
Security Everywhere:
A Growth Engine for the Digital Economy

Seizing new business opportunities by embedding security into the intelligent network infrastructure and across the extended network

Ever-expanding connectivity as a result of modern networks is transforming our world. We've seen this for some time with the widespread adoption of cloud computing which has created a digital economy that is fueling new business opportunities through greater speed, efficiency, and agility. Building on the power of the cloud, the Internet of Everything (IoE) is generating unprecedented opportunities for networked connections among people, processes, data, and things and is presenting a $19 trillion global opportunity to create value.*

We are now facing a similar evolution with respect to security. To capture opportunities made possible by new digital business models and the IoE, businesses of all sizes must also engage in a secure way. To do this, security must be everywhere—embedded into the heart of the intelligent network infrastructure and spanning throughout the extended network. Security needs to be as pervasive as the IoE itself.

A Complex Environment

Modern networks go beyond traditional walls and include data centers, endpoints, virtual environments, branch offices, and the cloud. These networks and their components constantly evolve and spawn new attack vectors, including mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and even vehicles. This increased connectivity changes the game on where data is stored, moved, and accessed. It also has fueled a shift to digitization, the transformation of objects like movies, books, healthcare records, and money into bits and bytes, which adds to the increasing amount of data. Further, mobility and the cloud have dramatically increased employee productivity and satisfaction, but also replaced the traditional network perimeter with a constantly morphing set of users, locations, applications, access methods, and devices. This presents the dual challenge of protecting a dynamic perimeter and creating a near-infinite number of points of vulnerability. All of these considerations create greater opportunities for attackers who are becoming increasingly sophisticated and professional in their approach.

So how have we evolved our approach to security? The truth is, not nearly enough. Caught in a cycle of layering on the latest security tool, it isn't unusual to find organizations with 40 to 60 or more different security solutions that don't—and can't—work together. Building up security staff in lockstep isn't possible given a worldwide shortage of security professionals estimated at one million people. IT teams struggle to deal with unrelenting attacks while attempting to skillfully manage bloating volumes of IT security tools.

Attackers are taking advantage of gaps in visibility and protection and the strain on security professionals that this complexity and fragmentation creates to penetrate the network. Environmentally aware, attackers navigate through the extended network, evading detection and moving laterally until reaching the target. Once they accomplish their mission, they remove evidence, but maintain a beachhead for future attacks.

*http://ioeassessment.cisco.com/learn

Defining Security Everywhere

To truly address today's dynamic threat landscape, evolving business models, and considerable complexity, security must be embedded into the heart of the intelligent network infrastructure and across the extended network—from the data center out to the mobile endpoint and even onto the factory floor. This rings true, not just for enterprises or small and medium-sized businesses (SMBs) managing their own networks, but also service providers that must be able to protect their customers through the network infrastructure they use to deliver their services.

With security everywhere, businesses can operate in an environment where security is:

- Pervasive – to persist across all attack vectors
- Integrated – to share information, intelligence, and capabilities with a rich ecosystem of applications and services
- Continuous – to allow for ongoing protection across the full attack continuum—before, during, and after an attack
- Open – to integrate with third parties, including complementary security technologies and threat intelligence feeds

Security *Is* Everywhere

Security everywhere is a reality and is available today. By combining our historical position of strength in network infrastructure with security innovation, Cisco has embedded security into and across the extended network without impeding business-critical resources and processes. We're helping customers extend security to wherever users are and wherever data is with advances in five key areas:

1. The broadest set of solutions from the network to the data center, cloud, branch, and endpoints

Most recently, Cisco introduced:

- Cisco® ASA with FirePOWER™ Services for SMBs, enterprise, and ruggedized environments extend integrated threat defense (firewall, application visibility and control [AVC], URL filtering, Advanced Malware Protection [AMP], and next-generation intrusion prevention system [NGIPS] on a single device) to organizations of all sizes and across all locations, even in the harshest environments.
- Cisco Cloud Web Security on Intelligent WAN protects against web-based attacks at branch offices.
- Cisco TrustSec® technology plus Application Centric Infrastructure (ACI) simplifies the provisioning and management of secure access to network services and applications and protects against targeted attacks and lateral movement of malware in the data center with software-defined segmentation.
- Cisco Secure Data Center automates provisioning of FirePOWER security (Cisco NGIPS and Cisco AMP) in the data center with ACI policy-driven application profiles.
- FirePOWER Threat Defense for integrated services router (ISR) embeds enterprise-level threat defense (NGIPS, AVC, URL filtering, and AMP) into the network fabric where dedicated security appliances may not be feasible, such as branch office locations.
- Cisco Hosted Identity Services provide context-aware identity enforcement as users connect from any device, anywhere, across the extended network, delivering a streamlined and more secure enterprise-mobility experience.
- Service provider security solution allows service providers to take full advantage of open and programmable networks while reducing risk to customers and data with multiservice security integration, unprecedented performance and scaling, and advanced orchestration and management delivered in a purpose-built, carrier-class Cisco FirePOWER appliance.
- Security Services improve security outcomes by providing operational leverage and talent to supplement in-house security teams with a growing portfolio of advisory, integration, and managed services.

2. **Unmatched visibility: See once; control and protect everywhere.**

Cisco sophisticated infrastructure and systems provide visibility that spans the entirety of the network, endpoints, virtual environments, mobile devices, and the cloud, as well as the data center. To truly deliver value, this visibility must be actionable so that businesses can make informed decisions. Learn how the Cisco Talos Security Intelligence and Research Group uses this visibility for aggregation and analysis of telemetry data, creating threat intelligence for Cisco products to protect customers from both known and emerging threats.

3. **Integrated security across the extended network; sharing intelligence, information, and capabilities for systemic response**

To combat multifaceted attacks launched through multiple attack vectors, businesses require advanced threat protection in combination with security sensors and enforcement everywhere and a central policy platform. Cisco embeds technologies into the network infrastructure to increase visibility across all network activity, provide context based on local and global threat intelligence, and allow control using analysis and automation to dynamically protect against detected threats.

- Network as a Sensor (Cisco IOS® NetFlow, Identity Services Engine [ISE], and Lancope) uses the Cisco network as a security sensor, based on the built-in NetFlow technology and additional capabilities, to detect malicious activities and sophisticated threats anywhere within their environment.
- Network as an Enforcer (TrustSec, ISE, and Lancope integration) extends those capabilities even further, activating the embedded TrustSec technology to turn the Cisco network into a powerful policy enforcer to apply security policies, control access to online resources, and block threats and attacks.

4. **The most effective advanced threat prevention across the full attack continuum**

- Boost protection before an attack.
- Respond faster during an attack.
- Contain and remediate after an attack.

Address real-world challenges with a threat-centric approach to security for faster time to detection (TTD) and time to remediation (TTR) – learn more.

5. **Retrospective security that can detect, contain, and remediate threats even after they have entered the environment**

Continuously gather and analyze data, identify suspicious behaviors and indicators of compromise, and accelerate response to mitigate damage. Learn more about our expanded Cisco AMP portfolio that now extends endpoint threat services to remote, VPN-enabled endpoints.

Conclusion

Just as modern networks have transformed our world, modern approaches to security will as well. Embedding security everywhere across the extended network clearly increases security effectiveness against advanced attacks. But it also allows security to become an enabler for businesses to take full and secure advantage of opportunities presented by new digital business models and the IoE.