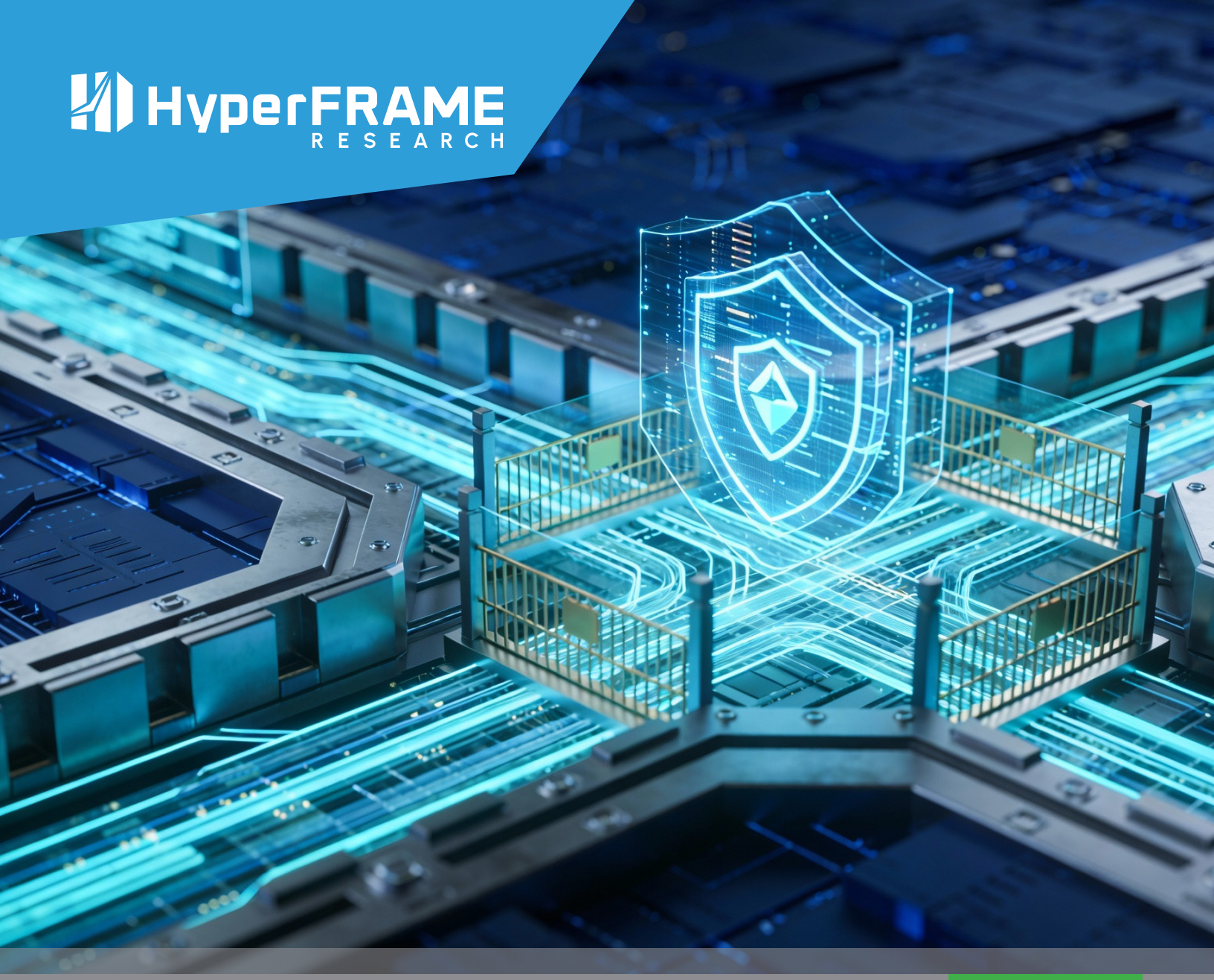
HyperFRAME RESEARCH



RESEARCH BRIEF

Zero Trust Security Made Simple: The Extreme Platform ONE™ Advantage

Unifying Security and Connectivity with an Autonomous Security Overlay for Simplified Operations and Maximum Protection

Authors:

Ron Westfall
VP and Practice Leader for Infrastructure and Networking

Steven Dickens
CEO and Principal Analyst

FEBRUARY 2026

Overview – Today's Top Network Security Challenges

Topmost network security risks consist of increasingly sophisticated threats, the expansion of the attack surface, and the complexity of managing defenses

The modern threat landscape is defined by the rapid evolution of AI-driven tactics, which have weaponized automation to launch attacks at an unprecedented scale. Adversaries are now using adaptive malware and hyper-realistic deepfakes to bypass traditional social engineering defenses, significantly boosting the success rates of ransomware and double-extortion campaigns. This surge in technical sophistication coincides with dissolving network boundaries, as the shift toward hybrid work, cloud-based infrastructure, and unmanaged IoT devices has effectively erased the traditional perimeter. These expanded environments can introduce a multitude of misconfigured entry points and heighten the risk of north-south and east-west compromise from vulnerable supply chains.

Compounding these external threats is the internal crisis of security tool sprawl, where an over-reliance on disconnected, siloed solutions has created an unsustainable burden for understaffed IT teams. This fragmentation leads to a critical lack of centralized visibility, making it nearly impossible to maintain a consistent security posture across the enterprise. Consequently, the resulting complexity often leads to security misconfigurations - now the primary catalyst for cloud-based data breaches - as personnel struggle to manage a cluttered defensive stack rather than focusing on proactive threat hunting and strategic risk mitigation.

As a result, innovative network security solutions are now essential because they replace fragmented, siloed tools with centralized visibility, enabling understaffed teams to eliminate the misconfigurations that currently drive cloud breaches. By leveraging advanced automation, these modern frameworks can effectively counter the scale of AI-driven threats and protect the dissolved network perimeter where traditional defenses no longer apply.

Why Innovative Network Security Solutions are Essential

Outsmarting the Automated Threat: Real-Time Intelligence for an AI-Driven World

The rapid evolution of AI-driven tactics has rendered traditional security measures insufficient, as adversaries now use automated, adaptive malware and sophisticated multi-extortion techniques to launch attacks at an unprecedented scale. To counter this, innovative network security solutions must leverage high-speed analytics and AI-driven measures to detect behavioral anomalies in real time. By shifting from reactive to proactive defense, organizations can neutralize high-volume threats before they breach the inner layers of the corporate environment.

To address these evolving risks, modern security frameworks must use real-time behavioral modeling and high-speed data processing to identify and neutralize atypical network activity the moment it occurs. By shifting from reactive to proactive defense, organizations can neutralize high-volume threats before they breach the inner layers of the corporate environment.

As the traditional network perimeter dissolves into a complex ecosystem of cloud services, remote workers, and unmanaged IoT devices, the attack surface has expanded beyond the reach of legacy firewalls. Modern security frameworks address this vulnerability by implementing identity-based security and Zero Trust architectures that verify every connection regardless of its origin. This approach ensures that as network boundaries continue to shift, security remains consistent across all north-south and east-west traffic, effectively securing entry points that were previously left exposed.

Innovation is critical to solving the internal crisis of security tool sprawl, which often leaves understaffed IT teams overwhelmed by disconnected alerts and siloed data. By consolidating these fragmented tools into unified platforms, organizations can achieve centralized visibility and automate policy enforcement across the entire enterprise. This simplification not only bridges the cybersecurity skills gap but also significantly reduces the risk of human error and misconfigurations, which are currently the primary catalysts for cloud-based data breaches.

Zero Trust Security

Identity Verification
Confirm User Identity

Device Verification
Ensure Device Security

Least Privilege Access
Limit Resource Access

Prioritize natively integrating security into the network fabric itself, simplifying management while enforcing a Zero Trust model

Extreme Networks sharpens and advances its cloud strategy by merging Network Access Control (NAC) and Zero Trust Network Access (ZTNA) into a unified, identity-driven policy engine to form a modern security foundation. By integrating these once-separate functions, organizations can automate security protocols for every user and device across the entire ecosystem. Whether a user is connected to corporate headquarters, a small branch office, or a remote home setup, this unified approach ensures that access is consistently verified and enforced based on identity rather than location. The network's autonomous partitioning and dynamic policy alignment ensure that rigorous security standards are uniformly maintained, even as the infrastructure scales or adapts to new requirements.

To create a truly resilient environment, security must be woven directly into the network fabric itself rather than added as an afterthought. Leveraging Extreme Fabric enables the implementation of automated micro-segmentation, effectively building a self-defending network. This architecture isolates potential threats and protects critical resources by automatically compartmentalizing traffic. This not only bolsters the organization's defense posture but also streamlines the deployment of new, secure services across the infrastructure without the usual manual overhead.

Extreme Networks sets itself apart by leveraging Fabric Attach to automate device onboarding, directly linking this capability to a unified Zero Trust and NAC identity engine for agile security integration. By weaving these automation features into the core infrastructure, the platform creates a self-defending fabric that ensures every newly connected device is instantly secured and compartmentalized without manual intervention.

Efficiency and risk reduction are further enhanced by integrating security and networking through a centralized cloud management platform, such as Extreme Platform ONE. By using AI and advanced automation, the network can consistently enforce policies and eliminate the fragmentation caused by siloed security tools. This centralized orchestration removes the complexity of managing disparate systems, which in turn drastically reduces the risk of human error - one of the leading causes of security vulnerabilities in modern enterprises.

Moreover, Extreme Platform ONE reduces Total Cost of Ownership (TCO) by consolidating wired, wireless, and security management into a single cloud-based dashboard, eliminating the high costs associated with maintaining fragmented, siloed tools. The platform's automated fabric architecture can significantly lower operational expenses by reducing manual workloads and preventing costly data breaches caused by human-driven misconfigurations. Its future-ready design provides long-term value by easily adapting to hybrid work and IoT expansion without requiring expensive, large-scale infrastructure overhauls.

Extreme Networks Meets the Topmost Network Security Demands

Delivering proof points in its network security strategy by demonstrating simplification, accelerated Zero Trust adoption, and measurable protection across diverse environments

Extreme Networks is pacesetting the transition to modern security by collapsing the deployment timeline for Zero Trust from weeks down to just a few hours. This is achieved through a unified, cloud-managed policy engine that integrates NAC and ZTNA into a single identity-based system. By merging these traditionally separate functions, organizations can rapidly establish a consistent security posture across both local and remote environments without the typical complexity of a staged rollout.

The platform's Secure Network Fabric provides a verifiable defense-in-depth strategy, using micro-segmentation to isolate network traffic and containing potential breaches. Independent penetration testing has confirmed that this fabric-based approach fundamentally changes the defensive landscape, effectively blocking the east-west lateral movement that attackers rely on to escalate a compromise. This ensures that even if one device is breached, the threat is localized and prevented from spreading to critical business assets.

The integration of these security functions into the AI-driven Extreme Platform ONE simplifies daily operations and reduces the burden on overstretched IT teams. By automating policy enforcement and routine security tasks, the platform minimizes the risk of human error, one of the leading causes of modern data breaches.

This technical excellence and market impact have been validated by multiple industry accolades, including the BIG Innovation and Globee Awards, cementing its reputation as clearly distinguished among the industry's most complete and streamlined identity-based access solution.

Key Use Cases: Digital Learning, Manufacturing, Healthcare

Delivering simple, secure connectivity and Zero Trust assurances across diverse networks and industry use cases through its foundational platform and unified policy model

Extreme Networks delivers a unified, identity-based security architecture that ensures consistent Zero Trust protection and regulatory compliance across diverse environments, from digital classrooms to mission-critical manufacturing floors. By consolidating management into a single cloud-based platform, organizations can automate complex tasks and utilize fabric micro-segmentation to eliminate lateral threats while significantly reducing operational overhead.

Whether using the on-premises capabilities of ExtremeControl or the cloud-native Extreme Platform ONE Security, organizations can achieve highly granular control by synchronizing with key Identity and Access Management (IAM) providers such as Microsoft Entra ID, Okta, and Google Workspace. By further integrating with Mobile Device Management (MDM) tools such as Microsoft Intune, the platform can enforce policies based on real-time device health and identity, ensuring that only compliant, authorized users gain access. As a result, users gain use case agility and integration ease:

Use Case Integration

1. Device connects to network via Extreme NAC
2. NAC queries Entra ID for authentication and/or group attributes (user cert, group-based policies).
3. Extreme NAC applies access policy (permit, quarantine, VLAN tag) based on both identity and compliance posture.
4. Entra ID manages the identity lifecycle, group membership, and federated authentication - all feeding into NAC.

Here are the key use cases that we see Extreme Networks fulfilling:

- **Healthcare (Automated Policy Enforcement):** By integrating either the on-premises ExtremeControl or the cloud-native Extreme Platform ONE Security with identity providers like Microsoft Entra ID and MDMs like Intune, organizations can automate complex security decisions at the moment of connection. For instance, if a healthcare professional connects an unmanaged tablet to a hospital network, the NAC instantly detects the lack of compliance and uses Fabric Attach to automatically isolate the device into a restricted guest segment. This unified approach ensures that regardless of whether the management plane is local or in the cloud, security policies remain consistent, identity-driven, and enforced in real-time without manual IT intervention.
- **Digital Learning (Campus & Remote):** To support the demands of modern digital learning, a unified policy engine delivers Universal ZTNA and Cloud NAC across the entire educational ecosystem. This ensures that students, faculty, and guests receive consistent, identity-based access regardless of whether they are on the campus LAN or connecting remotely. By enforcing least privilege principles, the network effectively safeguards sensitive data and maintains compliance with FERPA regulations, all while providing the high-performance Wi-Fi 6/6E/7 and scalable switching necessary for uninterrupted classroom experience.
- **Manufacturing (IT/OT Convergence):** In complex manufacturing environments, the convergence of IT and OT requires a sophisticated approach to isolation and uptime. A secure network fabric automatically segments the infrastructure from the corporate office to the factory floor, enforcing Zero Trust policies that keep mission-critical robotics and sensors separate from the general IT network. With Extreme Fabric Attach, edge devices such as controllers, sensors, and PLCs can automatically inherit the correct VLAN and security policies the moment they connect, eliminating manual provisioning and reducing configuration errors. This dynamic, identity-based onboarding extends micro-segmentation all the way to the device edge, preventing threats from moving laterally across the organization and ensuring that a breach in one area does not compromise the productivity or safety of the production line
- **Simplified and Centralized Management:** Operational efficiency is achieved through Extreme Platform ONE, which consolidates the management of wired, wireless, and security protocols into a single cloud-based dashboard. This centralized approach drastically reduces the complexity of overseeing multi-site networks, from remote warehouses to corporate headquarters. By eliminating siloed management tools, IT teams can automate routine manual tasks, allowing them to focus on scaling the infrastructure to meet future technological needs rather than getting bogged down in day-to-day maintenance.
- **End-to-End Resilience and Automation:** The strategy focuses on end-to-end resilience, utilizing a Zero Touch, Zero Trust Fabric that extends across the LAN, campus, and SD-WAN edge. This architecture leverages advanced tools such as WIPS and SD-WAN to optimize application performance and proactively mitigate risks. Through automated services and robust macro/micro-segmentation, the network allows for the rapid, secure deployment of new devices, maintaining a resilient security posture that protects the organization from the edge to the core.

Comparison of Traditional vs. Unified Security Architectures

Feature	Traditional NAC & ZTNA (Siloed)	Extreme Networks Unified Approach
Deployment Speed	Weeks or months of configuration and integration.	**Hours** via a cloud-managed, identity-based engine.
Policy Management	Separate policies for on-site (NAC) and remote (ZTNA) users.	**Single cohesive policy engine** for all access, regardless of location.
Lateral Movement	Limited isolation often relies on complex VLANs.	**Fabric Micro-segmentation** inherently prevents east-west movement.
Operational Effort	High manual overhead; prone to tool sprawl and “alert fatigue.”	**AI-driven automation** reduces manual tasks and human error.
Visibility	Fragmented views across different dashboards.	**Unified visibility** through Extreme Platform ONE.

Recommendations for Network Security Decision Makers

- **Consolidate Siloed Defenses into a Unified Identity Engine:** To eliminate the configuration errors and management gaps inherent in disconnected tools, evaluators need to prioritize platforms that merge NAC and ZTNA into a single, cloud-managed policy engine that secures users consistently across campus, branch, and remote environments.
- **Adopt Fabric-Based Micro-segmentation for Verifiable Defense:** Decision makers should shift away from complex, manual VLAN-based isolation and instead implement a self-defending network fabric that automatically compartmentalizes traffic to block east-west lateral movement and contain potential breaches.
- **Prioritize AI-Driven Automation to Overcome Resource Constraints:** To combat the scale of automated, AI-driven threats and the internal crisis of tool sprawl, key decision markers, such as CTOs and CISOs, should select solutions that use native agentic AI and centralized orchestration to automate routine security tasks and reduce the operational burden on IT teams.

Key Takeaways & Conclusion

Extreme Networks delivers competitively advantageous network security portfolio and execution of portfolio-wide strategy

Extreme's competitive edge lies in the native convergence of Zero Trust security and access control directly within the network fabric and cloud management layers. By embedding security into the infrastructure itself, organizations can avoid integration failures and the high complexity typically associated with stitching together disjointed third-party products. With Extreme Fabric Attach, devices at the edge automatically inherit the correct segmentation and access policies the moment they connect, eliminating manual provisioning and ensuring consistent enforcement. This unified architecture helps ensure that least-privilege access is applied across every environment, from the campus and branch to the factory floor and remote worker, effectively isolating breaches through automated micro-segmentation and protecting critical systems like OT infrastructure.

Beyond technical robustness, this approach delivers operational simplicity and a lower TCO by consolidating management under Extreme Platform ONE. The automated, open fabric architecture can reduce the burden on IT staff and minimize the risk of human-driven misconfigurations, which remain a leading cause of data breaches. This future-ready design is inherently adaptable to the demands of hybrid work and the proliferation of IoT devices, positioning Extreme Networks as the strategic partner for secure, long-term digital transformation.

ABOUT HYPERFRAME RESEARCH:

HyperFRAME Research delivers in-depth research and insights across the global technology landscape, spanning everything from hyperscale public cloud to the mainframe and everything in between. We offer strategic advisory services, custom research reports, tailored consulting engagements, digital events, go to market planning, message testing, and lead generation programs.

Our industry analysts specialize in rigorous qualitative and quantitative assessments of technology solutions, business challenges, market forces, and end user demands across industry sectors. HyperFRAME Research collaborates closely with your Analyst Relations, Product, and Marketing teams to build and amplify your thought leadership, positioning your expertise to enhance brand and product recognition. Through content that engages readers, viewers, and listeners alike, we ensure your voice resonates across channels.

CONTACT HYPERFRAME RESEARCH:

Steven Dickens
CEO & Principal Analyst | HyperFRAME Research

Email Address:

steven.dickens@hyperframeresearch.com

Telephone Number:

+1 845 505 1678

X: @StevenDickens3

LinkedIn: Steven Dickens

BlueSky: Steven Dickens

CONTRIBUTORS

Ron Westfall
VP and Practice Leader for
Infrastructure and Networking

Steven Dickens
CEO and Principal Analyst

INQUIRIES

Contact us if you would like to discuss this report and HyperFRAME Research will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "HyperFRAME Research." Non-press and non-analysts must receive prior written permission by HyperFRAME Research for any citations.

LICENSING

DISCLOSURES

HyperFRAME Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.


HyperFRAME
RESEARCH