Cybersecurity

Whitepaper

Optimize for resilience

Driving secure outcomes with a multi-vendor platform strategy

Erik Stiphout

Contents

1. Introduction

In today's multi-vendor security landscape, enterprises often deploy dozens of specialized tools to address different threat vectors. This best-of-breed approach can deliver strong capabilities in each domain, endpoint, e-mail, identity, and beyond, but it also introduces complexity.

Large organizations typically manage 45 - 80 different security tools, which can lead to siloed defenses, integration gaps and high recurring costs. No single solution is a "silver bullet"; and a security posture is always a journey requiring strategy, integration, and human expertise.

A value-driven approach to security

With that context, this whitepaper offers a balanced perspective for CISOs and other decision makers on how to maximize threat protection and modern SecOps through a unified platform approach, while thoughtfully incorporating specialist solutions where they add value. We will explore the benefits of consolidation, the role of niche tools in a "defense in depth" strategy, integration best practices, and considerations for Agentic AI and regulatory compliance (e.g., GDPR, NIS2) in a multi-vendor environment.

From "best in breed" to "best of both worlds"

80

average number of security tools used by a typical enterprise

80%

reduction in response effort from consolidating threat protection into strategic security platform (Microsoft Defender)

$1.49m

financial benefit of improved security posture with CrowdStrike Falcon Shield

Simplifying and consolidating security tooling can increase resilience and reduce costs. This paper advocates for a platform-agnostic, yet open approach to cybersecurity anchored by integrated solutions while recognizing the strategic value of incorporating best-of-breed technologies such as Microsoft, CrowdStrike, Varonis, Mimecast, Okta, and others where appropriate.

2. Executive summary

Key takeaways

In today's complex threat landscape, organizations often rely on a patchwork of security tools, which can lead to operational inefficiencies, integration gaps, inflated cost and increased risk. This paper offers the following analysis and conclusions:

1. **Unified platforms enable simpler and stronger security and compliance**
   Integrated security and compliance platforms streamline operations, reduce audit complexity, improve detection and response, and lower total cost of ownership compared to fragmented multi-vendor setups.

2. **Platforms can be enhanced with best-of-breed tools**
   Complement integrated platforms with specialized solutions (e.g., ProofPoint, Sophos, CrowdStrike, Mimecast) where they add unique value, ensuring proper integration to avoid silos.

3. **SIEM and SOAR are essential operational force multipliers**
   Solutions like Splunk, Microsoft Sentinel, or Palo Alto Cortex XSOAR as the main Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms have become essential for rapid threat detection, investigation, and response.

4. **AI enhances security but requires organizational adaptation and governance**
   Agentic AI strengthens threat detection, automates workflows, and improves analyst efficiency. However, realizing these benefits requires organizations to adapt their operating models, skills, and processes to support AI-driven agents, while addressing new governance, compliance, and regulatory challenges.

5. **Integration is critical for modern SecOps**
   Native interoperability across endpoints, identities, email, cloud, and data enables faster, coordinated responses and a unified view for security teams.

6. **Managed service providers add critical expertise**
   Managed services play a critical role in helping all types of organizations implement and maintain secure, scalable, and cost-effective security architectures. Hands-on experience and multi-vendor landscape knowledge can help any organization identify redundancy in tools and other cost centers.

A strategic approach should prioritize integrated platforms for simplicity and efficiency, while retaining flexibility to incorporate specialized solutions where they deliver a unique value or a business specific advantage.

3. Best-of-breed solutions in a multi-vendor ecosystem

Why multi-vendor security ecosystems persist

Despite the clear advantages of platform consolidation, most enterprises will continue to operate in a multi-vendor ecosystem to some extent. There are valid reasons why an organization might augment or even (temporarily) opt out of consolidated platform suite in favor of another vendor's product.

Enterprises often do so due to legacy systems, diverse business units, regulatory obligations, or specialized use cases. SMBs typically prioritize pricing, deal incentives, and available resources. In both cases, understanding practical, financial, and operational drivers is key to building a strategy that balances integration, flexibility, and risk.

Common reasons for having multi-vendor security ecosystems include:

- **Legacy investments and inertia**
  Significant investments in tools like CrowdStrike Falcon or Mimecast, deeply embedded in workflows and supported by trained staff, make rip-and-replace strategies impractical. Security leaders often retain proven tools while gradually moving towards unified platforms such as Microsoft, CrowdStrike, Trend Micro, or Sophos.
- **Specific strengths or requirements**
  Point solutions can deliver unique benefits. CrowdStrike excels in threat hunting and lightweight agents, while Mimecast offers e-mail continuity and advanced phishing detection. Organizations may also seek a "second opinion" for defense-in-depth or meet niche compliance needs with specialized encryption or DLP tools.
- **Vendor diversification**
  Some CIOs/CISOs adopt multi-vendor strategies to avoid lock-in, reduce single-vendor risk, and encourage competitive procurement. Even with broad portfolios, organizations may mix vendors for resiliency and innovation.
- **Organizational structure and skills**
  Large enterprises often have separate teams owning different domains – network teams favor Palo Alto, endpoint teams prefer Microsoft or CrowdStrike. Mergers and acquisitions add complexity, making overnight unification unrealistic. Security architects should focus on integrating disparate technologies into a cohesive strategy.

Best practices for managing multi-vendor security environments

Recognizing these realities, the goal for modern SecOps is to harmonize multi-vendor environments to approach the efficiency of a unified platform. Best practice is to place focus on integration, visibility, and data flow between tools by doing the following:

1. **Centralize detection and response**
   Establish a single source of truth for incident detection and response by aggregating alerts and telemetry into a centralized SIEM. Solutions like Splunk, IBM QRadar, or Microsoft Sentinel can fulfill this role. Ensure the SIEM ingests and correlates data from all sources using prebuilt connectors and APIs for tools like CrowdStrike, Palo Alto Networks, Okta, and Microsoft Defender. This creates unified incident timelines and supports faster, informed decisions.

2. **Integrate at the policy/prevention layer**
   Where possible, integrate third-party tools with platform preventive controls. Many EDR solutions support coexistence modes, allowing one tool to monitor while another enforces. Similarly, organizations often deploy secure email gateways alongside cloud email services for layered filtering and continuity. While this adds complexity, proper integration strengthens protection for high-risk channels.

3. **Align people and processes**
   Avoid team silos by promoting cross-training and unified playbooks. For instance, phishing response should include checks in Microsoft 365 and Mimecast. Regular purple-team exercises validate end-to-end workflows. Multi-vendor setups demand deliberate collaboration to prevent parallel, disconnected responses.

4. **Leverage automation and orchestration**
   Use SOAR solutions or cloud functions to link tools when native integration is lacking. For example, if CrowdStrike detects a threat, automation can disable accounts in Microsoft Entra ID or isolate devices via MDM. Conversely, a DLP alert could trigger CASB or ticketing workflows. These integrations prevent gaps but require effort—most "partnership" integrations share signals, not full connectivity. For hybrid environments, a strong SIEM + SOAR combo often delivers the best results.

SoftwareOne's Approach

We prioritize customer needs, tailoring security architectures to goals and existing investments. While integrated stacks like Microsoft offer efficiency, most customers operate hybrid environments. The real value lies in optimizing that mix and ensuring interoperability when leveraging platform-agnostic capabilities and best-of-breed tools where they deliver unique benefits.

4. The case for an integrated security platform

A modern unified security platform serves as a foundation for a Zero Trust strategy, combining multiple layers of protection into a single, integrated ecosystem. Instead of relying on a patchwork of point solutions, this approach pulls together key security capabilities under one umbrella.

Typical capabilities of an all-in-one security foundation

- **Endpoint protection and attack disruption:** Securing desktops, servers, and mobile devices against malware, ransomware, and intrusions, with AI-driven detection, behavioral analysis, and automated attack disruption to contain threats in real time.
- **Email and collaboration security:** Protecting users against phishing, business email compromise, and malicious content in messaging and file-sharing platforms, enhanced by AI-based threat detection and response.
- **Identity and access management (IAM):** Ensuring strong authentication (e.g., MFA), adaptive and conditional access based on user, device, and risk signals, and continuous identity threat detection powered by AI.
- **Cloud access security broker (CASB) and SaaS governance:** Governing the use of SaaS applications, enforcing security policies, and detecting risky behaviors and misconfigurations across cloud services.
- **Application security:** Protecting business-critical applications and APIs from vulnerabilities and exploits through runtime protection, app shielding, and continuous security monitoring.
- **Network security via SASE:** Enabling secure connectivity for remote and hybrid workforces using Secure Access Service Edge (SASE), combining zero trust network access, firewall-as-a-service, and secure web gateways.
- **Data security and compliance:** Providing visibility and control over sensitive data through integrated data loss prevention (DLP), encryption, and information labeling across endpoints, cloud services, and collaboration platforms.
- **Exposure and vulnerability management:** Continuously identifying, prioritizing, and reducing security exposure across identities, endpoints, cloud workloads, applications, and data by correlating vulnerabilities, misconfigurations, and attack paths.
- **Cloud-native, platform-agnostic SIEM and SOAR:** Delivering advanced threat detection, AI-assisted investigation, and automated incident response across the entire environment.

Security benefits of an integrated platform

A platform-centric approach improves efficiency, visibility, and consistency. It strengthens Zero Trust by unifying identity, device compliance, access control, and data protection. At the same time, the environment remains a flexible and cost-effective foundation on which you can build capabilities as they're required. By consolidating capabilities under a unified architecture, organizations benefit from:

1. **Real-time telemetry and threat intelligence sharing across all layers.**
2. **Faster attack detection and response.**
3. **Reduced operational complexity.**
4. **Streamlined enforcement of consistent Zero Trust policies enterprise wide.**
5. **A single pane of glass view, improving efficiency and resilience against evolving threats.**

Case studies and research confirm these benefits: one global survey found that companies using integrated platforms identified and contained threats significantly quicker on average than those with fragmented toolsets.

Further advantages

Operational and cost efficiencies

A unified security platform eliminates tool sprawl, reducing complexity, cost, and risk. Instead of juggling multiple consoles, agents, and contracts, teams manage one system. This removes redundant features, lowers licensing and maintenance costs, and cuts integration effort. Simplification means fewer errors and misconfigurations. Consolidation also improves financial performance, delivering predictable budgets and higher ROI compared to siloed tools. For smaller businesses, it reduces overhead and gaps across devices, identities, and cloud services—strengthening protection without adding staff. One platform streamlines operations, improves control, and turns security into a driver of efficiency.

Improved coverage and consistency

Endpoints, e-mail, web traffic, identities, and cloud apps are secured under one system, reducing gaps and improving response. Shared signals turn threats like phishing and malware into a single correlated incident, giving analysts more context and speed. Consistent policies apply across devices, e-mail, and storage, strengthening Zero Trust by linking compliance, identity, and access decisions. Non-compliant devices can be blocked automatically—something hard to achieve with disconnected tools. Leading vendors such as Microsoft, Palo Alto, Cisco, CrowdStrike, and Check Point now offer integrated suites that rival specialized tools in areas like endpoint protection, SIEM, and identity security.

Integrated platforms are the new standard

Security vendors have shifted from niche tools to integrated platforms. CrowdStrike now includes cloud security, identity protection, and SIEM; Palo Alto and Fortinet added SASE, CASB, and automation; Cisco and Microsoft offer unified suites combining identity, endpoint, and cloud security. This trend towards platformization gives enterprises more choices, but most will still run multiple vendors for legacy or specialized needs. Strong platforms act as the core, supporting open APIs and flexible workflows for integration. SMBs benefit even more, reducing tool sprawl and management overhead. Consolidation improves efficiency, visibility, and Zero Trust enforcement, but leaders must assess gaps and avoid single points of failure. The goal: lower complexity and cost while retaining adaptability and depth.

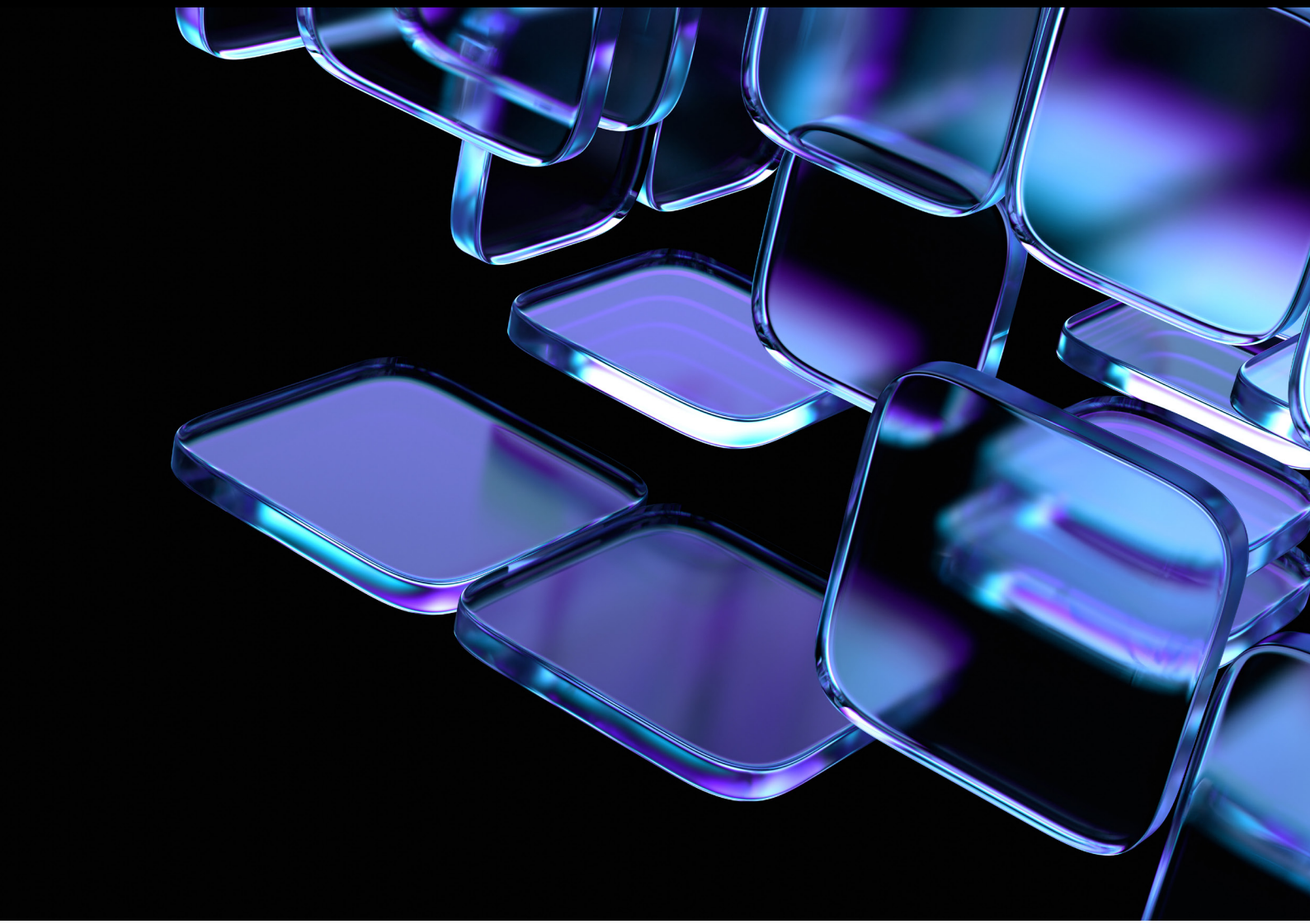
5. The role of AI and agentic systems in modern security architectures

Gaining the upper hand with AI

Artificial Intelligence (AI) is transforming cybersecurity, but it's a double-edged sword. On one hand, AI-driven tools and agentic AI (capable of autonomous decisions) offer unprecedented advantages. They boost SecOps efficiency by automating threat detection, triage, and response at machine speed and scale. Early deployments show promise: autonomous SOC assistants can remediate incidents in seconds, reducing alert fatigue and mean-time-to-response by orchestrating across tools with minimal human input. In an era of relentless attacks and talent shortages, these AI "co-pilots" act as force multipliers, handling routine tasks and surfacing critical insights faster than ever.

On the other hand, AI introduces new risks and attack surfaces. Its ability to learn and act autonomously creates opportunities for adversaries, such as manipulating models to bypass controls or leak sensitive data. Threats include model poisoning, adversarial examples that trick detectors, and rogue agents causing unintended damage—like deleting critical files or shutting safety down systems. Generative AI can also expose confidential data, while "shadow AI" use by employees in unsanctioned tools bypasses compliance safeguards.

To harness AI safely, organizations must evolve governance, detection, and response strategies and regular testing strategies to continuously evaluate an AI agent's ability to respond correctly to threats that it discovers. Traditional security policies need updates to include AI in threat models, monitor AI outputs for anomalies, and enforce strict data-handling rules. Crucially, AI systems require robust logging, human review checkpoints, fail-safes and continuous testing regimes to ensure responses are accurate. The goal: leverage AI's benefits without creating blind spots. Effective adoption demands equal focus on innovation and AI-specific risk management.



Integrated systems are becoming a necessary edge

The list of risks and mitigation strategies on the following page is not exhaustive, but it illustrates the need to adapt classic security controls to the AI era. Many mitigation strategies involve extending existing best practices such as input validation applied to AI model prompts and AI agent roles or adversarial testing and AI-specific policy enforcement. This represents new practices that security teams should build expertise in. This is most visibly found in the tools implemented to build these mitigations which will often span multiple vendors and technologies.

You might use a cloud provider's AI content moderation API alongside your own proxy filters to stop prompt injection, or a combination of your CASB and an AI vendor's admin settings to control "shadow AI." Thus, even risk mitigation brings home the importance of integration across systems.

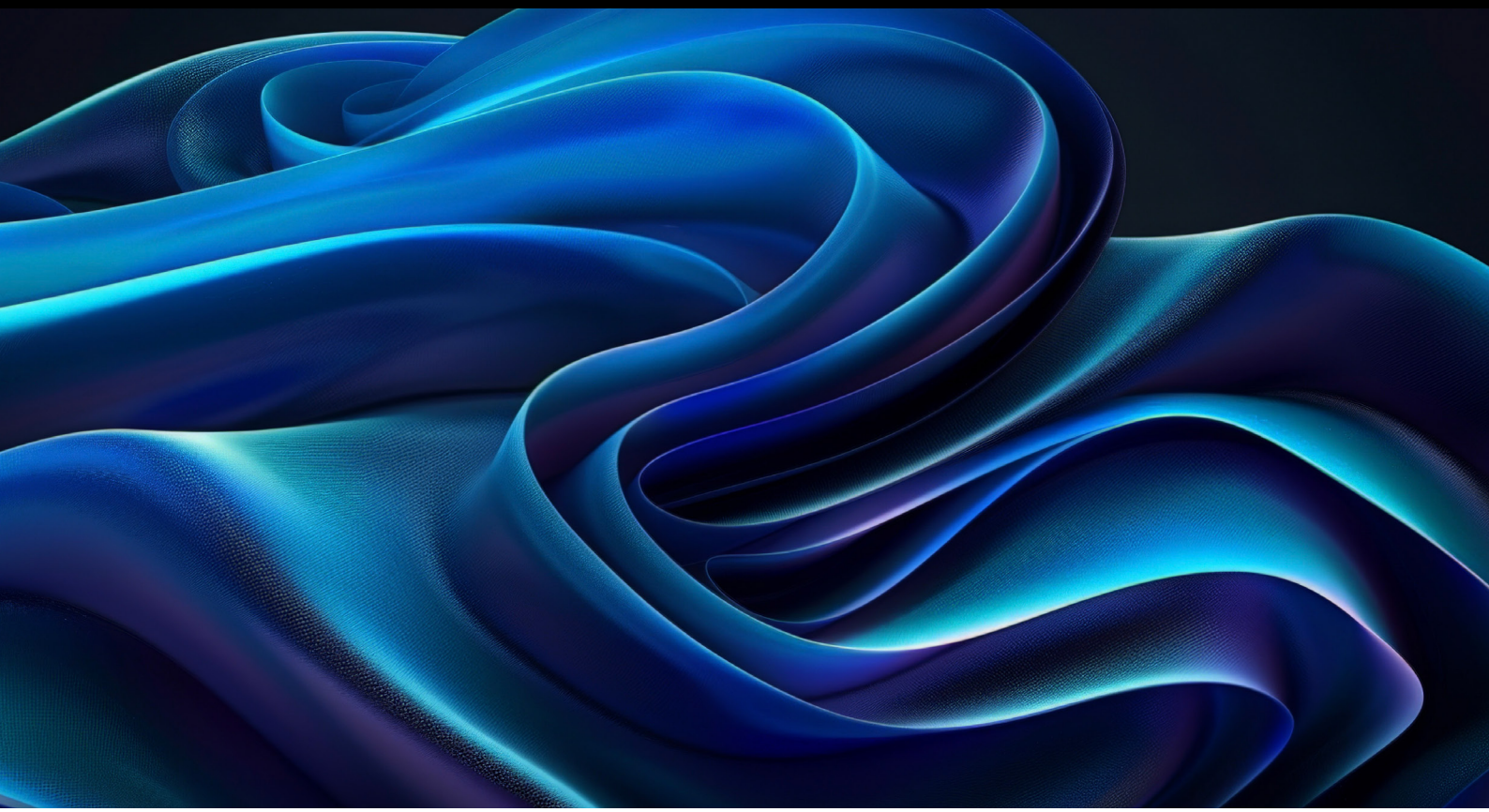
Whether integrating large language models from providers like OpenAI, Anthropic, or Google, or orchestrating AI-driven workflows across platforms such as AWS Bedrock or Azure OpenAI, the complexity of securing these systems demands a unified yet flexible approach.

5.1 AI and agentic systems: emerging risks and mitigation strategies

AI Risk	Description	Mitigation Strategy
Prompt Injection & Model Manipulation	Attackers manipulate AI inputs (prompts) or exploit model flaws to bypass controls, cause misbehavior, or extract sensitive data from AI models. This can lead to an AI system ignoring policies or revealing confidential information it was meant to keep hidden.	Implement strict input validation and content filtering for AI prompts (e.g. disallow certain commands or data patterns); apply rate-limits and anomaly detection to AI queries. Use data classification and access control tools to restrict sensitive data exposure to AI (only provide models the minimum data they need).
Autonomous Agent Misuse	An agentic AI with decision-making power might take unintended or harmful actions due to bugs, poorly defined goals, or malicious instructions. For example, an AI incident responder could inadvertently shut down a critical server, or an attacker might trick an AI agent into escalating privileges.	Scope and permission of AI agents carefully and apply least-privilege access, so an AI can only perform a narrow set of actions. Enforce human verification for high-impact actions ("human in the loop") until trust is established in the AI's reliability. Maintain detailed audit logs of agent activities and have alerts for any out-of-policy actions.
Shadow AI & Unapproved Tools	Employees or business units may adopt AI services (e.g., an online AI coding assistant or a chatbot builder) without security vetting. These tools might process sensitive company data in the cloud, outside governance controls, creating compliance and data leak risks.	Discover and monitor AI usage through tools like cloud access security brokers (CASBs) or SaaS management platforms that can detect traffic to AI services. Once identified, bring them under policy: either sanction and secure them or block them if risky.

AI Risk	Description	Mitigation Strategy
Data Leakage via AI Outputs	AI-generated content may inadvertently include confidential information. This can happen if an AI was trained on sensitive data or if an AI summarizes a private document too verbosely. There's a risk of regulated data (personal data, financial info) showing up in AI outputs without proper controls.	Treat AI outputs with the same caution as any data channel. Use sensitivity labelling and classification on inputs and outputs of AI: e.g., tag data that an AI processes, and configure the AI or a post-processing tool to mask or avoid regurgitating certain content. In short, don't fully trust AI to know what's secret and put guardrails on what it can output and to whom.
Compliance Gaps	AI systems may process personal data or make decisions affecting people without proper oversight, potentially violating privacy laws or industry regulations. Lack of documentation on AI decision logic or insufficient record-keeping could also breach compliance requirements (for example, GDPR's requirement for explainability or audit trails).	Embed AI into your compliance framework: conduct Data Protection Impact Assessments for AI projects involving personal data (as you would for any major data processing). Use compliance management tools or modules to map AI systems against regulations and maintain documentation of AI models (training data sources, how the model was validated for bias and accuracy, etc.) to show regulators or clients that due diligence was done.
Overreliance on AI for Threat Response	There is a risk in leaning too heavily on AI to run security operations without human judgment. AI might miss subtle context or fall for sophisticated deception, and if humans step back too much, a critical alert might be ignored because "the AI didn't flag it." Over-automation can also lead to complacency, where the organization is slow to react when the AI encounters something novel.	Human-in-the-loop by design is necessary so security teams should decide upfront which incidents or decisions require human confirmation. Finally, have a fallback plan for when AI systems are down or proved wrong. In summary, use AI to augment, not replace, expert judgment, especially in complex or crisis scenarios.

Table: Major risks introduced by AI/agentic systems and approaches to mitigate them in a cybersecurity context.



6. Navigating regulatory compliance (GDPR, NIS2, etc.) in a multi-vendor strategy

While threat protection and SecOps are central to this whitepaper, governance, risk, and compliance (GRC) remain critical for security leaders, especially in regulated industries or under laws such as GDPR or the EU AI Act. A multivendor security environment adds complexity: each tool uses different logging formats, retention policies, and reporting standards. This makes gathering audit evidence and enforcing policies time-consuming and prone to gaps.

Simplifying your compliance tooling within a single strategic platform brings the following benefits:

- **Own a single source of truth**
  Unified platforms simplify compliance by centralizing control libraries, assessments, and regulatory mapping for frameworks like ISO 27001, GDPR, NIS2, and NIST. Solutions from Microsoft Purview, Google Cloud DLP, Amazon Macie, Palo Alto, and Cisco offer dashboards that consolidate evaluations across email gateways, endpoints, cloud services, and identity systems. This reduces manual effort and improves visibility.

- **Cover data protection gaps**
  Data classification and DLP also benefit from a single policy plane. Leading platforms allow consistent definitions of sensitive information and enforce policies across email, storage, collaboration tools, endpoints, and cloud apps. Without this, organizations run separate DLP products for each channel, increasing overlap and risk.

- **More effective enforcement**
  Regulations like GDPR demand clear insight into personal data and consistent handling of retention, deletion, and access control. Unified compliance solutions help discover and label personal data across workloads. Privacy tools such as OneTrust remain valuable for program-level governance, but enforcement depends on security and productivity platforms.

- **Find records more easily**
  Audit and investigation workloads are easier with integrated platforms offering long log retention and unified search. In multivendor setups, logs often reside in silos, forcing organizations to export data to SIEMs or data lakes for correlation. Similarly, records management and eDiscovery are streamlined under unified systems, avoiding multiple archives for email, files, and chat. While connectors can pull data from external systems, they require planning and remain partial.

Both large enterprises and SMBs will benefit from consolidation. Larger firms face complexity from legacy tools; smaller firms lack staff for audits. A primary compliance system reduces operational overhead, cost, and audit complexity. Third-party tools still play a role, but their outputs should feed the central compliance view.

7. Conclusion

A platform-centric, yet open approach to security

Resilience today demands organizations manage risk effectively and efficiently. Our position is that adopting a unified security platform as the backbone of your cybersecurity strategy is a winning approach for both enterprises and SMBs.

This strategy is not about vendor loyalty or chasing trends, it's about resilience, clarity, and agility. Over-complex toolsets slow response and create blind spots. Attackers "think in graphs," moving laterally, while defenders often "think in silos." A modern platform enables holistic threat visualization. At the same time, relying exclusively on one vendor can be risky; flexibility remains essential. Introduce specialized tools only when they add measurable value and can effectively interoperate with one another (or be consolidated through the use of an effective SIEM/SOAR platform.).

Consolidated platforms from vendors such as Microsoft, CrowdStrike, Palo Alto Networks, SentinelOne, or Google Cloud deliver end-to-end visibility, reduce operational overhead, and enable faster, coordinated responses across modern attack surfaces. In an era of high-velocity threats and limited security manpower, this integrated foundation often marks the difference between reactive and resilient security. Industry research consistently shows improved outcomes and cost advantages from thoughtful consolidation.

Being pragmatic and value-driven

Platform-centric does not mean platform-exclusive. CISOs must remain pragmatic and value driven. Where a platform offers strong native capabilities and automation, maximize that investment. Where gaps exist or specialized tools provide distinct advantages, integrate them. For example, an organization may use CrowdStrike for advanced threat hunting while retaining Mimecast for compliance archiving. The key is integration, avoiding new silos and ensuring all tools contribute to a unified operating model.

Our recommendation: maximize platform capabilities, periodically reassess other tools, and ensure strong integration via APIs, SIEM/SOAR connectors, and shared telemetry. Over time, many organizations retire standalone products, reducing cost and complexity. A platform-plus strategy delivers modern SecOps success, eliminates visibility gaps, and keeps organizations agile as threats evolve – aligning security with business outcomes and enabling CISOs to lead with confidence.

How we help clients succeed

Drawing on experience across global enterprises and SMBs, SoftwareOne helps clients strike the right balance.

We start by assessing the current environment: Are teams overwhelmed by alert fatigue or too many consoles? Are niche risks driving tool sprawl? From there, we define a roadmap that typically consolidates onto a primary platform, supported by workshops, pilots, and ROI analysis, while evaluating which legacy tools to retire, integrate, or retain. The goal: a unified architecture augmented by a few purpose-built technologies, orchestrated under coherent SecOps processes.

SoftwareOne security experts work with clients in 60+ countries. We offer advisory, professional and managed services around Microsoft, AWS and Google, and partner with all leading security vendors. We hold in-depth expertise in the latest security practices and technologies (including Microsoft, Splunk, Trend Micro, CrowdStrike, Sophos, and more.)

Whether you're ready to engage us to maximize the value and minimize risk, or you'd like to explore our services further, reach out and arrange a meeting with our security and compliance experts.

Let's talk

T. **+41 44 832 41 69**
E. **info@softwareone.com**

CONTACT US TODAY

Find out more at
www.softwareone.com

SoftwareOne Corporate Headquarters
T. +41 44 832 41 69
E. info@softwareone.com