the edge will slow application adoption, reducing return on investment.

- **It's a strategic gateway to the widely distributed organizations to connect.** Providing a seamless experience to your employees, partners, and customers—wherever they happen to be—is most important. A second-class network will deliver deviating levels of services to key audiences.

- **It is the bridge between the organization and their customers.** If you're a part of a retail or hospitality business, sub-par access will stunt your ability to connect with customers on a personal level and negatively impact your brand.

- **It is built to power and support growing IoT device demands.** The network edge adapts the physical environment by moving virtually all industries into the digital age by improving operations and lowering costs. Without the right functionality at the edge, organizations can be left behind in terms of cost reduction and operational efficiencies.

- **It is the optimal place to understand what is happening with the business.** In a distributed network, only the edge sees all the data traffic, by harvesting data and analytics from the edge.

Data about users, applications, devices, and threats businesses can derive insights that truly help in making better decisions to support employees, reduces risk and cost, and deliver information to the targeted audience. Without the right level of consistent granularity, this data becomes skewed and untrusted.

Is Commoditization of the Edge a Good Thing?

Many organizations are being tasked with becoming digital-first to deliver faster innovation, better experience, and higher security. However, refreshing the network to meet these demands is a daunting task because the network foundation established today will need to support the business in the coming years. Choosing a networking vendor is a critical decision that will dictate whether you keep innovating and saying yes to the business or slow down while struggling with poor capabilities.

With digital transformation, no one really knows what the future holds, but one thing is clear: the demand on your network will grow exponentially. Whether it's IoT, the cloud, sophisticated security threats, or even augmented reality, digital transformation will change how you operate and serve the business.

What is good enough today, will not be acceptable in the near future—and it all starts with the network. You have to innovate faster, reduce cost and complexity, and control risk. Organizations that are truly digital ready know that as they drive toward these changes they can't compromise on what matters.

What Is the Risk?

Being ready for the digital-first world is not about addressing a single place in the network. It is about starting at the network access edge and using common functionality in the core and the WAN with a digital-ready architectural approach. Why is this broad approach so critical? It's because today's digital-first world moves faster and pivots quicker, which means you and your network need to be ready. Organizations that are ready for the digital world don't take unnecessary risk by compromising on what matters. They know that:

1. It takes only one bad experience to render your latest innovation useless.

   Inside your business, it's all about innovation. But at the edge, where your apps meet the real world and where new IoT devices will drive fundamental business change, inconsistent connectivity and slow performance could turn off users for good. This affects device performance and cuts off the insights you need to stay competitive. With Cisco, insight is in your DNA: not only insight into the network that improves performance, but also real-time consumer insights that create more personalized experiences.

2. It takes only one "no" to ruin your reputation.

   Your world is moving fast, and if you can't keep up you will be discarded, essentially making you a fourth utility. Adding to this complexity is that resources and budgets are slim. Configuring and reconfiguring your network branch by branch and device by device can turn a "simple" update into a TCO sinkhole. With Cisco, automation is in your DNA. This allows you to automate and manage your entire network—wired, wireless at your campus, through the WAN, and in your branches—as a single entity from a single place.

3. It takes only one incident to become everyone's problem.

   We don't need to tell you what network downtime costs. Nor do we need to talk about how cybersecurity plays an important role in ensuring uptime by keeping malware from threatening your network services.

So why would you buy networking infrastructure that doesn't control access, prevent attacks, and detect and contain breaches? How can you trust a company with building your foundational network when it is unable to make that network secure? With Cisco, you can turn your network into a sensor of threats and enforcer of security policy, at the branch and HQ, wired and wireless. Don't leave security to the other guys.

Cisco Delivers Intelligence at the Edge

Digital-ready organizations build on the Cisco® Digital Network Architecture (DNA) that delivers innovation and intelligence everywhere in the network. Why? It is simple. Cisco DNA is focused on protecting, simplifying, and enabling the business, end to end. Only Cisco can deliver this because Cisco DNA is the only solution that allows you to:

1. Provide better experiences and gain highly granular Insights across users, devices, applications, and threats. Being digital ready means delivering the right experience to empower employees, engage customers, and deliver valuable insight to optimize the user experience, develop new revenue streams, and control costs. The high-availability infrastructure identifies changes and automatically adapts to support increased capacity. As the only strategic network partner with Apple, Cisco allows organizations to deliver up to a 20 percent increase in audio quality, up to a 90 percent reduction in web browser failures, and up to an 86% reduction in network message load from iOS devices during roaming. Industry-leading location accuracy up to 1 meter and the ability to use real-time NetFlow data gives a concise understanding of user interaction and threat impact. This provides a real-world depiction of what is truly happening in your environment.

2. Simply establish policy and manage change at scale while reducing hardware and software churn across wired, wireless, and WAN. The ability to manage all network domains as a single network fabric from a centralized location speeds up the time to adapt the network and optimize the user experience, with organizations achieving a 79 percent reduction in deployment costs. An open and programmable infrastructure that delivers APIs across the LAN, WLAN, and WAN and within other strategic data stores allows you to collect, develop, and deploy new applications and control mechanisms on their own.

A wide community of developers exists to learn from and co-create with to gain the benefit of best practices and Cisco guidance to meet any use case.

Completive solutions are able to manage one or two network domains, such as wired and wireless, but do not deliver end-to-end centralized management. Competitive solutions that just use APIs do not have the tight community and expertise that Cisco delivers.

3. **Complete threat visibility and protection for internal and external risks** across wired, wireless, and WAN. The network acts as a sensor and an enforcer by validating traffic against policy at every network hop. This ability allows the network to identify and remediate potential threats quickly, reduce risk, and uphold compliance. In turn, organizations avoid 99.2 percent of threats and adapt their network to new threats 98 percent faster than with traditional methods. They also achieve a 140 percent return on investment.

Other solutions look for threats only at the access layer and use information from known malware. This means modern malware can infiltrate the network disguised as normal traffic and then conduct malicious activity from the interior of the network. The organization is left to puzzle information from disparate sampled data to try to identify where impact occurs so they can remedy it.

Digital organizations are also breaking down silos, knowing that the production network and data center need to work in unison to deliver better user, device, and application experiences. Cisco DNA is focused on analyzing, simplifying, automating, and protecting the business by delivering innovation and intelligence from where the users begin to where the applications end.

Provide Better Experiences and Gain Highly Granular Insights

The network edge is the point at which employees are empowered, customers are engaged, and IoT devices are enabled, and it is a source of valuable insights.

- **Provide the very best user experience for iPhone and iPad on a corporate network.** With new features in iOS 10 combined with the latest networking software and hardware from Cisco, businesses everywhere can take full advantage of their infrastructure to deliver a great user experience for apps, calling, and collaboration. Cisco and Apple have joined together on development efforts to deliver the best wireless connection for your mobile employees and to offer an easy way for IT to prioritize the apps that matter most to business when using iOS devices on a Cisco network. No other vendors in the industry are providing this level of interoperability.

- **Gain always-on, always-ready reliability at the network, access, and end-device level for zero user impact.** Cisco solutions deliver networks with multitiered resiliency to deliver confidence that the network is there when it is needed and that you and IoT devices are powered and working for your business.

- **Automatically adapt the Wi-Fi network when and where it is needed.** Deliver a constant high-quality experience with wireless innovations that go beyond the wireless standard. Cisco networks improve the capabilities of legacy and the latest mobile devices, remove interference, and adapt capacity to meet varying demands.

- **Better support IoT devices with failsafe power to assure availability and improve performance.** Cisco networks have failsafe power built into the switches that IoT devices connect to, coupled with fog computing that provides the ability to automatically decide the optimal place to process data from IoT devices . Cisco networks are prepared for the new connected world.

The difference between being business relevant and being just another utility is dependent on how well the user experience is delivered and on data accuracy.

Enterprises can expect a higher reliability for real-time apps, with up to a 20 percent increase in audio quality for Wi-Fi calling, a 50 percent reduction in network management overhead due to fewer service set identifiers (SSIDs), and enhanced performance with up to an 86 percent reduction in network message load from iOS devices, while roaming end users can benefit from longer battery life when using iOS devices on a Cisco network.

- Gain a realistic view of users, devices, applications, and threats with up to 1-meter accuracy. Cisco provides industry-leading location-based data granularity to better understand how users interact with the environment to make better business decisions.

Business-to-consumer (B2C) organizations such as retail, hospitality, and education have been able to achieve less than 1-meter location accuracy with Wi-Fi plus Bluetooth Low Energy BLE and produce direct revenue increases. Some examples include a 20 percent increase in non-room revenue by Hyatt Regency, a threefold increase in customer dwell time, and an 80 percent improvement in user experience at the Starry Bowar mall – all while delivering personalized mobile experiences.

Simply Establish Policy and Manage Change at Scale

Organizations struggle to get away from the costly and the time-consuming act of constantly reconfiguring and adapting the network device by device to meet the ever-increasing demands of the business. Cisco provides a way to simply manage the network, whether it is one or many sites. The digital business requires the network to be more agile, which means the network needs to automate processes and new services with day-zero and day-one capabilities and remove the need for manual intervention. This capability enables the digital business to deploy and maintain a network suitable for today's quickly evolving landscape.

- Manage a single quality-of-service (QoS) policy and adapt based on performance across the network. Cisco solutions use the same QoS policy across the LAN, WLAN, and WAN to provide better application handling from end to end. They can automatically prioritize key applications, such as latency-sensitive voice and collaboration, based on usage and service ratings, with application visibility and control taking into account changes in the environment along with QoS definitions to make sure business-critical applications receive a high priority.

- Turn up new network segments and branches faster and at a lower cost with zero-touch deployment. The plug-and-play application of the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) reduces resource consumption and time needed to configure, deploy, and turn up new network branches and segments with zero-touch deployment for Cisco Enterprise Networks routers, switches, and wireless controllers.

- Add new software and hardware functionality without replacing equipment. Cisco networks allow organizations to use existing access points, controllers, and switches to add new functionality when it becomes available without performance impact.

- Achieve simple license management and portability for infrastructure upgrades. Take advantage of new capabilities important to your business without going through the time-consuming process of license management. Transfer existing software licenses to new hardware when upgrading infrastructure.

- Expand functionality by using your existing wireless access point footprint and power to meet new use cases. Add new functionality via modules to existing access points to add new industry-standard functionality or functionality from third-party ecosystem partners.

Cisco is able to speed the deployment and reduce deployment costs by 79 percent by decoupling software from hardware and virtualizing the WAN edge.

Complete Threat Visibility and Protection for Internal and External Risk

The network edge is the number one point for unauthorized or hostile access, because it's where users and devices are onboarded within both the campus and the branch. It has to be trusted to identify and control what's getting onto the network. It also needs to work in unison with security solutions in the core and branch to defend against the latest malware attacks.

With the Cisco Identity Services Engine, Cisco TrustSec®, and Cisco StealthWatch, you can turn your network into a sensor and enforcer to improve protection and response time. Meaning you are able to avoid, identify, and remediate threats as they enter the network or, if they get past the initial access, as they proliferate through the network. Cisco DNA allows you to:

- **Manage user and device access with software segmentation,** not lots of static VPNs and SSIDs. Assure that employees, guests, contractors, temporary workers, and customers have access to the things they need and not to information they don't. This software-based user and device group approach offers greater scale and allows you to reduce configuration errors, add more devices faster, and properly classify users and devices better than with traditional manual approaches, resulting in the ability to make changes 98 percent faster.

- **Embed security everywhere to detect and contain threats at the access and within the network.** Validate traffic at every network intersection in the access, core, and branch. Even if the malware is introduced via a user device or an IoT device, or someone is purposely trying to steal data, a Cisco network infrastructure can identify where the threat exists and take action to stop or limit the impact.

- **Quickly analyze and remediate threat impact using real-time NetFlow data.** Go beyond conventional threat detection and harness the power of NetFlow. With it, you get advanced network visibility, analytics, and protection. You see everything happening across your network. You can uncover attacks that bypass the perimeter and infiltrate your internal environment.

- **Use a global ecosystem to keep ahead of the latest threats throughout the entire network.** Keep updated on the latest threats to avoid or rapidly eliminate threats across the entire network from a single place, using threat data shared from around the globe, to stop attacks even if you cannot see them, promptly notify you of their existence, and close the door to prevent it from accessing data stores or other devices in the network.

Defending critical assets at the edge. Organizations can avert ~100% of network breaches by using the network as both a sensor and an enforcer. This can be done while also delivering deeper insights to improve protection and achieve faster response.

A recent Forrester research paper shows that Cisco TrustSec allows IT to implement changes 98 percent faster, lower cost by up to 80 percent, and deliver a return on investment of 140 percent.

Continued Innovation at the Network Edge

With the expected explosion of connectivity bringing significant opportunity, companies are starting to recognize that this transformation will require fundamental changes to their network infrastructure and the ability to manage and analyze the data. We are leading the way through this transformation by driving innovation in network infrastructure, management of infrastructure, and analytics to extract actionable insights from the data.

Cisco aims to transform troubleshooting that is reactive to proactive, and reduce resolution time from days to minutes. We will do so by treating every device in the network as a sensor and a distributed data processing element. By getting data from devices in the edge, distributing processing closer to the source of the data, we can perform analytics at line speed to generate actionable insights through machine learning.

With the largest installed base and custom ASIC solutions, Cisco is uniquely positioned to design hardware and software optimized for analytics. Harness the power of installed base. Wired and wireless combined in one network will mean that intelligence on the edge can help you troubleshoot problems, whether they happen at the edge or not, in seconds. And over time, correct potential problems even before they occur. This will help IT departments deliver on the service-level agreement SLA for the network and application performance required for the future.

Conclusion

With so much depending on the network edge, the commoditization of the wired and wireless LAN and WAN introduces risk that could result in security breaches, loss of productivity and revenue, loss of opportunity, and lack of visibility. The Cisco network edge allows organizations to go beyond an off-the-shelf, standard-bound approach, delivering high-value intelligence at the edge to innovate faster, reduce cost and complexity, and lower risk. This approach allows organization to:

- Protect the business with a strong first line of defense

- Confidently deliver applications to target audiences

- Deliver a seamless experience to employees anywhere

- Engage with customers to drive new revenue streams

- Better manage IoT devices and optimize the physical environment

- Provide the optimal view as to what is truly happening in the business

For More Information

To learn more, visit the Cisco Unified Access™ Technology page at http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.