eBook

The Power of Cybersecurity Consolidation

From greater visibility to more efficient security performance, organizations have a lot to gain by taking a platform approach.

Contents

INTRODUCTION

Confronting complexity

The expanding enterprise attack surface and increasingly diverse IT/data environment have pushed cybersecurity teams to deploy dozens of independent point solutions to combat specific threats and risks.

This trend has resulted in unmanageable complexity—a benefit for attackers and the enemy of efficient security management. Countless consoles, siloed data, and a constant flood of alerts all raise the risk of missed threats and incomplete responses that could lead to data loss, financial damages, or legal penalties.

To consolidate their disparate security environments, most organizations are seeing they need a platform-based approach with broad third-party integration capabilities to meet their business requirements for better security outcomes and value, bridge skills shortages, and assure compliance.

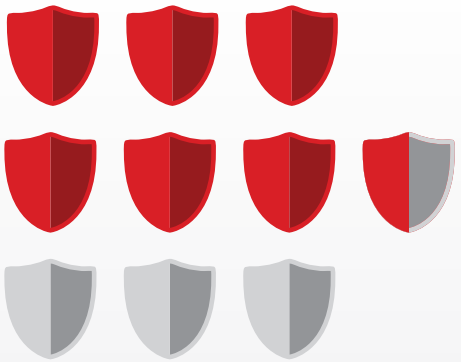
DRIVER

Stronger security outcomes

Alert overloads make it challenging for today's security operations centers (SOCs) to prioritize threats, while low visibility across security vectors, siloed data, and reporting with little context hamper their ability to make informed, risk-based decisions. Deprived of actionable insights into security performance, many struggle to know how best to strengthen overall security posture.

Consolidating tools and technologies into an integrated platform helps address these issues, bridging the gap between threat detection, response, and risk management by:

- Providing **centralized visibility** into more security vectors including endpoints, email, servers, cloud resources, the network environment, and more.
- Enabling **richer, more consistent reporting** to quantify risk across vectors and assets.
- Integrating **artificial intelligence and machine learning** (AI/ML) to identify patterns and anomalies, reduce false positives, accelerate response times, and enable more confident actions.
- Supporting **automation** to speed up time to cut through noise and mitigate threats sooner.



65%

of organizations pursuing or planning for consolidation expect to improve their overall risk posture.

Gartner

Top 5 Trends in Security Vendor Consolidation

DRIVER

Increase value and bring costs under control

Cybersecurity tool sprawl is inherently expensive. Maintaining and operating dozens of point solutions creates overlap and duplicate functionality while slowing down time to detection and devaluing security investments. This sprawl often results in 'shelfware'—safeguards that go unused despite spending on training, hosting, support, and maintenance.

For most organizations, getting more business value out of security is an even higher priority than cutting costs. A consolidated approach streamlines the security technology stack, improving SOC efficiency and helping optimize spending by:

Reducing the cost and complexity of procuring, licensing, and managing security products from multiple vendors, with greater access to training and volume discounts.

Maximizing the value of existing security investments through integration of third-party tools into a single central platform that relieves administrative burden and excess reporting.

Informing risk-based decision-making and unified management to improve security performance, justify spending, and provide better support to individual business units.

Enabling digital transformation projects by enabling adoption of new technologies with confidence in security because the overall environment is contextualized, visible, and better protected.

DRIVER

Bridge the skills gaps

The more security tools an organization has, the more full-time employees it needs to manage them. Yet cybersecurity, IT, cloud, and other technical fields face well-documented skills shortages. In cybersecurity, those shortages have reached crisis levels.

Staffing and upskilling challenges often result in burnout, churn, and underperformance. A platform approach makes it easier for organizations to do more with the personnel they have—and not overburden them—by:

- **Minimizing the need for expertise in specific toolsets**, since fewer tools are needed overall and the full environment is centrally visible and managed.
- **Putting time back in the hands of SOC team members** with automation, analytics, prioritization, and AI/ML insights that allow security staff to be focused and proactive instead of chasing false positives or getting mired in tedious, low-priority tasks. The platform acts as a single "brain" that spares analysts from having to piece insights together across multiple engines.
- **Incorporating generative AI** to accelerate mean-time-to-understanding, decode potentially malicious scripts, and expose stealthy threats—enabling junior analysts to contribute more while speeding up activities done by mid-level or senior team members.

54%

of surveyed organizations said addressing the skills gap was a top security challenge in 2023.

Trend Micro

Executive Insights: Top Cybersecurity Insights for CISOs

DRIVER

Comply with confidence

Complex, disconnected security environments make it hard for CISOs to tell their board directors and executives with any kind of certainty: "Yes, we're fully compliant." Yet that's increasingly what's expected of them, given the reputational, financial, and regulatory consequences of non-compliance.

An integrated platform puts high-quality and complete information into CISOs' hands so they can confirm performance and compliance by:

- Providing the **visibility, measurement, and reporting** to identify faster and more easily where the organization is compliant, where it isn't, and how to fix it where not.
- Eliminating guesswork from compliance assessment and allowing CISOs to **operate "faster than board speed"**—staying ahead of the curve, providing consultative recommendations, and avoiding unwanted surprises.
- Improving **communication and collaboration** among internal teams to ensure security practices and procedures are followed, raise awareness of risks earlier, and take collective action when needed.

48%

of organizations find ever-changing compliance standards to be their biggest cloud security obstacle.

Trend Micro

Executive Insights: Top Cybersecurity Insights for CISOs

Consolidation and integration go hand in hand

As attackers continue to become smarter and more insidious, and as the attack surface continues to grow, adopting a consolidated cybersecurity platform with third-party integrations is increasingly critical—the only way to maximize visibility and respond to threats effectively.

Enterprises have invested heavily in point security solutions. Most will want to preserve at least some of those legacy tools when they migrate to a consolidated platform, at least until they reach their end of life. And of course, no vendor can claim an all-in-one solution that covers every potential risk or threat.

That's why a security platform must support a diverse, multivendor toolset. APIs cease to be a chokepoint or trade secret and instead support the integration of as much third-party security technology and infrastructure as possible. That not only makes rich telemetry more available but also facilitates better remediation decisions.

Third-party integrations also make platform migration easier because they allow for an iterative process. CISOs can prioritize what to bring over first, make workflow changes gradually, and focus on quick wins.

Big benefits, quick wins

A platform approach can bring a range of nearly immediate benefits by consolidating the security environment:

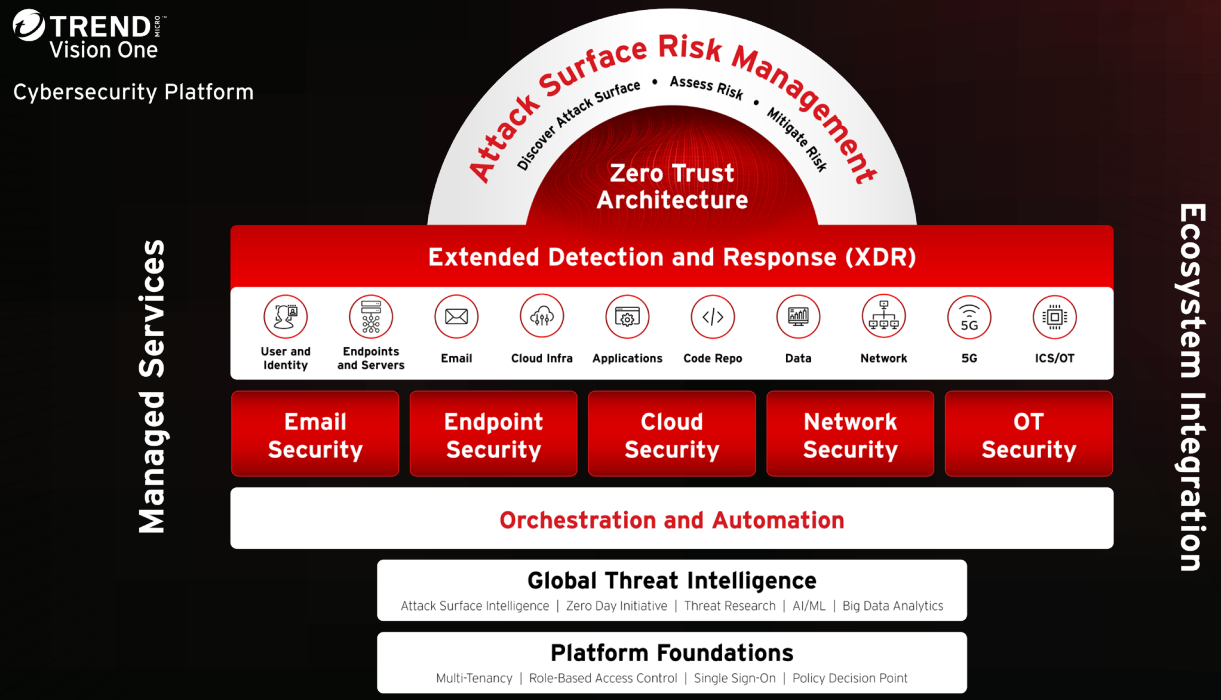
- **Improved visibility**
- **Fewer silos**
- **Faster detection and more complete response**
- **Improved reporting and communication**
- **Stronger collaboration**

PRODUCT

Trend Vision One™: A true cybersecurity platform

Trend Vision One delivers the full benefits of a platform approach to cybersecurity management, with comprehensive protection, prevention, detection, and response capabilities powered by AI and leading threat research and intelligence. It supports diverse hybrid IT environments, automates, and orchestrates workflows, and delivers expert cybersecurity services, so you can simplify and converge your security operations.

Learn more here



About the author

Trend Micro VP of Cybersecurity, Greg Young, co-chairs the federal government Forum on Digital infrastructure Resilience (CFDIR) and the federal National Cross Sectoral Forum (NCSF) for Critical Infrastructure. He also holds a cabinet appointment from the Government of Barbados to that country's Cybersecurity Working Group.

Coming from a military police and counterintelligence background, Greg previously served as CISO for the federal Department of Communications, and as Research Vice President and analyst at Gartner, where he chaired four Security Summits.

Greg received the Confederation Medal from the Governor General of Canada for his work on smart card security. You can hear more of his insights on the **Real CyberSecurity Podcast**, which he co-hosts with Trend Micro's Bill Malik.

Greg Young
VP of Cybersecurity