Networks are Transforming and Security Risk is Growing

The emergence of the hybrid workforce—where employees can now work fluidly between corporate offices, branch offices, home offices, or on the road—has dramatically changed how and where business is done. At the same time, more applications are moving to the cloud, expanding the potential attack surface and putting not just businesses, but public and governmental organizations in further jeopardy.

Businesses must transform their network to handle a massive, ever-growing number of users, devices, and applications and tackle a myriad of connectivity and security challenges. **By harnessing the power and value of their network, they can drive their business priorities and enrich their customers' experiences.**

With this opportunity comes risk.

Network security challenges are evolving along with business priorities. Few organizations have enough security expertise and funding to overcome the challenges they face. Companies must choose modern networking solutions that deliver security capabilities that extend from the client device through the network and into the cloud, alongside agile and flexible connectivity solutions to close IT security gaps and deliver the experience and business outcomes demanded by leadership, customers, and staff.

Challenges

In a 2022 report, the Ponemon Institute defines the IT Security Gap as the inability of an organization's people, processes, and technologies to keep up with a constantly changing threat landscape. It diminishes the ability of organizations to identify, detect, contain, and resolve data breaches and other security incidents. The consequences of the gap can include financial losses, diminished reputation, and the inability to comply with privacy regulations such as the EU's GDPR and the California Consumer Privacy Act.

What is causing this lack of confidence in organizations and what is the role of the network equipment provider in helping close the gaps?

Attackers are sophisticated, financially motivated, and eager to attack

Cybercrime is now a trillion-dollar industry driving up costs and putting reputations at risk. Attackers are adept at using a combination of proven techniques and new innovations to test the perimeter of the network for weak points that will provide access to business-critical data and systems.

Modern networks must be protected from malware and ransomware, distributed denial-of-service (DDoS) attacks, network intrusions, and more, creating a secure platform for users, devices, and applications to perform their functions within the IT environment.

Consistent application and enforcement of security policies is getting harder

New work models are adding more devices to the network. Over 4 billion Wi-Fi devices hit the market every year. IoT devices are exploding especially in manufacturing and healthcare, with 27 billion expected to connect by 2025.[2] Each device becomes a potential risk vector. Network administrators are challenged to ensure consistent policy and management across wired and wireless environments, and to protect against sophisticated attacks.

Moving from the data center to the edge requires a combination of **traditional security solutions and secure infrastructure.**

Adoption of SaaS applications and migration of data to the cloud is increasing threat surface

Worldwide end-user spending on public cloud services is expected to grow 20.7% to $591.8 billion in 2023, up from $490.3 billion in 2022, according to the latest forecast from Gartner, Inc. This is higher than the 18.8% growth forecast for 2022.[3] Companies have to manage a mix of sanctioned (company-approved), tolerated (not ideal, but allowed), and unsanctioned (unauthorized/shadow IT) SaaS applications that employees use for both their business and personal needs.

Companies are storing and using more data than ever in the cloud, including highly sensitive business and customer data. Protecting this increased amount of data is challenging when it leaves the network and moves across multiple cloud applications and users.

Lack of visibility across the network

A secure network requires the ability to view equipment and traffic activity so anomalies can be investigated for potential risks to the environment. Without this visibility, network administrators risk being unable to identify and respond to performance or security risks before they disrupt the business.

Network Equipment Providers Play a Critical Role in Closing the Gap

IT organizations expect new approaches to security will be required to solve the security gap and 37% of them are expecting network infrastructure providers to deliver these capabilities.

Organizations should look for security capabilities that extend to all connection points across the network to stop infiltration and lateral movement, block attempts to deliver malicious payloads that disrupt traffic flow, protect access to sensitive data, and provide visibility to all points in the network.

What are the critical capabilities that companies should expect from network equipment providers?

- ✓ Secure wireless
- ✓ Robust segmentation
- ✓ Policy enforcement at every point in the network
- ✓ Granular access control policy
- ✓ Secure data in transit and breakout to the cloud
- ✓ Unified management from the cloud

Investing in the right design, the right network infrastructure, and the right management software to run it fills the security gaps represented by traditional deployments.

Modern design incorporates networking solutions that provide the flexibility, agility, and resiliency required to effectively deliver the value and user experience demanded in current work environments. The most effective solutions have the hardware and software components to help you solve the challenges of today, support evolution over time, and deliver the value of connecting everyone, everywhere, securely, all the time.

How Extreme Networks Solutions Helps Close the IT Security Gap to Reduce Risk and Simplify Operations

Extreme Networks equipment and software has always been designed with built-in security capabilities, enabling layers of security across wired, wireless, SD-WAN, and the cloud.

Our vision of transforming the Infinite Enterprise with One Network, One Cloud, One Extreme is grounded in the idea that security is foundational and must be viewed, (like everything in the network design), through a customer experience lens rather than as trade-offs in scalability or agility.

A security mindset is applied to every offer from Extreme Networks.

Security capabilities are unified across our products through a layered approach that is simple and scalable.

This is one of the reasons Extreme is recognized by Gartner as a leader in wired and wireless infrastructure for the fifth consecutive year. A part of this criteria examines a solution provider's ability to provide security across all of the infrastructure components and the software capabilities used to manage, analyze, and protect them.

Our strategy incorporates a multi-layer approach to applying security to protect the path of packets through the network. We deliver the critical capabilities you expect from a network equipment provider and continue to invest in new security capabilities that not only fill the IT security gaps of today but can meet the needs of our customers as they continue on their security journey.

"The question was how could we refresh our networking gear, achieve a better total cost of ownership, and enhance network operations and security all at the same time? That's how we ended up with Extreme"

– Colin Summers,
Director of Network Services for OSF HealthCare

Secure the Air and Wireless

Wireless is the preferred way to access data and applications whether working at a large campus a small branch or remote. Extreme's wireless portfolio has many security features that protect access over the air to reduce the risk of threats without diminishing user experience.

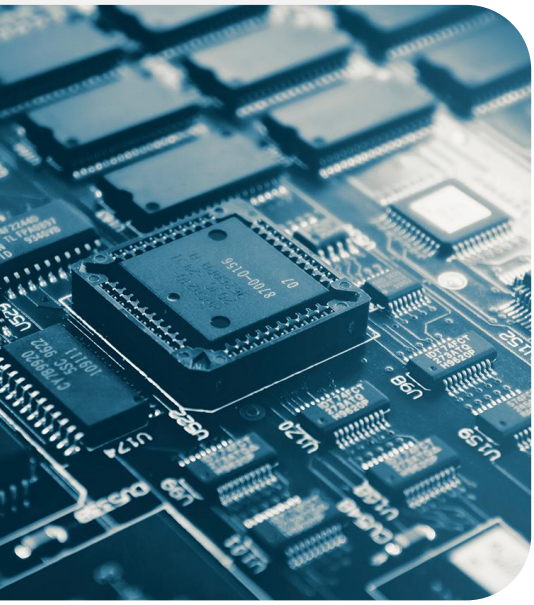
Wireless Security Classification and Monitoring

Extreme AirDefense is the industry-leading capability that protects your wireless LAN by accurately detecting and mitigating wireless vulnerabilities and unusual network activity, like attempted denial-of-service (DoS) attacks.

AirDefense security and compliance functions work seamlessly across your wireless network to detect and neutralize rogue devices, enforce policies, prevent intrusion, and ensure regulatory compliance. Automated tools for threat mitigation and policy enforcement give you the confidence of real-time response to risks and the peace of mind of having an effective security posture.

AirDefense includes:

- ✓ 24x7x365 WLAN network monitoring for protection against wireless attacks
- ✓ Industry-leading threat detection library with over 300 catalogued threats
- ✓ Real-time detection of rogue devices with automatic rogue termination for rapid response to attacks, protecting your network until the device can be physically removed
- ✓ Policy enforcement with instant notification and response based on policy violations
- ✓ Wireless Vulnerability Assessment to remotely test for vulnerabilities from the perspective of a wireless hacker



Secure hardware

Embedded Trusted Platform Module (TPM) chip technology built into the device prevents device tampering and provides a layer of security against threats like firmware and ransomware.

Unlike other products, Extreme access points include a full Layer 2-7 firewall that protects against DoS attacks against MAC and IP layer. A stateful firewall provides Layer 3-7 protection with deep packet inspection and a bi-directional flow-based engine.

Extreme access points operating as sensors support 802.11a/b/g/n/ac/ax standards to scan multiple bands and are capable of listening to multiple MIMO streams.

Robust Network Segmentation and Policy Enforcement at Every Point in the Network

Network Fabric

Fabrics are often employed to simplify deployment and operations. However, the right fabric solution can also significantly boost security by supporting uniform policy enforcement and segmentation. Extreme Fabric Connect is highly scalable and can extend across multiple locations from the remote branch to the data center and connects different device types using IEEE-standard protocols. Extreme automatically includes fabric with all Universal and VSP switches making security inherent.

Key security features include:

Stealthy Design that prevents discovery of the network topology by eliminating the ability to scan the entire network. In the core, Ethernet switch paths keep IP addresses invisible to IP scanning attacks. The Fabric, virtual services and segments appear dark when scanned.

Provisioned only at the Edge, networkwide segments are automatically distributed throughout the network, eliminating error-prone and time-consuming manual configuration practices.

Hyper-segmentation which enables the creation of virtualized isolated segments where assets can be grouped by sensitivity and access can be controlled makes it more difficult for an attacker to move laterally through the network in search of valuable data limiting impact if attacker gets in.

Increased resiliency with ultra-fast failover capabilities that redirects traffic from failed devices to maintain high availability while minimizing threats.

Eliminate back door entry by automatically removing visibility of decommissioned devices from the network and eliminating access to anything associated to that device.

Granular Access Control

In addition to limiting user access, a network access control capability also blocks access from endpoint devices that do not comply with corporate security policies. This ensures that malware cannot enter the network from a device that originates from outside of the organization.

Network Access Control (NAC)

Extreme Control is our easy to deploy, granular device level control based on policies that can be easily scaled network wide. Along with complete logging of what, when and where devices are accessing the network, there are automated incident response capabilities based on business rules.

Key features include:

Enabled enforcement of consistent, highly secure access policies and the granular control of users and IoT devices for network onboarding from a single screen.

Protection of corporate data by proactive prevention of unauthorized users and compromised endpoints from gaining access to the network.

Enablement of secure BYOD, guest access and IoT access with rolling out of real-time policies based on the security posture of the device matching endpoints with attributes, (such as, user, time, location, vulnerability, or access type), to create an all-encompassing contextual identity.

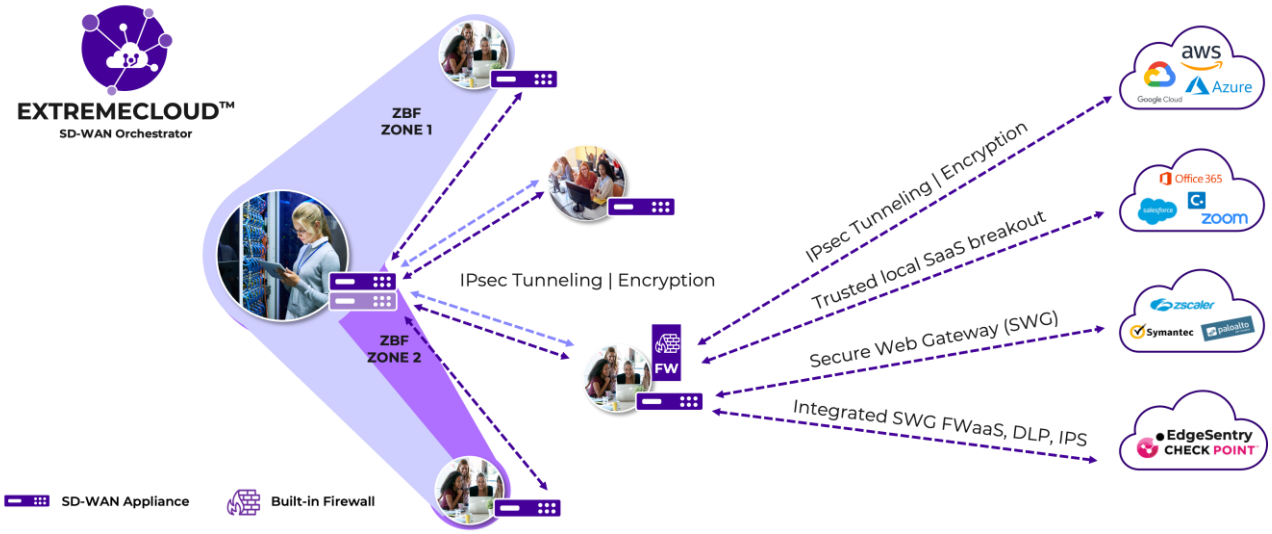
Role-based identities that follow a user, regardless of where or how they connect to the network.

Automated incident response which allows you to dictate actions for the system to take based on defined business rules.

Securing the WAN and Extensions to the Cloud

Digital transformation, employees who work fluidly between corporate offices, branches and home and the fact that companies are storing and using more data than ever in the cloud effects WAN architecture and security. Routing all IaaS and SaaS-bound traffic through an enterprise firewall at the data center permits centralized control but uses unnecessary bandwidth however local cloud breakout using the internet can lead to new security and compliance issues with increased management overhead.

Extreme's SD-WAN solution provides robust integrated WAN security and secure internet access to protect networks from threats emerging from the World Wide Web. It provides a secure, flexible solution that reduces complexity, while helping protect users, applications, and data from attackers.



ExtremeCloud™ SD-WAN has a comprehensive range of built-in security features and options that protect your traffic in transit, segment users, enforce business policy for cloud breakout, and secure your network from inbound internet threats.

Our standard service provides:

- **IPsec encrypted tunnels** Used to secure branch-to-branch, branch-to-data center, and branch-to-IaaS traffic. This means that all traffic travelling through the internet is encrypted and delivered through secure tunnels ensuring that the data comes from a trusted source and, reducing the chance of interference and eavesdropping by third parties.

- **Zone-based access and segmentation** Additional security features can be leveraged by segmenting traffic into zones that are application aware allowing for granular application of security policy. Applications can be assigned by zones and based on policy, and traffic is allowed directly via the Internet, denied or sent through an integrated secure web gateway (SWG) or backhauled to a data center firewall for further inspection.

EdgeSentry, powered by Check Point, is a fully integrated advanced WAN security solution provides additional essential capabilities for connecting SD-WAN-enabled branches to the web in a secure and controlled manner. EdgeSentry combines SWG, firewall as a service (FWaaS) and a cloud access security broker (CASB) to protect users from malicious web traffic, vulnerable websites, viruses, malware, and other cyber threats.

EdgeSentry

Unified Management in the Cloud

The ExtremeCloud platform is architected for security and resiliency. Why do we offer cloud-enabled management tools?

- ✓ Operating from the cloud provides redundancy and resiliency at a much lower cost and higher reliability than many competitive and traditional on-site offerings.

  For example, the Extreme Networks cloud uses 21 global PoPs across the big three IaaS providers, whereas most others rely on as few as three and sometimes from a single vendor. Additional resiliency and redundancy come from our multi-vendor strategy that ensures uptime and the best speed possible, so our customers can be confident of our reliability.

- ✓ Cloud-enabled management tools benefit from the shared experience of all our customers. Anonymized data from each company operating in the cloud allows us to see opportunities to apply zero-touch improvements for continuously enhanced service delivery, ensuring an improved experience for all customers.

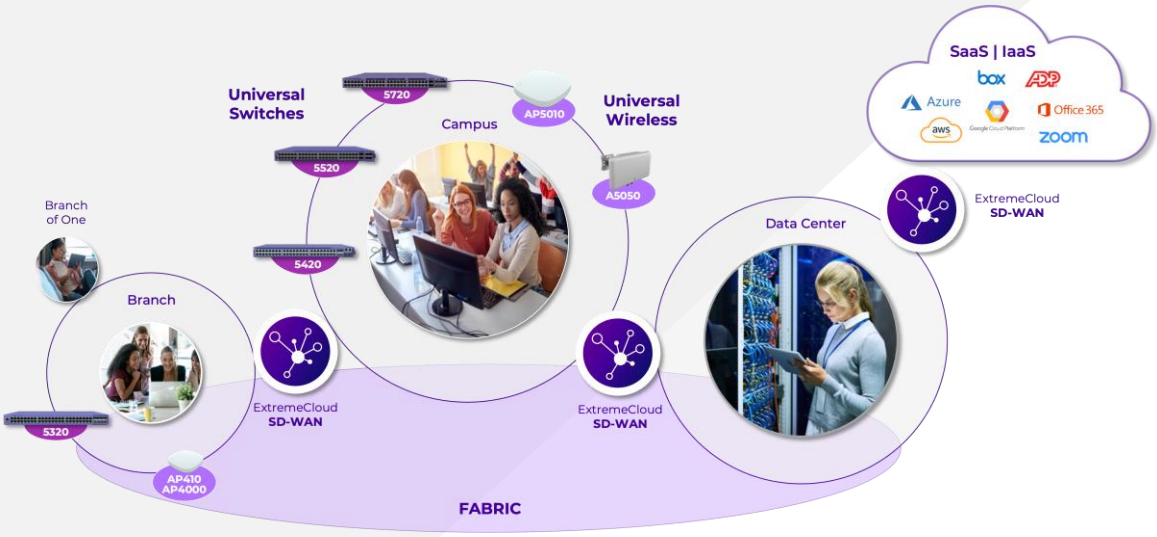
In addition to resiliency, we want our customers to be confident that our cloud is secure so that their data and the networks managed in our cloud are secure. We've done the work and undergone the scrutiny required to prove our commitment to reducing the likelihood of data breaches.

Extreme Networks is the first major cloud-managed networking vendor recognized by the global standard for commitment to information security management systems best practices and controls.

In addition to the protections offered by hosting providers AWS, Google, and Microsoft Azure, Extreme goes above and beyond the cloud facility certifications to ensure data privacy and protection by:

- Adopting and implementing the ISO 27001 family of certifications for best practices in global information security management (includes ISO 27017 & ISO 27701)

- Obtaining global certifications in:
  - ✓ SOC2 compliance
  - ✓ CSA certifications,
  - ✓ GDPR compliance



Connecting Everyone, Everywhere, Securely All the Time

We're driven to improve our customers' businesses, and connectivity is just the foundation. We make the network a strategic asset. We help identify and solve business challenges. We simplify and improve the way you work and are relentlessly focused on finding new ways to drive better outcomes.

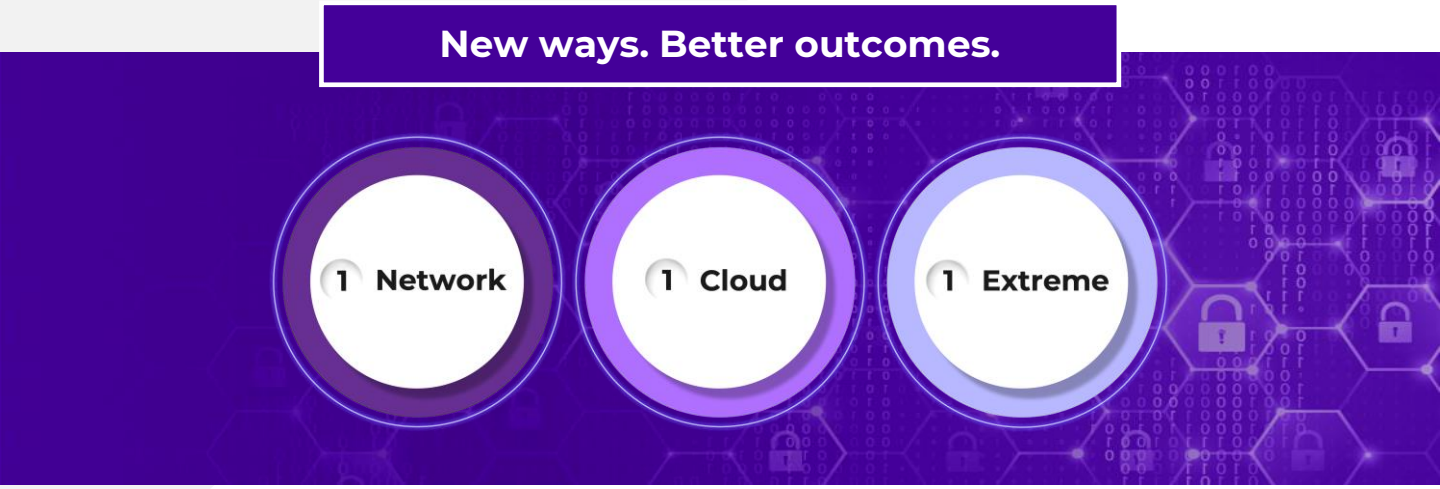
At Extreme, our mission is to create new ways and better outcomes for our customers.

We've created a vision for meeting today's challenges by enabling transformation to what we call the Infinite Enterprise. This is characterized by infinite distribution of your users, your sites, your environment: infinite connectivity. Companies need to scale operationally and from a network and technology level. This requires agile delivery of consumer-centric experiences that are demanded by IT teams and end users. This is the end state.

To get to that state, we've developed a strategy and architecture that we call One Network, One Cloud, One Extreme. Think of the network operating as a singular topology. There are no longer borders between a data center, a campus, and a branch; all of these environments work seamlessly across wired, wireless, and SD-WAN, as well as network fabric capabilities.

All of this is managed by a singular cloud, both on the front end in terms of driving these various capabilities across the network as well as unified from a back-end perspective.

Securing the Infinite Enterprise requires security at all pivotal points in the network. Every endpoint is part of your network and therefore part of your security solution. Why treat your network equipment and access security systems as separate solutions? Instead, they should be fully integrated so that you can be confident your network is secure.



[1] 2022 Global study on Closing the IT Security Gaps, Ponemon Institute
[2] Cisco Annual Internet Report, 2020 and IoT trends to keep an eye on in 2023 and beyond. TechTarget,Jan 19 2023
[3] "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023" Gartner October 31 2022.
https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

Extreme networks