EXTRAHOP

From the C-Suite to the SOC:

How Consolidating Network Security Solutions Transforms the Enterprise

Table of Contents

A Growing Call for Consolidation

Network security threats have become increasingly complex. Modern adversaries have moved on from using easily recognized forms of malware to achieve their goals. They're now weaponizing advanced tactics, like EDR killers, to circumvent and undermine traditional security controls. Such activity is leading to catastrophic data breaches, significant financial losses, reputational damage, and operational disruptions for organizations around the world.

In response to escalating threats like these, enterprises have adopted a wide array of specialized tools to monitor network traffic, identify suspicious activities, and initiate threat responses. According to a survey by 451 Research, the average IT and security team uses between 10 and 30 tools just to monitor applications, network infrastructure, and cloud environments.[1]

This fragmented approach, while born from a desire for comprehensive protection, often gives the illusion of security. The reality is that simply adding more tools doesn't equate to stronger defenses. It's time to explore how strategic consolidation can genuinely deliver superior security, efficiency, and business resilience.

Together, we'll uncover how a consolidated network security strategy offers transformative advantages throughout your organization—whether you're a CISO aiming for stronger defenses within a set budget, a CFO focused on optimizing organizational spend, or a Head of SecOps dedicated to driving efficiency.

1. **Is Your Organization Suffering from Security Tool Sprawl?,** Dark Reading, September 27th, 2019

Security

Comprehensive Visibility

Ironically, the sheer number of specialized security tools that organizations have implemented often leads to fragmented visibility, rather than comprehensive insight. Individually, these tools collect important data and insights, but the disparate nature of these tools creates critical gaps, leaving security teams without a cohesive, real-time view of the network.

Instead of fragmented views, unifying capabilities like network detection and response (NDR), network performance monitoring (NPM), intrusion detection systems (IDS), and forensics empower your security team with unprecedented clarity.

A consolidated solution provides a complete view of your attack surface within one dashboard. You can effortlessly track sophisticated lateral threats—from on-premises servers, to cloud workloads, or compromised remote devices, to internal resources—while seeing all network activity, alerts, and health in a single pane of glass. This automatic correlation equips your team to detect and respond to a wide variety of attacks, including those that leverage environmental transitions, ensuring comprehensive coverage.

Unify all your network insights with an all-in-one platform that delivers 360-degree network visibility, unparalleled context, and complete control over the attack surface.

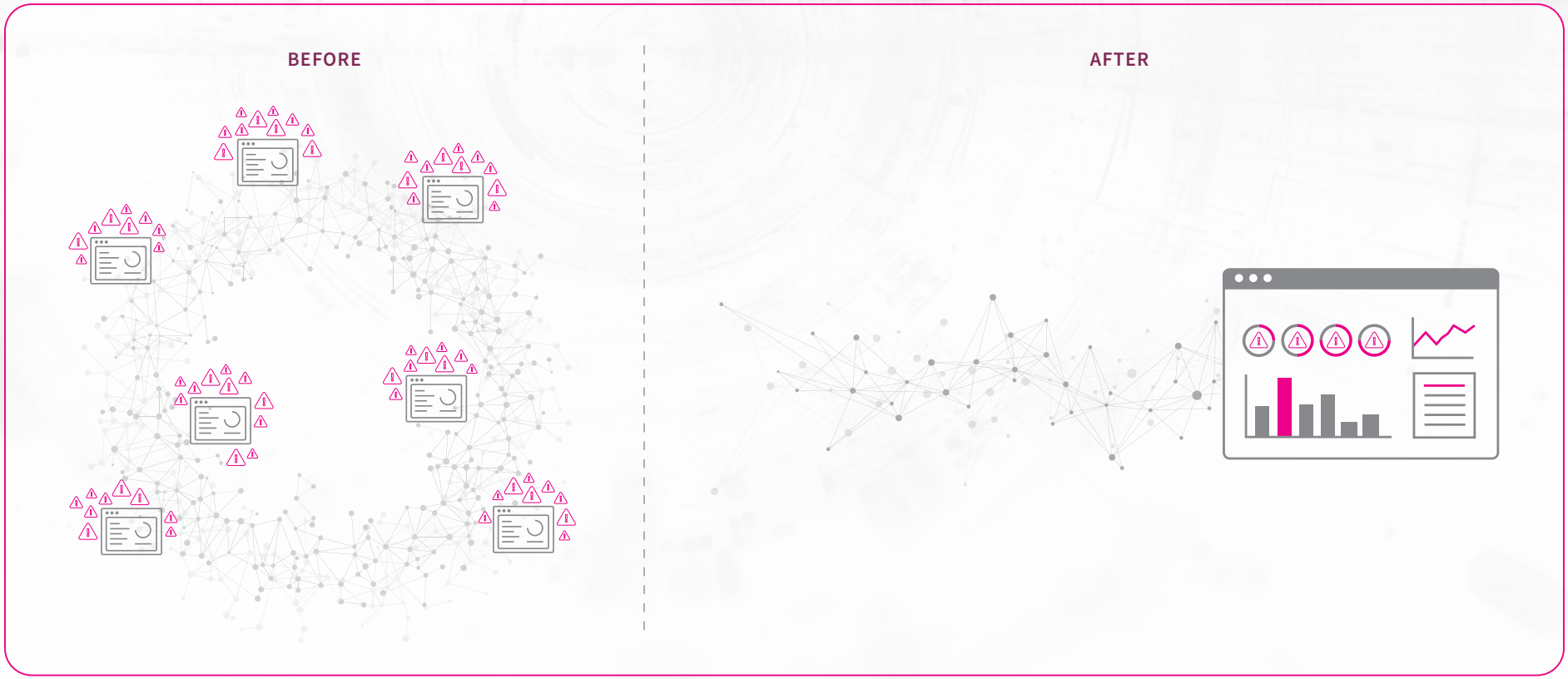
LEARN MORE
about modern network detection and response (NDR)

Less Noise, More Insight

The average security operations center (SOC) is under siege, fielding upwards of 4,484 alerts per day.[2] The sheer overload of security alerts, many of them false positives, leads directly to analyst fatigue. This makes it hard to identify real threats quickly. When true alerts go unnoticed or unaddressed for too long, attackers have more time to cause damage, seriously compromising an organization's security posture.

This burden is exacerbated by the fact that these alerts are coming from multiple, disparate security tools. Each tool operates independently, with its own logging format and alert criteria, which just creates even more work.

With one platform, SOCs don't have to expend time and energy sifting through a torrent of disorganized data. A consolidated solution intelligently correlates and contextualizes events across these otherwise disparate data sources.



2. **Cybersecurity Incident Correlation in the Unified Security Operations Platform**, Microsoft Defender XDR Blog, August 8th, 2024

Faster Threat Detection

Speed matters. The average time it takes for a cyberattack to escalate and spread through a system has plummeted to just 48 minutes. Even more concerning, the fastest observed breakout time is a mere 51 seconds.[3] For every moment a threat goes undetected, the risk of escalation grows, turning isolated incidents into costly, enterprise-wide compromises that jeopardize data, systems, and business partnerships.

A consolidated platform, however, can accelerate threat detection and investigation. Instead of analysts manually sifting through disparate logs and alerts, the platform integrates everything, automatically pulling together and making sense of critical alerts from across your entire infrastructure.

This gives analysts a holistic and immediate understanding of the full attack narrative as it unfolds. They can see the connections between seemingly isolated events, which means they can quickly understand the scope and severity of a threat. By bringing all these insights together in one place, organizations can significantly shorten the time between an initial alert and confirming a true threat, allowing for much faster response and mitigation.

48 Minutes
average breakout time

51 Seconds
fastest breakout time

> **“Most organizations deploy a patchwork of legacy tools that create a fragmented view of the network and add unnecessary complexity, leading to critical delays in threat detection, investigation and response.”**
>
> **Kanaiya Vasani**
> Chief Product Officer
> ExtraHop

3. **CrowdStrike 2025 Global Threat Report**, CrowdStrike, 2025

Management and Operations

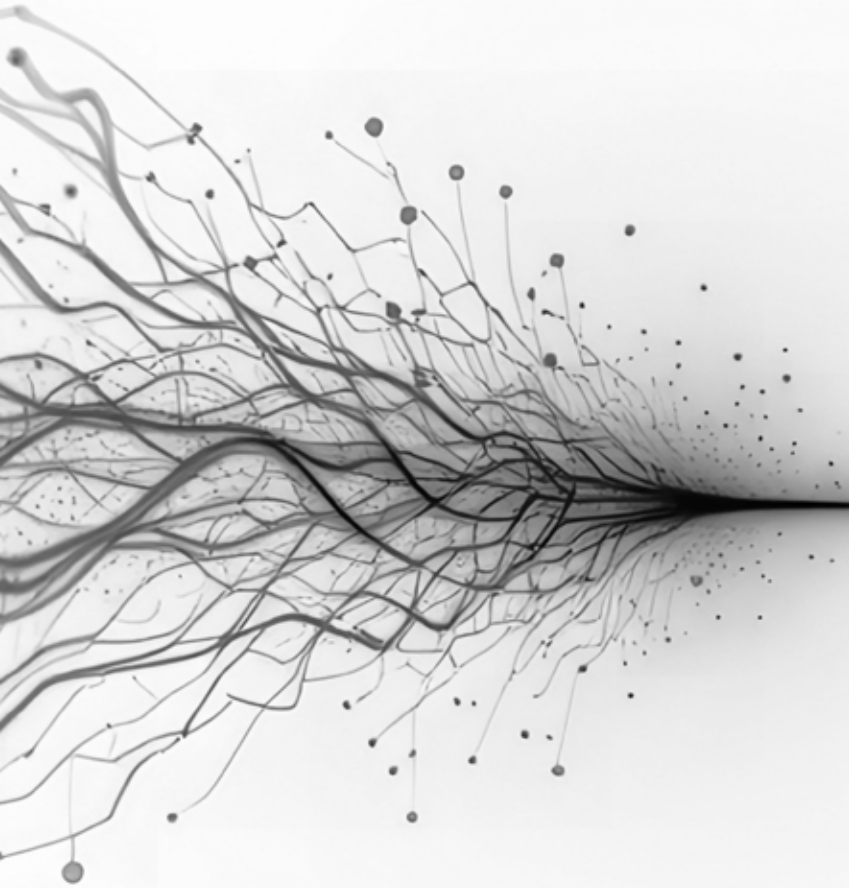
Increased Productivity

SOCs that are contending with multiple, disparate tools often have what can only be described as a "Frankenstack"—a patchwork of solutions that creates invisible operational debt, taxing analysts' time, attention, and focus.

When security teams operate with disparate tools, security personnel often need to log into each system, reformat information, and manually transfer insights between tools. The process is beyond inefficient; it pulls expertise away from actual threat detection and response. What's more, every time an analyst switches between these tools, they're not only navigating different workflows, but they're also engaging in cognitive switching. This mentally taxing process depletes energy and wastes precious time.

This is where a consolidated platform can transform productivity. The cohesive, unified view drastically reduces the time spent on basic activities, like data aggregation. According to IDC, analysts gain, on average, 20 percent more time through tool consolidation.[4] That time is immediately redirected from mundane tasks to pivotal analysis and response work.

4. North American Security Tools and Vendors Consolidation Study: Insights on Product Consolidation Plans, IDC, April 2024



SOC & NOC Alignment

Many organizations grapple with the following challenge: their SOC and network operations center (NOC) are making vital decisions based on fragmented tools and isolated data. This fractured approach leads to glaring inconsistencies—even of basic details like the number of actual devices or endpoints.

These discrepancies can lead to blind spots and inefficiencies, meaning security policies might not be applied everywhere, potential improvements are missed, and critical security gaps remain exposed, leaving the entire organization vulnerable.

Consolidated security means that the SOC and NOC teams can operate as a synchronized force against threats. In the event of a sudden network slowdown, both teams can work together using the same dashboard and data sources to determine if it's related to a network issue, or if it's related to a potential denial-of-service (DoS) attack. One cohesive solution means real-time collaboration, crystal-clear situational awareness, and the power to respond with unmatched agility.

Reduced Vendor Sprawl

The proliferation of cybersecurity tools, often referred to as vendor sprawl, has introduced an unintended layer of complexity to security operations. Vendor sprawl places an immense management burden on teams, often overstretching their capabilities.

Each new tool introduces its own unique interface, configuration demands, and relentless update cycles, forcing security professionals to become experts on every tool across the ecosystem. This becomes a significant drain on resources, requiring continuous, costly training that's increasingly difficult to maintain amid a persistent cybersecurity talent shortage.

A consolidated solution entirely eliminates the headaches associated with managing multiple vendor relationships. Instead of navigating separate vendor ecosystems, billing cycles, subscriptions, renewals, and update schedules, teams only need to engage with a single vendor. This dramatically simplifies procurement, streamlines technical support, and ensures a cohesive security architecture, allowing security teams to focus on strategic initiatives rather than administrative burdens.

Business

Cost Savings

The proliferation of security vendors inevitably translates to a complex web of financial burdens. More vendors mean more contracts, each laden with a cascading array of interconnected costs—from data volume fees to tiered support and integration fees.

A unified platform transforms the cost equation, and organizations are taking notice. Consolidating systems is proving to be a key strategy for achieving measurable cost savings and a stronger return on investment (ROI).

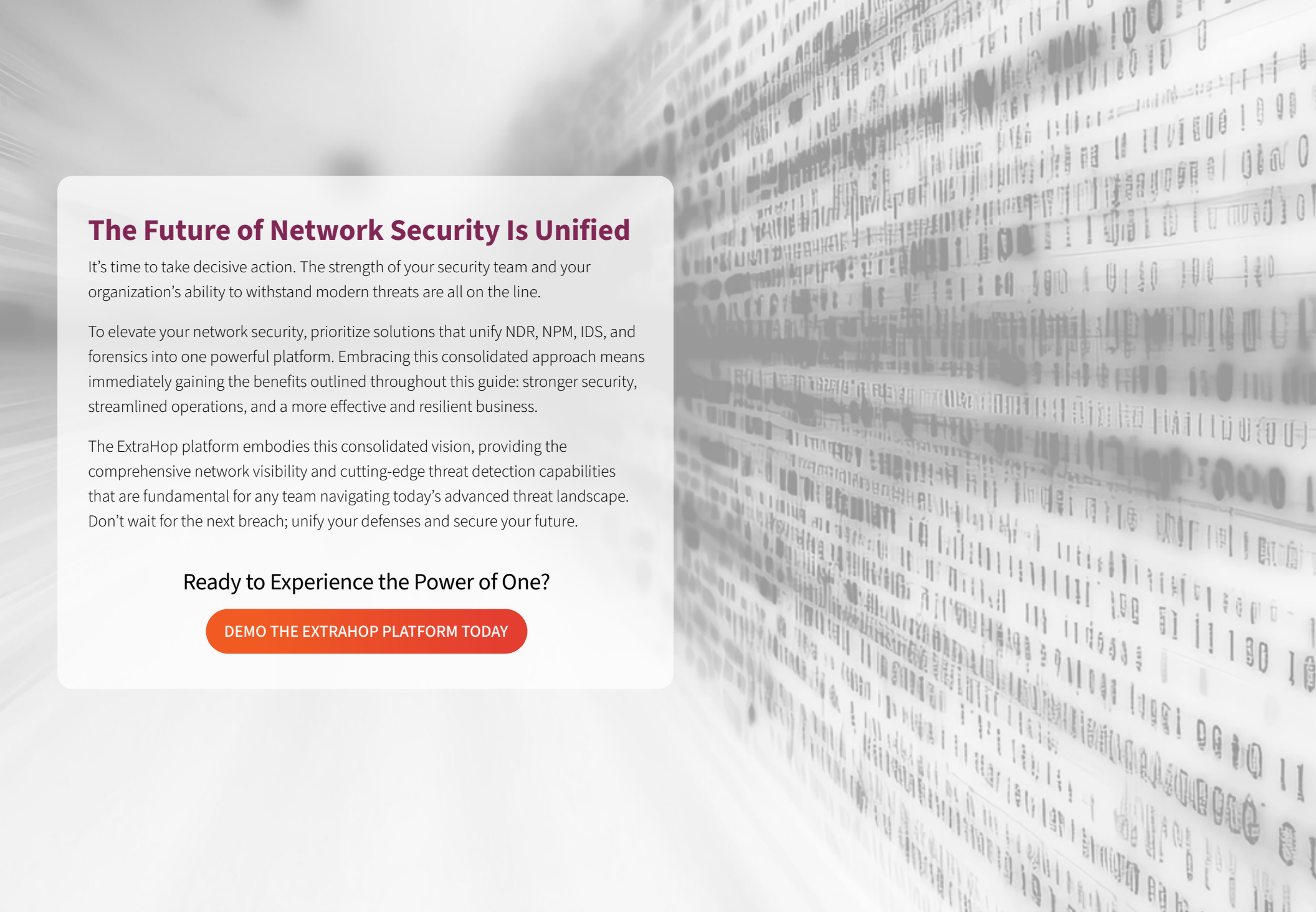
The most immediate financial gains stem from eliminating redundant licensing fees and excessive support contracts, as organizations often pay for overlapping functionalities or underutilized tools. Beyond this, consolidation significantly cuts down on other pervasive cost layers: reducing operational overhead from managing multiple vendors, lowering training expenses multiplied by each new platform, and minimizing costly integration complexities.

Compliance Simplified

Cybersecurity compliance audits often bring dread, especially in organizations with many vendors, where audits quickly become frantic searches across siloed tools.

Every tool requires its own audit trail, has its own reporting methodology, and reflects the vendor's own interpretation of regulatory requirements. The fragmentation creates compliance gaps that security regulators are quick to expose, potentially resulting in fines or legal consequences.

A unified security platform simplifies compliance. Whether it's showing compliance with HIPAA, PCI-DSS, ISO 27001, or another framework, a consolidated solution enables them to maintain a repeatable audit process. Instead of scrambling to gather disparate data from various systems, all necessary information is centralized and easily accessible. This not only reduces the time and effort spent on audits but also improves accuracy and consistency, helping to ensure continuous adherence to regulatory standards and mitigate the risk of non-compliance penalties.



The Future of Network Security Is Unified

It's time to take decisive action. The strength of your security team and your organization's ability to withstand modern threats are all on the line.

To elevate your network security, prioritize solutions that unify NDR, NPM, IDS, and forensics into one powerful platform. Embracing this consolidated approach means immediately gaining the benefits outlined throughout this guide: stronger security, streamlined operations, and a more effective and resilient business.

The ExtraHop platform embodies this consolidated vision, providing the comprehensive network visibility and cutting-edge threat detection capabilities that are fundamental for any team navigating today's advanced threat landscape. Don't wait for the next breach; unify your defenses and secure your future.

Ready to Experience the Power of One?

DEMO THE EXTRAHOP PLATFORM TODAY

About ExtraHop

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response.

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance management, intrusion detection, and forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®