BUILDING A MODERN, SCALABLE SECURITY ARCHITECTURE

Cybersecurity has never been more important, as society has become increasingly dependent on always-connected services. Business, IT, and security leaders must work closely together to operate effectively within this technology-enabled world. Yet, while well-thought-out strategies and architectural decisions can endure some level of expansion, a fundamental re-architecture is often needed to support future growth.

Current security strategies aren't enough to keep up with advancing technologies.

As more security controls are needed and security architects race to close security gaps, complexity increases. Despite investment in widely accepted industry security strategies (e.g., zero trust, SASE, XDR, generative AI, etc.), most organizations continue to struggle to achieve desired security outcomes.

68% of organizations employ more than 15 security tools, each operating with its own limited view into what is happening.
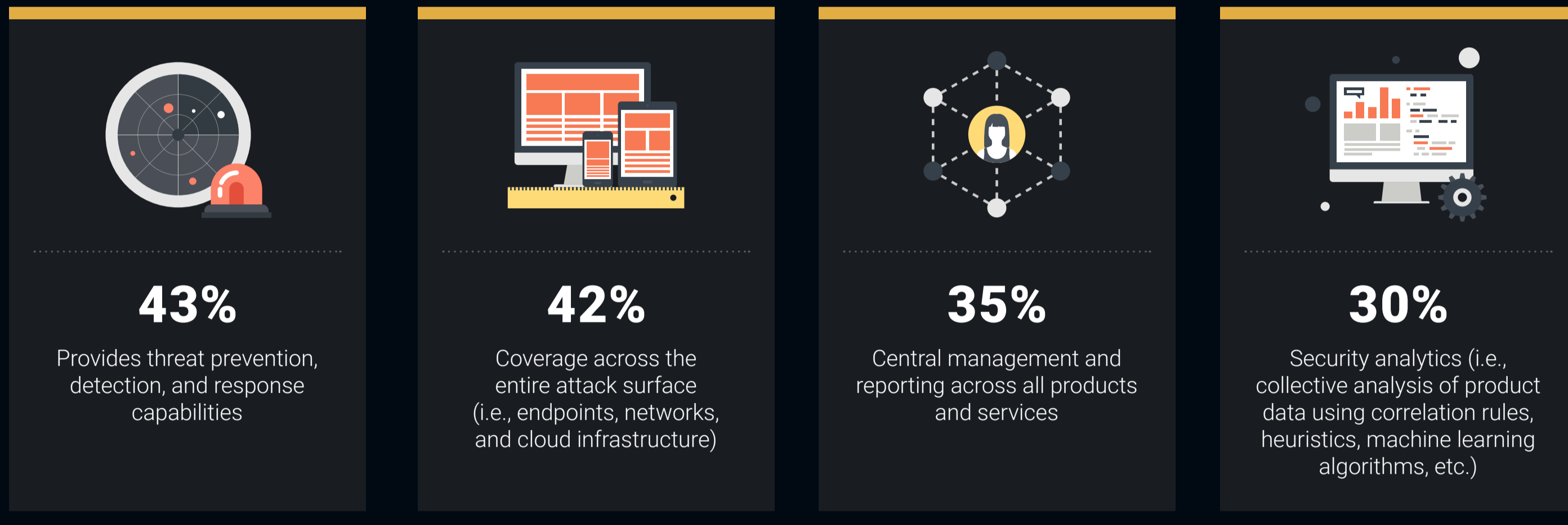
0%   100%
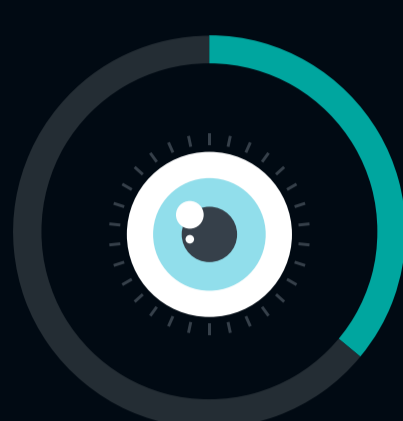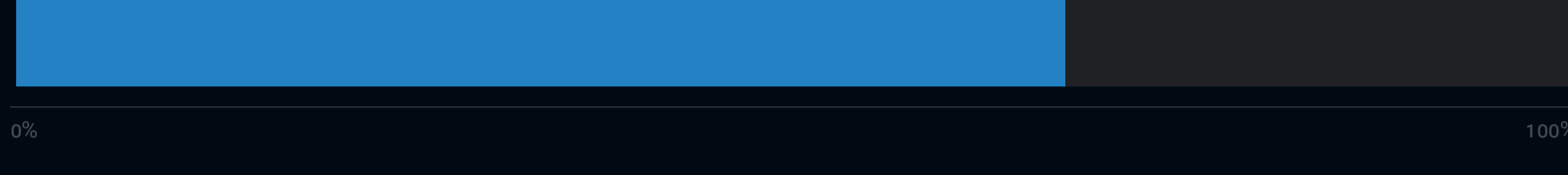
36% of organizations have trouble gaining a complete picture of their security status due to the increase in separate security tools.

66% of organizations are actively consolidating security operations tools, aimed at reducing cost, complexity, and policy alignment.

Security teams want platforms to provide prevention, detection, and response capabilities across the entire attack surface. Centralized management and security analytics matter too.

» Most important attributes of a cybersecurity "platform" for threat detection and response

43% Provides threat prevention, detection, and response capabilities

42% Coverage across the entire attack surface (i.e., endpoints, networks, and cloud infrastructure)

35% Central management and reporting across all products and services

30% Security analytics (i.e., collective analysis of product data using correlation rules, heuristics, machine learning algorithms, etc.)

Cisco Security Cloud enables organizations to protect their entire IT ecosystem while simplifying the end-user experience.

The Cisco Security Cloud is an AI-enabled unified platform for end-to-end security across hybrid multi-cloud environments. It provides the needed capabilities to securely connect people and devices to applications, data, and tools, while optimizing performance and improving security.

» The Cisco Security Cloud Platform Enables Organizations to:

Simplify security with a cloud-native platform that securely connects users, devices, and IoT to their systems, apps, and data across multiple clouds and networks.
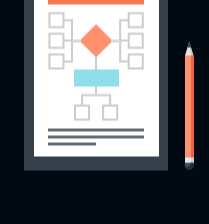
Support all cloud platforms, providing flexibility and scale with no vendor lock-in.

Reduce friction for end users, simplifying how they interact with their data and applications and bringing security closer to them.

Leverage APIs for integration and a robust developer ecosystem so that their environment can evolve along with your business.

Increase efficiency with unified policy, management, UI, and dashboards to help security teams work seamlessly from end to end.

Hunt, investigate, and remediate threats through actionable insights across networks, clouds, endpoints, and applications.

Operating at machine scale

Businesses need to have visibility and the ability to process massive amounts of data within microseconds. They need to operate at machine scale, rather than at human scale. The use of AI and ML is core to achieving this scale and requires the analysis of both networking and security telemetry.

" Because no two operating environments are the same, **AI-driven technologies learn user trends, services, and application metrics specific to a business operation,** generating a customized performance curve for analytical decisions."
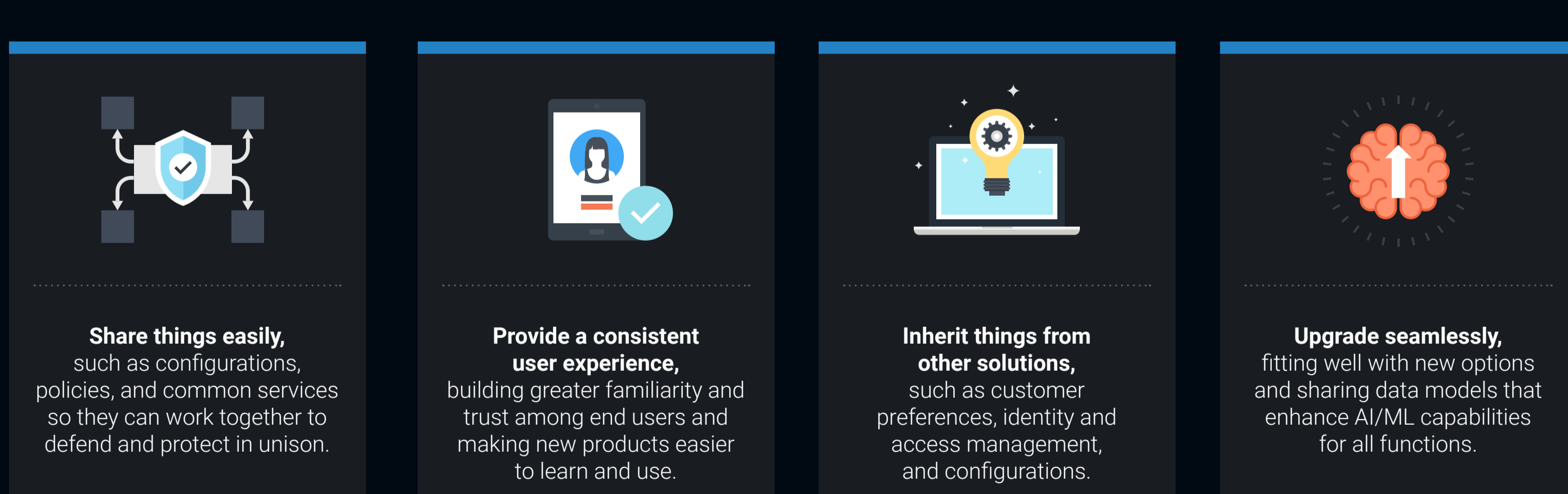
- *Dave Gruber*, Prinipal Analyst

This AI-driven baseline is continually adapted as it grows and changes, enabling the Cisco Security Cloud to make decisions for what is normal and what is not. This personalization is the true power of AI and ML within Cisco's products.

Inherent advantages come with integrated solutions.

Integrated Security Solutions Improve Outcomes

When security solutions work together, they can drive improved outcomes in efficacy, efficiency, and scalability. They can further help people work better together in a more consistent, collaborative manner. Integrated solutions offer several benefits that independent tools do not, including that they:

Share things easily, such as configurations, policies, and common services so they can work together to defend and protect in unison.

Provide a consistent user experience, building greater familiarity and trust among end users and making new products easier to learn and use.

Inherit things from other solutions, such as customer preferences, identity and access management, and configurations.

Upgrade seamlessly, fitting well with new options and sharing data models that enhance AI/ML capabilities for all functions.

Accelerating Operational Performance Across User Types

When security solutions work together, they can reduce friction across many types of users and have the potential to drive significant positive outcomes for users:

End users: Security solutions improve end-user experiences through seamless and fast connections, and a continuous and dynamic granting of trust.

IT teams: The solutions provide centralized, cloud-delivered policy management across multi-cloud and on-premises environments that reduces effort and improves consistency.

Security analysts: They enable security controls, analytics, and advanced AI capabilities to work collaboratively, stopping threats faster and providing better protection, detection, and response, all with less analyst intervention required.

Application developers: They also free developers to focus on business logic instead of security functions by implementing security policies through code.

Integrated security solutions drive value beyond basic security objectives.

Legacy security strategies and architecture are hindering security program advancement at a time when security is more critical than ever. Security leaders face unprecedented challenges in complexity and diversity, requiring new thinking in their approach. More collaborative, integrated architecture is needed to enable expansion and growth without adding complexity. TechTarget's Enterprise Strategy Group recommends that security leaders consider moving to integrated platforms, such as Cisco Security Cloud, to accelerate and scale security programs.

CISCO