Stronger Together

WHY XDR, SPLUNK, & MXDR ARE THE FOUNDATION OF MODERN CYBERSECURITY

INTRODUCTION

The Security Trifecta

Cybersecurity has entered an era where speed, instead of scale, is the defining factor between resilience and compromise. Threat actors no longer hack in manually; they now leverage automation, stolen credentials, and AI-assisted techniques to blend into normal activity and move quickly. In many modern breaches, the time between initial access and material impact (such as data theft, ransomware execution, or operational disruption) is measured in just minutes or hours.

Despite this reality, many security programs are still designed for a slower threat model. Logs are collected after the fact, alerts are reviewed in isolation, and investigations depend heavily on manual effort and without sufficient context. Security teams are overwhelmed by volume while simultaneously lacking clarity.

Adding to the problem is the human challenge. Skilled analysts are in short supply and maintaining consistent 24/7 coverage is difficult even for well-resourced organizations. As environments evolve and grow more distributed, it becomes increasingly complicated to keep response processes effective.

For most organizations, modern security operations is built in stages. Many begin with XDR to establish real-time visibility and control across core attack surfaces such as endpoints, networks, firewalls, email, and identities. XDR can deliver immediate value without the overhead of managing large-scale log infrastructure. Then as security maturity increases, so do requirements. When organizations reach the point where they have advanced use cases or need capabilities such as deeper forensic analysis or long-term log retention across data sources, they often turn to SIEM or SOAR solutions.

This ebook explores that security journey through a practical trifecta:

- **Cisco XDR:** delivering behavior-based detection, correlation, and automated response to stop threats in real time
- **Splunk:** providing long-term visibility, log analytics, forensic depth, and compliance-ready data retention as security maturity grows
- **Port53 Managed XDR (MXDR):** operationalizing the stack with continuous monitoring, expert-led response, and ongoing optimization

Together, these components form a modern security model designed not just to detect threats, but to stop them.

Read more about XDR and MXDR in these blogs:

www.port53.com/blog-xdr

www.port53.com/blog-the-role-of-open-and-native-integration-in-xdr

www.port53.com/blog-how-mxdr-delivers-better-business-outcomes

CHAPTER 1

The Modern Threat Landscape

The modern threat landscape is defined by convergence. A single attack campaign may involve phishing emails, credential theft, lateral movement, and API abuse, often unfolding quietly over time. While each individual signal might seem lacking in severity, the real danger lies in how those signals connect. Compared to the quick attacks mentioned in the last section, these are deceptively slow. The initial breach is quick, but total compromise involves adversaries remaining undetected for extended periods, often approaching or exceeding 300 days.

Today's adversaries aren't noisy or reckless. They are deliberate, stealthy, and patient. They leverage legitimate credentials, live off the land using native tools, and continuously adapt their tactics, techniques, and procedures (TTPs) to evade traditional, single-source security controls. Once inside, they move across environments, carefully blending into normal business activity.

For example, ransomware campaigns from groups such as SafePay and Akira escalated in 2025, targeting organizations from SMBs and K-12 districts to large universities. These actors were indifferent to industry or size, instead exploiting a universal weakness: fragmented security visibility. Akira in particular saw a rise in successful ransomware incidents because early signals of compromise were overlooked or evaluated in isolation. Initial access blended into normal operations through valid credentials, trusted tools, and routine administrative activity. Without contextual visibility connecting signals over time, defenders are forced to respond reactively, confronting the ransomware payload only after the attack chain is already complete.

This creates a profound time asymmetry between attackers and defenders. Threat actors can move quickly using automation and pre-built playbooks, while defenders are often constrained by manual investigation and fragmented workflows. Security teams may spend days attempting to correlate activity across disconnected tools, long after the attacker has already achieved their objective.

Environmental complexity only amplifies the challenge. Hybrid infrastructure, multi-cloud platforms, SaaS applications, and remote workforces have erased the traditional network perimeter. Each new platform generates valuable telemetry, but without integration and context, also blind spots.

The result is a dangerous paradox: organizations are collecting more security data than ever, yet attackers continue to succeed. This gap exists because detection alone is not enough. Visibility without context produces noise, not insight. Modern security requires an architecture that can correlate signals across domains, understand attacker behavior over time, prioritize what truly matters, and act quickly, all before any damage is done.

CHAPTER 2

Detection and Response at Speed

Extended Detection and Response (XDR) emerged in response to a fundamental shift in how attacks unfold. Modern attackers don't operate within a single threat vector, and security tools that analyze in isolation can't capture the full story. This fragmentation allows attackers to move laterally, adapt their tactics, and remain undetected for months. XDR addresses this gap by correlating activity across threat vectors, transforming disconnected signals into a coherent view of attacker behavior over time.

Cisco XDR is built specifically for this reality. It takes telemetry from across the security stack and continuously analyzes behavior using analytics, AI, and contextual enrichment. Rather than chasing after every anomaly, Cisco XDR focuses on finding patterns that indicate real adversary activity before those actions escalate into impact. By shortening the gap between intrusion and detection, Cisco XDR enables security teams to shift from reactive investigation to proactive action. The result is fewer alerts, higher confidence, and incidents that reflect meaningful risk instead of isolated events.

Cisco XDR is also intentionally open and extensible. It integrates with the Cisco security portfolio and many third-party tools while operating alongside SIEM and SOAR solutions such as Splunk. This gives organizations broad visibility into threats while allowing them to adopt XDR as an entry point to real-time security operations without replacing existing investments.

Moreover, Cisco XDR leverages unparalleled network visibility to expose lateral movement and hidden threats that endpoint-centric tools often miss. By combining deep network telemetry with unified visibility across endpoint, identity, firewall, email, cloud and more, it delivers comprehensive threat insights that eliminate blind spots and detect stealthy attacks.

CHAPTER 3

Your Foundation for Visibility and Compliance

Splunk plays a foundational role in modern security since it solves one of the hardest problems at scale: turning massive volumes of diverse data into usable insights. As a SIEM, Splunk takes telemetry from across operating systems, applications, cloud platforms, identity providers, and network devices, then normalizes and indexes that data for fast, flexible analysis.

This uniquely powerful capability enables security teams to reconstruct events with precision, searching across months or years of data to understand attacker behavior, determine scope, and identify root cause. For threat hunting, Splunk enables analysts to ask complex questions of their data, uncovering patterns that static detections might miss.

Splunk also becomes essential as security requirements expand beyond real-time response. Many compliance and regulatory frameworks require one year or more of raw security data to be retained, searchable, and auditable. While XDR platforms prioritize high-fidelity detections and can retain incident data for a short-term time, Splunk serves as the long-term system of record that governance, risk, and compliance teams depend on.

In practice, organizations tend to introduce Splunk at clear inflection points in their security journey:

- **When they want to perform custom threat hunting beyond standard vendor detections, including analysis tailored to their environment and risk profile**
- **When compliance or regulatory requirements demand extended retention and access to raw security logs**
- **When they need to analyze and correlate mature or proprietary data sources, such as ERP systems (e.g., SAP), telecom or ISP datasets, internal threat intelligence, or external intelligence feeds that fall outside typical XDR telemetry**

It's important to note that Splunk's strength lies in its flexibility and customization. That same flexibility means realizing full value often requires thoughtful data onboarding, tuning, and operational expertise. Splunk excels at revealing what exists in the data and what patterns emerge over time, rather than determining what requires immediate action in the moment.

This is where XDR and Splunk naturally complement one another. XDR delivers fast, out-of-the-box detection, correlation, and response for the most common and time-sensitive attack paths. Splunk provides depth, context, and customization as security programs mature and expand.

To reduce the operational burden associated with SIEMs, Port53 offers managed Splunk services: handling deployment, tuning, data optimization, and ongoing improvement. This allows organizations to benefit from Splunk's full analytical power without slowing down security operations or overloading internal teams.

That's why when an organization is ready to level up, Splunk is the data backbone of a broader threat detection and response strategy.

Please refer to page 20 for an infographic with more information on the XDR + Splunk customer journey

CHAPTER 4

The Power of Cisco XDR & Splunk Together

Extended Detection and Response (XDR) emerged to address a growing imbalance in modern security operations. As environments expanded, traditional tools continued to operate in insolation, generating an overflow of alerts that required manual correlation and constant attention. Cisco XDR is designed to absorb much of the reactive burden that defines day-to-day security operations through managing triage, correlation, detection, and response. By analyzing activity across domains, it can identify patterns and risks that cohesively reflect real attacker behavior.

With Cisco XDR, this shift is achieved by fundamentally changing where the work happens. The burden of detection engineering is moved away from individual security teams and placed on Cisco Talos, which continuously researches adversary behavior and delivers detections mapped to real-world tactics and techniques. At the same time, alert correlation and triage no longer depend on analysts manually stitching together signals. Instead, Cisco XDR applies AI-driven analysis to automatically group related activity, suppress noise, and surface only the incidents that represent credible risk. This allows security teams to focus on investigation and response.

Response is central to this model. Guided investigations provide immediate context, while automated playbooks and event chaining accelerate containment. This enables consistent, repeatable response (even with limited staff) and helps organizations reduce dwell time without requiring deep, tool-specific expertise for every decision.

This approach also reshapes how Splunk is used within modern environments. In an age where data is one of the most valuable enterprise assets, Splunk remains the platform that allows organizations to make sense of that data: to operationalize, analyze, and derive value well beyond security alone. While it's true that Splunk is a terrific data platform, it can also augment XDR's detection and response capabilities. For example, customers can perform deeper investigation and threat hunting in Splunk SIEM with customized remediation workflows via Splunk SOAR.. Security teams gain speed and focus through XDR, while Splunk retains the flexibility and depth needed to get long-term value from enterprise data.

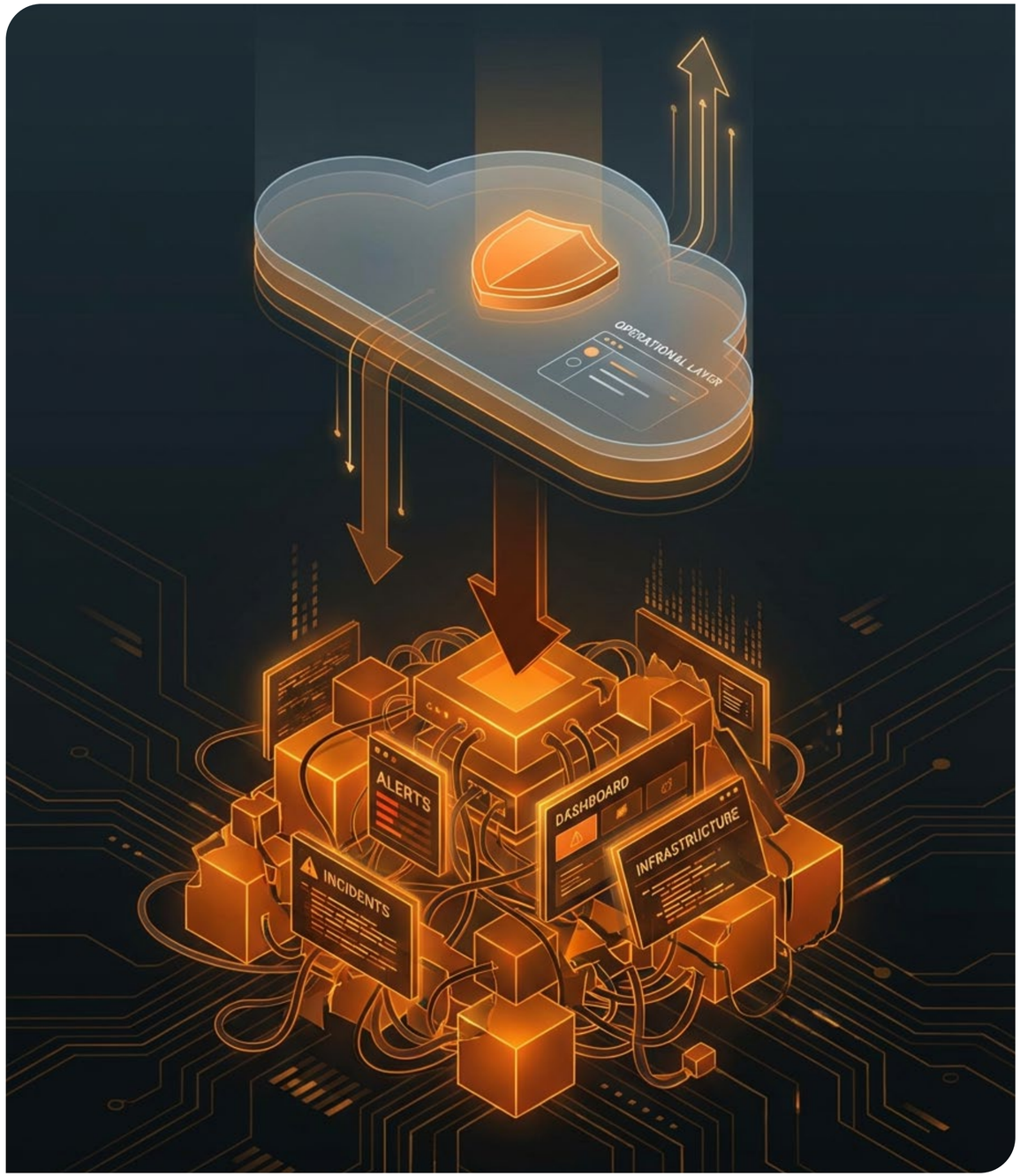
Cisco XDR is built to fit naturally into this outcome-driven model. It integrates where appropriate, supports third-party telemetry, and works alongside platforms like Splunk without requiring organizations to deploy everything at once or overhaul existing investments. Customers can adopt XDR to modernize real-time security operations and expand into broader data analytics when their maturity and requirements demand it.

Ultimately, Cisco XDR transforms raw telemetry into prioritized, actionable intelligence, while freeing Splunk to operate as the high-value data platform it was always intended to be. Together they enable organizations to move faster, reduce risk, and extract more value from their data over time.

Please refer to page 20 for an infographic with more information on the XDR + Splunk customer journey

CHAPTER 5

Port53 Brings It All Together



Even the most advanced tools can't deliver results without skilled operators and disciplined processes. This is where many organizations struggle. It's possible to build and sustain a 24/7 SOC, maintain detection quality, and keep pace with evolving threats, but for many businesses this ends up being costly, complex, and distracting from core business priorities.

In many ways, building an in-house SOC today is like building your own data center in the early 2000s. It's doable, but requires massive upfront investments, ongoing operational burden, and constant tuning just to keep it running. This challenge is especially highlighted with platforms like Splunk. While incredibly powerful, deployment, integration, and long-term optimization demand specialized expertise and significant time.

Managed XDR (MXDR) changes this model by delivering enterprise-level security operations outcomes without requiring organizations to build and run them internally. Much like AWS abstracted infrastructure to provide unlimited compute without the operational headache, Port53's MXDR abstracts security operations. It allows organizations to realize the full promise of their security data without having to run an SOC themselves.

Port53's MXDR is built on Cisco XDR and Splunk, with full lifecycle ownership: from Splunk deployment and data onboarding to detection engineering, SOAR automation, and response. Port53 analysts provide 24/7 coverage, actively investigating suspicious activity and taking action, not just generating alerts. That includes isolating endpoints, disabling compromised accounts, and coordinating solutions with customers. Just as importantly, Port53 continuously tunes, refines, and optimizes to ensure security improves. Over time, the gap closes between what security tools promise and what organizations actually experience.

CHAPTER 6

The Business Impact of a Unified Stack

A **unified detection and response approach delivers** value at every stage of an organization's security journey. For day-to-day, real-time security operations, XDR provides the essential capability to detect and respond quickly. Faster Mean Time to Detect and Respond reduces the impact of incidents and limits financial and operational damage. High-fidelity detections reduce alert fatigue and analyst burnout, improving retention and morale.

As organizations evolve, new business milestones introduce new security requirements. A manufacturing company integrating SAP and ERP systems, for example, benefits from extended telemetry and correlation to maintain visibility across IT and operational environments. When that same manufacturer wins a DoD or federal contract, security priorities shift again. Data retention, auditability, and compliance become mandatory rather than optional. At this stage, adding Splunk alongside XDR enables centralized visibility, long-term data retention, and consistent response workflows that support compliance readiness and successful audits.

For highly dynamic environments such as telecoms or ISPs, security maturity continues to grow. These organizations often rely on custom intelligence feeds and proactive threat hunting to address advanced and sector-specific threats. Here, Splunk extends XDR by enabling deep analytics, custom detections, and hypothesis-driven hunting, all while XDR continues to handle real-time detection and response.

Across every situation, security outcomes improve as the stack matures. This journey-based approach enables business agility, allowing organizations to adopt new technologies, meet regulatory demands, and pursue new opportunities with confidence that security can scale alongside the business.

CHAPTER 7

Choosing the Right Stack for Your Organization

Most organizations already have the right pieces of the puzzle in place. The goal isn't to start over, but to optimize, integrate, and mature your existing security stack over time..

For many teams, that journey starts with XDR. Cisco XDR delivers the core capabilities required for effective, real-time detection and response: reducing alert noise, improving prioritization, and enabling faster containment. For organizations focused on basic to advanced security operations, XDR alone can provide immediate improvement without unnecessary complexity.

As security requirements evolve, the need for deeper visibility and customization grows. At this stage, Splunk becomes a powerful complement to XDR, serving as the system of record, enabling advanced analytics, and supporting informed hunting while XDR handles real-time response.

Operational maturity is the final piece. Organizations without 24/7 coverage or the capacity to continuously tune detections can rely on Port53 MXDR to operate and improve the entire stack. Port53 bridges the gap between tools and outcomes, ensuring response processes remain effective as complexity increases.

Key questions should guide each step of this journey: Who owns detection and response today? How quickly can threats be contained? Are tools integrated or just coexisting? As the environment becomes more complex, is the current model still sustainable?

Answering these questions honestly highlights where integration and managed expertise can deliver the greatest security impact.

CONCLUSION

Modern Security, Managed For You

As the threat landscape continues to evolve, accelerated by the rise of AI and increasingly sophisticated attack techniques, organizations need more than point solutions to stay secure. They need a security platform and a trusted partner that can adapt as quickly as the threats themselves.

Splunk, Cisco XDR, and Port53 MXDR come together to deliver a unified, scalable approach to modern security. By combining broad visibility across the environment, advanced threat intelligence, and expertly managed detection and response, this model enables organizations to see more, detect faster, and respond with greater precision.

Most importantly, this integrated approach evolves alongside your business and the threat landscape by reducing complexity, improving security outcomes, and allowing internal teams to focus on what really matters.

XDR + SPLUNK

Customer Journey

FOUNDATIONAL

- Foundational TDIR
- Native Investigative Sources
- Endpoint + Network + Identity
- Threat Intelligence Mgmt
- Case Management
- Managed Analytics / Priority
- Asset Inventory
- Threat Visualization
- Managed Out of the Box Automation & Integrations
- Simplified Investigation Integrated SOAR solution
- Essential Third-Party Integrations
- Integrated Endpoint Forensics
- Agentic AI Investigations
- AI Generated Reporting
- < 1 year of Data Storage

TRANSFORMATIVE

- Unlimited Integrations
- Dashboards & Reporting
- Investigative Search (SPL) & Federated Search
- Basic Detections
- Cloud Deployments
- Government (GCC / State / Local) Essential ComplianceInfoSec Monitoring> 1 year of Data Storage
- On-Premise Support

MAXIMIZED

- Ad-hoc Investigations
- Deep Threat Hunting
- Bespoke & Unlimited Automation
- Detection Engineering
- Integrated Foundational TDIR
- Endpoint & Log Forensics
- AI Assisted Searches
- Out of the Box Automation FEDRAMP Low & High
- Everything in ES & XDR
- Detection Validation
- Insider Threat / UBA
- Customizable Risk-based Alerts
- Asset Risk Intelligence
- Next Generation Sandbox
- Detection Validation
- Machine Learning Took Kit
- Data Science Took Kit

LEARN MORE

For additional information about Managed XDR please visit the following webpages:

Cisco XDR

Port53 Managed XDR

SHARE