Enterprise Strategy Group™

WHITE PAPER

Architecting a Scalable Security Data Fabric for the AI Era

5 Building Blocks of a Scalable Security Data Platform

By Dave Gruber, Principal Analyst
Enterprise Strategy Group

July 2025

This White Paper from Enterprise Strategy Group was commissioned by Splunk and is distributed under license from TechTarget, Inc.

Contents

An Inflection Point for Cybersecurity

Massive AI-driven transformation is underway in all aspects of IT, resulting in an unprecedented acceleration in the pace of change. Security leaders must respond by engaging in this transformation, rethinking and rearchitecting previous security strategies to keep up.

At the same time, the advent of AI has also fueled an accelerated pace of innovation and change in the threat landscape, requiring rapid change in cybersecurity infrastructure to defend against this new AI-powered threat landscape.

Concurrently, the application of AI-driven cybersecurity innovations creates an opportunity for security leaders to rethink traditional technology stacks, security staffing models, and cybersecurity infrastructure architecture.

Underlying this opportunity is the need for a new level of security data architecture—one capable of feeding the AI security engine. The security data pipeline and platform are foundational enablers to this transformation.

This paper will explore the requirements that underlie this need and provide a perspective on what it will take to satisfy these requirements.

Data Is the Fuel for AI

AI models and applications are data-hungry beasts, requiring massive amounts of "raw materials" to power the large language models, AI-enabled tools, and the future of agentic AI applications. A new focus on data pipelines fueling this transformation is, therefore, critical to the current and future pace of AI innovation across all functions.

The cybersecurity agenda has already been on a data quest to capture, aggregate, correlate, and power analytics and threat detection mechanisms over the past several years. But the demands placed on these critical data assets have increased exponentially with the advent of AI-powered security solutions. Security architects must, therefore, reevaluate security data pipeline and management architecture and mechanisms in support of this new, more demanding, more diverse set of needs required to support an AI-driven solution stack.

Hungry for Data

Security architects must reevaluate security data pipeline and management architecture and mechanisms in support of a new, more demanding, more diverse set of needs required to support an AI-driven solution stack.

New Hybrid Operating Models

More distributed data architectures will be required, providing access to massive amounts of signals generated throughout IT infrastructure, across cloud, edge, on-premises, and third-party applications and supply chain. And while centralized data will continue to be desired, hybrid federated data architectures will become the norm, with more intelligent data movement and storage models for data in motion and at rest.

A Data Platform for Resilience

As security leaders and architects prepare for this new environment, the underlying security data platform must power a rich set of capabilities that extend beyond core security operations. This data set will inform IT and risk leaders, enable auditing and compliance activities, and power a new set of agentic AI solutions to collaborate with humans in the delivery of a resilient operation.

As the security solutions stack evolves to protect a rapidly changing IT infrastructure and associated attack surface, this new data platform must be extensible, flexible, and scalable in its ability to leverage new signals, actions, and

operating environments. This means that the security data platform must be able to serve the needs of this diverse operating environment, supporting multiple security platforms and specialized security tools as they continue to emerge in support of the growing and changing attack surface. This data platform must also enable rapid innovation and adoption of AI-enabled capabilities both within existing security tools stacks and within net-new solutions and tools as they become available.

Tools Consolidation: Moving to a Continuous Process

While many focus on security platform adoption in support of tools consolidation initiatives, tools consolidation agendas will quickly become a continuous process for most, as specialized, new security tools are adopted to protect emerging infrastructure not yet protected by major security platforms. In parallel, as the use of security platforms continues to grow, it will become commonplace for organizations to leverage multiple security platforms to achieve coverage across the entire operating estate.

To support this operating diversity within the security tools stack, the security data platform must be capable of ingesting and analyzing signals and operating characteristics across this ever-changing environment, while providing scale, extensibility, and configurability without the need for specialized engineering or custom integration activities.

Meanwhile, the data platform must enable risk and resilience analysis and reporting, offering a perspective tailored to each stakeholder group, including cybersecurity leadership.

A New Model for Security Operations

As the opportunity to modernize security operations in the AI era becomes real, a deep focus on detecting all levels of cyberthreat across the attack surface continues. The accelerated pace of threat diversity requires an optimized threat detection and intelligence operating model, capable of stitching together signals across the estate as advanced threat activities progress. More advanced, more automated threat detection rules engineering will, therefore, be needed to keep up. Beyond basic detections, continuous analysis of attack patterns will become critical as proactive security activities focus on mitigating future risk.

As the adoptions of AI-enabled systems enable the responsibilities of security analysts to shift from more tactical investigation to more strategic risk mitigation activities, individuals will likely take on responsibility for specific parts of the operating environment, requiring new dashboards, risk metrics, and risk analytics aligned to these areas. These new workflows will require a nimble, highly configurable workbench that can be tailored to the specific responsibilities and operating model within individual SecOps teams.

Similarly, leadership will want tailored insights and metrics that align with specific organizational risk and security responsibilities.

A More Autonomous SOC

Rapid Change Is Underway

The rapid pace of innovation in the use of agentic AI capabilities will drive significant process and organizational shifts in long-time SecOps models.

In the advent of AI, agentic AI, and AI assistants, the autonomous security operations center (SOC) conversation has become lively.

Automation is certainly not a new agenda in SecOps, with Enterprise Strategy Group research reporting that 92% of organizations are automating SecOps processes, with 79% automating processes associated with tier 1 or tier 2

analyst activities.[1] Security orchestration, automation, and response tools and built-in workflow automation have been prevalent, and the use of AI assistants to automate specific tasks has quickly become a popular use case.

While most still have concerns about the level of autonomous operation that will be attainable, it's clear that AI capabilities are fueling rapid growth in SOC automation. Most also agree that, to keep up with the AI-enabled threat landscape, more automation is needed to support all aspects of the cybersecurity function.

Enterprise Strategy Group believes the rapid pace of innovation in the use of agentic AI capabilities will quickly prove valuable, but at the same time will drive significant process and organizational shifts in long-time SecOps models. While this change will feel uncomfortable for many, it will be rapidly embraced and will quickly become the new operating norm for the function.

The Future of SIEM

Enterprise Strategy Group research reports that 96% of organizations are currently using or deploying SIEM solutions as the data platform to support their SecOps function.[2] This same research revealed that 48% of organizations are reevaluating existing SIEM investments as they prepare for the AI era.

Further, this research showed that the tools consolidation agenda is very active, with 97% of organizations consolidating tools or investing in larger security platforms.[3] Many security platform providers are adding SIEM capabilities into their platform offerings, fully integrating with the other native security capabilities offered with the platform. These platforms often also provide a limited set of out-of-the-box integrations with other third-party security tools, in addition to API that enable further custom integrations.

The Future of Security Data Platforms

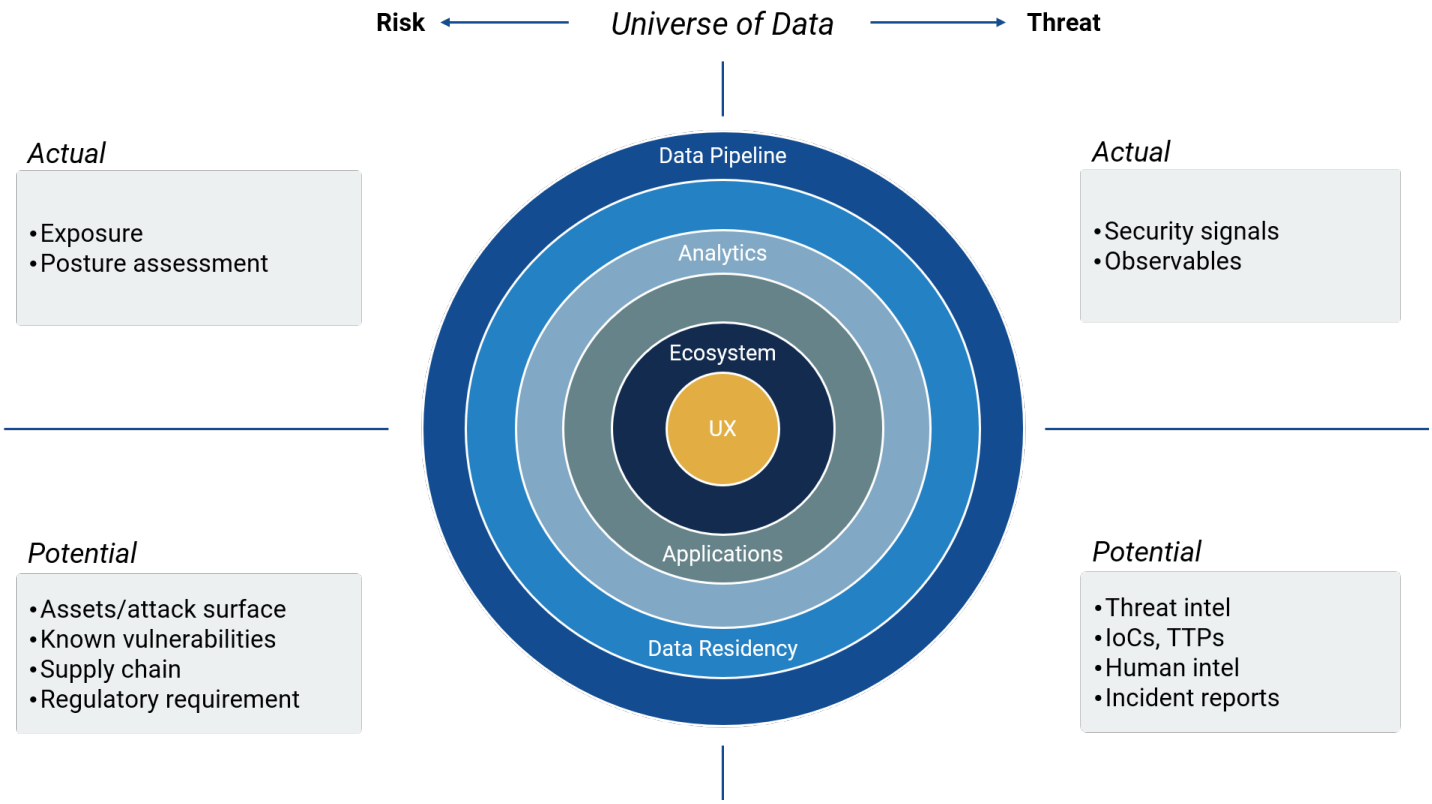
More federated, flexible data architectures that incorporate risk agenda and the ability to rapidly employ AI and agentic capabilities will be needed to support an AI-enabled security model.

Since it simplifies the security stack, this "all-in-one" architecture will seem appealing to many, causing them to question standalone SIEM investments. But for many, concerns about locking into proprietary data models and the need for a more extensible, flexible data platform layer capable of supporting a more diverse multiplatform and tools environment will motivate the use of an independent security data platform.

Supporting this need, stand-alone SIEM solution providers are accelerating innovations, embracing the need for more federated, flexible data architectures, while incorporating the risk agenda and rapidly employing AI and agentic capabilities to improve efficiency and efficacy.

[1] Source: Enterprise Strategy Group Research Report, *The Future of SecOps in an AI-driven World*, April 2025.
[2] Ibid.
[3] Ibid.

Figure 1. Security Data Platform Architecture



Source: Enterprise Strategy Group, now part of Omdia

5 Building Blocks of a Security Data Platform

While at the heart of the security data platform is a rich, comprehensive data set, the ability to meet the diverse needs of the many functions and tools served requires a scalable, highly configurable set of operating capabilities on top of the data set. Below is a checklist for the five major building blocks of a scalable security data platform.

1. **Rich, Comprehensive Data Set**
   - Signals From Everywhere—Activity
     - Logs and telemetry from detection and response tools across all threat vectors
     - Signal enrichment
     - Signal correlation
     - Signal prioritization
     - Noise reduction
     - Observability—extending use cases beyond security
   - Threat Intel
     - Indicators of compromise (IoCs); tactic, techniques, and procedures (TTPs); TTPs used by specific threat actors
     - Extensible threat intelligence (TI) consumption (external sources, internal sources, history, etc.)

    - Threat assessment—malware sandbox
    - Threat and attack history
    - TI management, sourcing/speeding new TTPs, IoCs, etc.
- Risk Data/Assets/Vulnerabilities/Exploits/Exposure
    - Asset inventory
    - Coverage gaps
    - Risk scoring
    - Functional/organizational risk
    - Risky identities
- Organizational Context
    - Who should be using what parts of my infrastructure?
    - What about machine identities?
    - Insider threat?
    - Privileged activity?
- Standards Support
    - OCSF
    - STIX/TAXII
    - Broad connectivity/APIs/out of the box (OOTB)

2. **Data Pipeline, Management, Residency, and Scalability**
    - Data Ingestion from Anywhere; OOTB Connectors for All
        - Ease of ingesting new sources
        - Structured and unstructured data support
    - Data Export
        - Sharing data with other systems and tools
    - Optimization: Data Storage and Management
        - Not all data is equal. Where should the data reside? Why?
        - Hot-warm-cold data > this is part of “managing” the data.
    - Flexible Data Residency Options
        - Cloud and on premises
        - Federated storage and access
        - Centralized vs. federated storage and access
        - Data sovereignty support
    - Extensibility/flexibility of the data model/schema
3. **Analytics and Applications: Powerful, Flexible, and Scalable**
    - Threat Detections—Seeing Suspicious or Malicious Activity
        - Tailoring detections to an organization’s specific environment

  - Signal prioritization
  - AI-driven enrichment
- Posture, Risk, and Exposure Management
  - Identifying/detecting exposures
  - Coverage—Where are my security controls not operating effectively?
  - Where do I lack visibility? (rogue assets, missing data, etc.)
  - Risk quantification
- Investigations
  - Correlation: Stitching signals together (correlation)—How much manual? Automated?
  - Data enrichment
  - Human and AI-driven enrichment support
  - Mitre ATT&CK mapping and enrichment
  - Threat intel enrichment—informed investigations
  - Malware analysis
  - Determining the full breadth and scope of an attack
  - Uncovering all damage, recon, etc. activities associated with an attack
  - Search across the estate for like activities/patterns of attack
  - Forensics activities (query for more forensics details—direct to/from an asset)
  - AI-assisted insights regarding threat patterns, history, and actions
- Hunting
  - Creating a hypothesis/premise
  - Rapid search supporting specific hypothesis or TI
  - Correlation to other adjacent activities
  - Automated hunting
- Metrics/Reporting/Dashboard
  - Compliance reporting
  - Posture over time
  - Strengths/weaknesses
  - Customizability
  - Role-specific
- Audit/Compliance Analytics
  - Specific regulatory support
  - Audit preparation
  - Rapid audit response architecture
- Workflow Analytics
  - Escalation/routing

  - Collaboration
  - Incorporating automated workflows when needed

4. **Response Actions**
   - Comprehensive, OOTB Response Options and Automation
     - Isolate an asset
     - Block an IP/port
     - Execute a playbook
     - Forensics data capture
     - Sandbox detonation
     - Update security controls to close gaps, misconfigurations, etc.
   - AI-driven Actions
     - Autonomous activities
     - Agentic activities
     - Prescriptive activities
     - Strengthen security controls to close gaps, misconfigurations, etc.
   - Complex, Multi-stage Action Orchestration
     - Playbooks
     - Well-defined actions
     - Loosely defined actions
   - Extensibility Model to Enable Customized Response Actions
     - Extensibility of response actions—new connections, new actions, etc.
5. **Community and Ecosystem**
   - Knowledge Sharing
     - A rich community knowledge base, sharing insights, extensions, use cases, methods, configurations, and more
     - Threat intel and investigation collaboration/sharing and TI pipeline
   - Talent
     - A broad talent/resource pool
     - Education, training, and certifications
   - Ecosystem
     - A shared community ecosystem providing additional platform tool extensions, shared threat intel, platform connectors, and add-on capabilities
     - A marketplace enabling platform users to find and learn about available tools, extensions, and other platform-related technology provided by others

Conclusion

SOC modernization for the AI era requires a powerful data platform, capable of serving the needs of a diverse and rapidly changing SecOps environment. The data platform must bridge the needs of multiple security platforms and specialized tools, while supporting the rapid innovation of AI-driven solutions.

This data platform requires rich threat detection and response capabilities but will need more.

As the security data set continues to grow, the data platform must massively scale while providing deployment and usage flexibility, extensibility, and scalability, all while leveraging AI to strengthen the many operating capabilities to speed SOC transformation in the AI era.

Enterprise Strategy Group recommends that security leaders and architects look wholistically at the future state of the operating model and solutions stack to ensure this critical architectural component will support program and organizational growth during this period of rapid innovation and change.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com