The Ultimate Guide to Cloud-Native SIEM

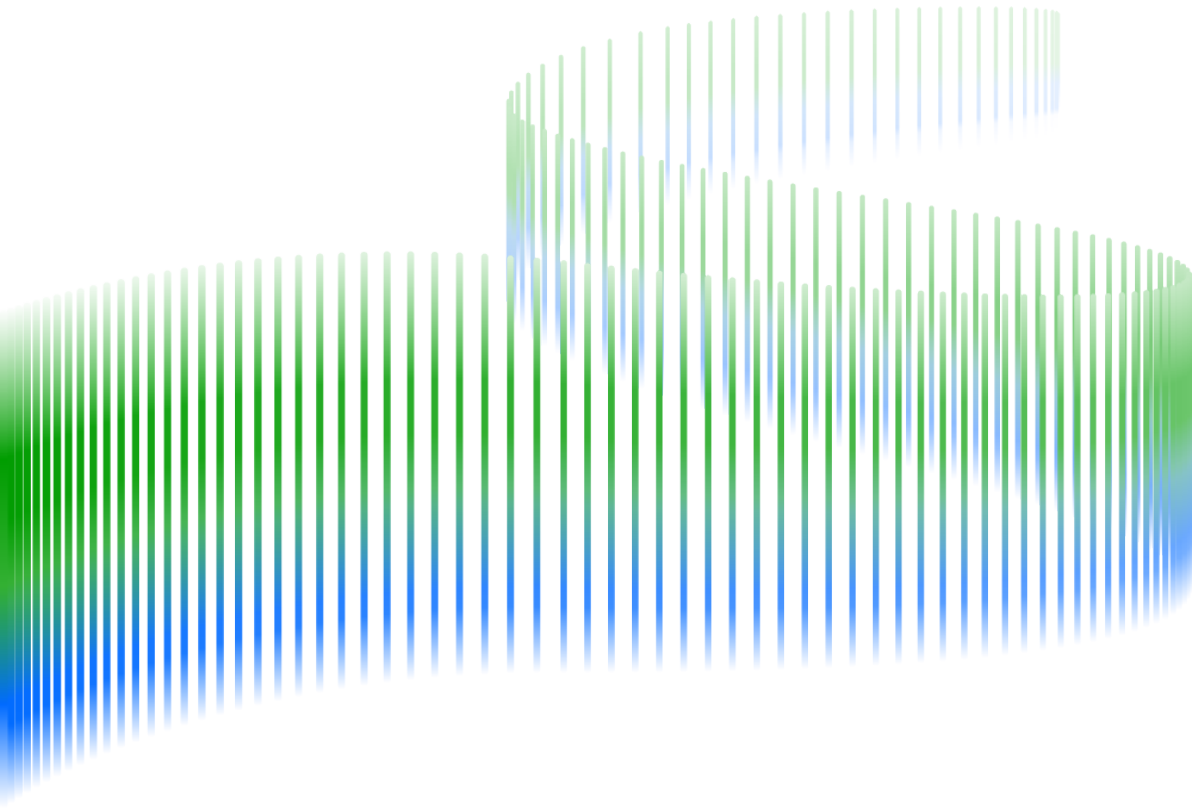


Table of Contents

Introduction

The role of security information and event management (SIEM) has evolved significantly over the last two decades. While traditional SIEMs have grown more powerful, they've also become harder to manage, slowing down threat detection, investigation, and response (TDIR) and overburdening already stretched security teams.

A modern, cloud-native SIEM changes that. Built for speed, scale, and simplicity, cloud-native SIEM platforms streamline log ingestion, correlation, investigation, and case management within a single interface. They reduce operational overhead, eliminate the need for complex infrastructure, and make it easier for analysts to focus on the highest-criticality threats.

Cloud-native SIEM makes it easy to bring in logs from on-premises systems, SaaS applications, cloud infrastructure, and third-party tools (even high-volume or newly adopted sources). Events are normalized at ingestion using a common information model (CIM), enabling consistent correlation across your environment. With full indexing in the cloud, search queries return results faster, helping analysts investigate incidents and find answers without delay.

Today's cloud-native SIEM must do more than manage logs. It must deliver precise detections, support real-time search and dashboards, and provide intelligent automation that helps analysts respond faster and security leaders demonstrate measurable value. When combined with self-tuning behavioral analytics and AI-driven triage, a cloud-native SIEM can surface high-risk threats while reducing noise and alert fatigue.

Organizations are rapidly shifting to hybrid and SaaS environments, adding complexity to data collection and correlation. Cloud-native SIEM makes it easier to ingest data from both on-premises and cloud-based systems, normalize it using a common model, and apply advanced analytics to uncover risks across the attack surface.

This guide explores how cloud-native SIEM supports modern security operations. You'll learn how it compares to legacy models, which features are most important, what to consider when evaluating vendors, and how to make the move from an on-premises deployment to a cloud-native solution. Whether you're modernizing your SOC or evaluating options for your next phase of growth, this guide will help you assess what's possible and how to get there.

What Does a SIEM Solution Do?

A SIEM solution collects, parses, and correlates log data from across your environment (cloud, on-premises, and third-party sources) to help your security team detect threats, investigate incidents, and meet compliance requirements. It centralizes alerts and events, applies detection logic, and creates a foundation for security operations.

SIEM plays a key role in threat detection, alert triage, incident response, forensic investigations, and audit preparation. It helps teams investigate historical events, reconstruct attack timelines, and demonstrate adherence to regulatory frameworks. But traditional, on-premises SIEMs lack the detection capabilities needed to identify modern threats at scale, leaving gaps that attackers can exploit. As data volumes grow (often into terabytes per day) and attack surfaces expand, these systems struggle with slow queries, limited analytics, and high overhead. Too often, they flood analysts with low-value alerts while missing real threats.

Security teams need a more efficient and effective approach that combines high-performance log management with behavioral analytics, automated workflows, and flexible deployment options.

What Is Cloud-Native SIEM?

Cloud-native SIEM delivers log management and TDIR, the core capabilities of SIEM, through a scalable, cloud-based platform. It's built to take advantage of the cloud's elasticity, speed, and lower operational burden.

Unlike retrofitted legacy systems, a true cloud-native SIEM can ingest and normalize logs at scale, support high-speed search, and apply behavioral models to surface anomalies and high-risk events. It provides unified visibility across cloud, hybrid, and on-prem environments and enables analysts to investigate incidents and manage cases through a single interface.

Cloud-native SIEMs that integrate AI and automation improve detection accuracy and accelerate response, helping teams reduce noise, close coverage gaps, and keep up with fast-moving threats.

Why Cloud-Native SIEM Is Needed

Many legacy SIEMs were originally designed as monolithic platforms that rely on proprietary software and fixed infrastructure. They were built to collect data, not to deliver precise threat detection at scale. As environments grow more complex and attackers more evasive, these legacy systems fall short, creating a growing gap between what SIEMs are expected to do and what they deliver.

This SIEM effectiveness gap has several causes:

- **Limited detection capabilities:** Most legacy SIEMs rely on static correlation rules and lack the analytics needed to detect threats like lateral movement or privilege escalation, especially when compromised credentials are involved.
- **High data volume, low context:** These systems often encourage collecting all data without filtering for relevance. The result is alert overload, with little context to support investigation or response.
- **Manual enrichment:** Most legacy SIEMs can't enrich data in motion. Context must be added after investigation, slowing down detection and increasing investigation effort.
- **Complex query languages:** Proprietary or specialized syntax limits usability. Many analysts are unable to fully leverage their SIEM without advanced skills or deep training.
- **Resource constraints:** Security teams face growing responsibilities with limited staff and budget. High storage and infrastructure costs make scaling difficult.

Cloud-native SIEM addresses these limitations with a modern architecture and built-in intelligence. It offers a faster, more flexible path to effective TDIR:

- **Modern data lake architecture:** Designed for scale, performance, and cost efficiency, cloud-native platforms ingest, index, and normalize large volumes of log data in real time.
- **Dynamic scalability:** Storage and compute scale automatically with your needs, without requiring manual sizing or architectural overhauls.
- **Integrated enrichment:** Data is enriched with context at the point of ingestion, making detections more precise and investigations more efficient.
- **Behavioral analytics and machine learning:** Self-tuning models baseline normal activity and highlight high-risk anomalies across users, devices, and entities.
- **Built-in automation:** Analysts gain speed and consistency with automated threat timelines, dynamic risk scoring, and AI-generated case summaries.
- **Fast content updates:** Detection logic and rule packs are updated in the cloud to keep pace with evolving threats.
- **Flexible delivery and management:** Cloud-native SIEM supports hybrid deployments and managed services models, enabling MSSPs and internal teams alike to scale efficiently.

Cloud-native SIEM delivers stronger detection, faster response, and better use of your team's time. From compliance reporting to threat hunting, cloud-native platforms bring critical threats into focus while automating routine investigation and response tasks.

For most security teams today, cloud-native SIEM represents the most practical, future-ready choice. It combines behavioral analytics, automation, and integrated threat detection in a single solution that scales with your environment and your team.

Cloud-Native SIEM Features and Capabilities

A modern, cloud-native SIEM helps organizations centralize event data across on-prem, hybrid, and cloud environments. It enables fast, flexible ingestion from different sources, including cloud apps, infrastructure, and endpoint tools, and normalizes that data to support real-time TDIR.

Cloud-native platforms are especially well suited for hybrid deployments, where visibility must span multiple clouds and data centers. They reduce infrastructure complexity, streamline operations, and support scalable detection programs with built-in intelligence.

Key capabilities of cloud-native SIEM include:

- **Centralized monitoring:** View integrated systems, workloads, and applications across cloud and on-prem environments through a unified interface.
- **Real-time alerting:** Correlate and score security events to generate high-fidelity alerts that prioritize meaningful security events.
- **Data management at scale:** Simplify data collection, storage, and normalization with a CIM and scalable data lake architecture.
- **Automated workflows:** Use AI agents and automation to generate case summaries, classify threats, and recommend next steps for response.
- **Threat timelines:** Automatically reconstruct security incidents with visual timelines that highlight key events, behaviors, and risk scores.

Cloud-Native Versus On-Premises SIEM

When deploying SIEM, organizations have a choice: run it on-premises or use a cloud-native platform managed by the vendor. Cloud-native SIEM removes the need for infrastructure provisioning and accelerates time to value, while also simplifying updates, scaling, and ongoing maintenance. Both options offer benefits, but they differ greatly in terms of flexibility, cost, and operational burden.

Cloud-native SIEM advantages:

- **Faster deployment:** Cloud-native SIEM can be deployed without provisioning hardware and vendors often assist with configuration and onboarding, so teams see value sooner.
- **Always up to date:** Detection rules, threat intelligence, and platform features are updated automatically without downtime or manual intervention.
- **Elastic scalability:** Log ingestion, storage, and compute scale dynamically as your needs grow, without needing to rearchitect or provision new hardware.
- **Lower operational burden:** With managed infrastructure, security teams can focus on improving coverage and reducing risk instead of maintaining systems.

Key considerations when comparing cloud-native and on-prem SIEM:

- **IT resources:** With two-thirds of companies reporting an IT skills shortage, cloud-native SIEM helps offload routine maintenance and tuning to the vendor or an MSSP.
- **Control and compliance:** On-premises SIEM may be preferred for sensitive or regulated environments that require local control. However, this comes with more upkeep, slower upgrades, and higher overhead.
- **Cost structure:** Cloud-native SIEM offers lower upfront costs and predictable subscription pricing, while on-premises deployments require larger capital investments and ongoing hardware maintenance. Upgrades and expansions are more complex and costly on-prem.
- **Data security in transit:** Moving data offsite introduces considerations around encryption and compliance. Reputable vendors offer strong protections for data in transit and at rest, including encryption and role-based access controls.
- **Access to raw log data:** Some vendors restrict access to raw logs unless you purchase additional storage. Look for a cloud-native SIEM that supports data lake architecture, enabling long-term storage, deep forensic analysis, and audit readiness.

Strategic Benefits of Cloud-Native SIEM

Massive Scale

Security data is growing faster than most on-premises SIEMs can manage. The rise of cloud applications, remote work, and connected devices has driven a sharp increase in log volume, and retaining only a subset of data limits visibility and weakens detection. Cloud-native SIEM leverages elastic compute and scalable storage, making it feasible and cost effective to ingest, store, and analyze more data across more sources.

With data lake architecture and built-in normalization, cloud-native SIEM enables organizations to retain full-fidelity log data, supporting forensic investigations, compliance audits, and deeper analytics. It also provides a unified view across hybrid environments, combining insights from cloud-native services, on-prem systems, and third-party tools.

Global organizations benefit from cloud infrastructure that supports region-specific storage and access controls. Role-based permissions, identity management, and data masking help enforce governance while ensuring that security teams can collaborate effectively across geographies.

Fast Deployment

Deploying an on-premises SIEM can take weeks or months. Cloud-native SIEMs can be up and running in a fraction of the time without waiting on hardware, manual provisioning, or patch cycles.

Prebuilt integrations, automated parser onboarding, and native support for cloud services speed up log ingestion and enable faster coverage across use cases. This reduces time to value and eliminates the friction of configuring rules or tuning data sources.

Faster Value, Lower Barriers

Legacy SIEMs often require specialized skills, extensive customization, and ongoing professional services. Cloud-native SIEM platforms remove many of those barriers. With built-in automation, user-friendly interfaces, and continuously updated content, teams can start detecting threats and responding to incidents faster without relying on SIEM engineers to manually manage indicators of compromise (IoCs), parser logic, or correlation rules.

Security teams can sign in, connect data sources, and start investigating within hours instead of weeks. This allows teams of all sizes to adopt advanced detection and response capabilities without the overhead of maintaining a complex on-prem stack.

Reduced Total Cost of Ownership (TCO)

Cloud-native SIEM shifts the economic model from upfront capital expenditure to predictable operating costs. There's no need to overprovision hardware or account for future scale; the platform grows with you.

Reduced staffing demands, fewer infrastructure dependencies, and automated updates further lower operational costs. At the same time, improved detection, faster triage, and more efficient response reduce the mean time to detect (MTTD) and respond (MTTR), which directly impact overall security performance and return on investment.

Automated Updates and Continuous Improvement

With legacy SIEM, staying current requires constant attention from SIEM engineers: evaluating updates, testing integrations, and planning upgrades. Even minor changes can introduce risk or delay.

Cloud-native SIEM removes that burden. The vendor handles maintenance, pushing new detections, integrations, and features directly into the platform. Updates roll out automatically and consistently across tenants, so you're always equipped to detect and respond to emerging threats, including zero-day exploits, without manual effort.

As new detection rules, playbooks and incident response checklists become available, they can be deployed immediately or tailored to fit your environment. Threat intelligence feeds are also continuously updated with new malicious IPs, domains, and IoCs, keeping your coverage current and your analysts focused on real threats.

Near-Real-Time Threat Detection

Modern SIEMs must operate at speed. With cloud-native infrastructure, detections happen in near real time, even at enormous scale. Events are parsed, enriched, and correlated as they're ingested, enabling immediate visibility into high-risk behavior.

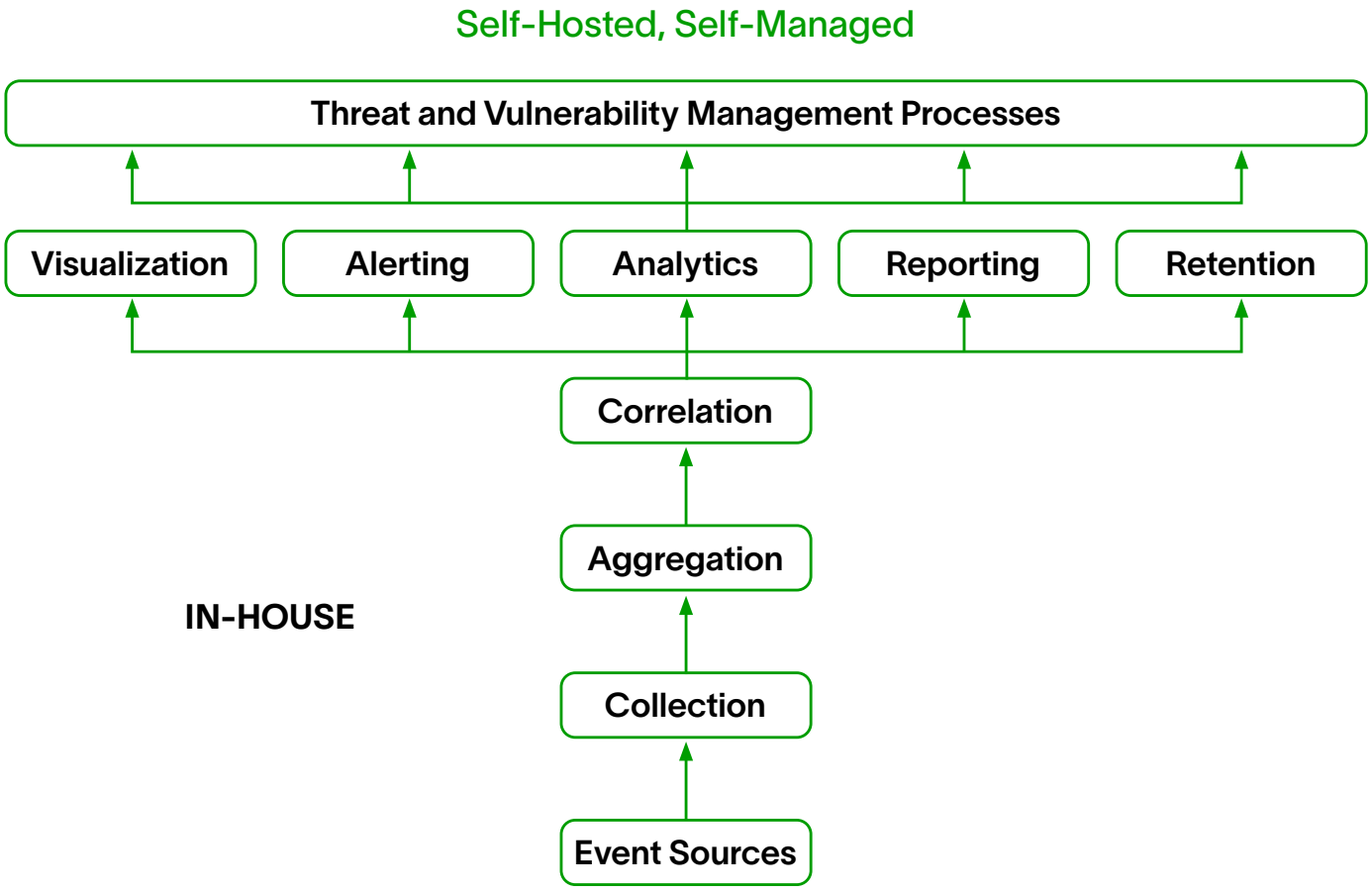
Unlike legacy systems that delay analysis to manage compute limitations, cloud-native SIEM enables live threat detection and case generation without introducing latency. Integrated search and investigation workflows provide instant access to relevant context, so analysts can respond faster and more confidently.

When deploying a SIEM, you can choose from a range of hosting and management models, each with different responsibilities for your internal team and the vendor or MSSP you partner with. The right choice depends on your existing infrastructure, security expertise, and operational priorities.

Which Cloud-Native SIEM Hosting Model Is Right for You?

When deploying a SIEM, you can choose from a range of hosting and management models, each with different responsibilities for your internal team and the vendor or MSSP you partner with. The right choice depends on your existing infrastructure, security expertise, and operational priorities.

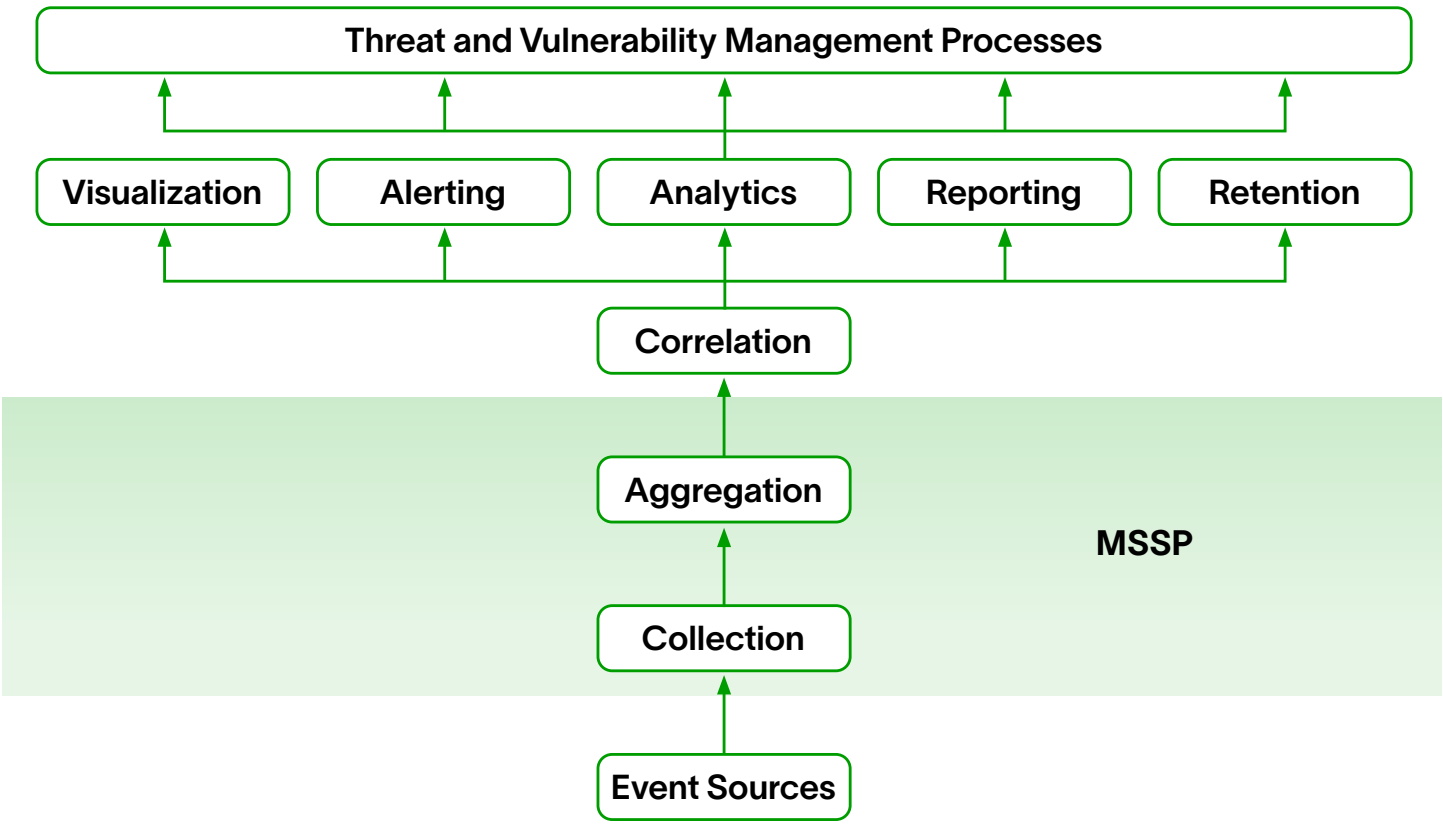
Deployment Models



This is the traditional SIEM deployment model. Your team is responsible for purchasing, deploying, and maintaining all software and hardware. You manage infrastructure, tuning, updates, and security operations in house. This approach offers full control but requires significant investment and a team with deep SIEM expertise.

You handle: All aspects of deployment, management, and operations

Cloud SIEM, Self-Managed

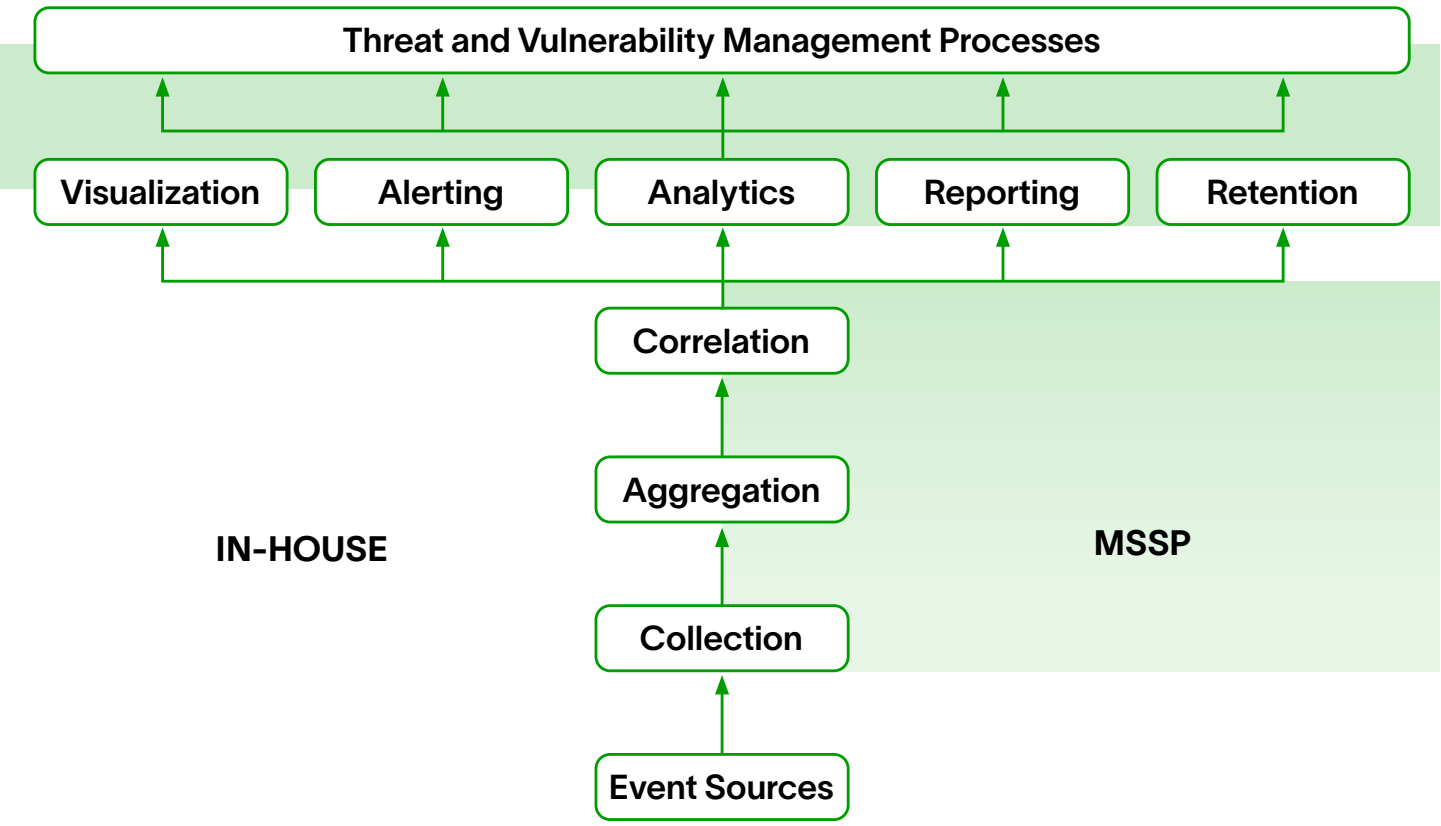


Your SIEM is hosted in the cloud, but your team manages the correlation, alerting, analysis, and dashboards. This model gives you the benefits of cloud scalability and flexibility while retaining operational control.

MSSP handles: Event ingestion and aggregation

You handle: Correlation, analysis, dashboards, and investigation workflows

Self-Hosted, Hybrid-Managed

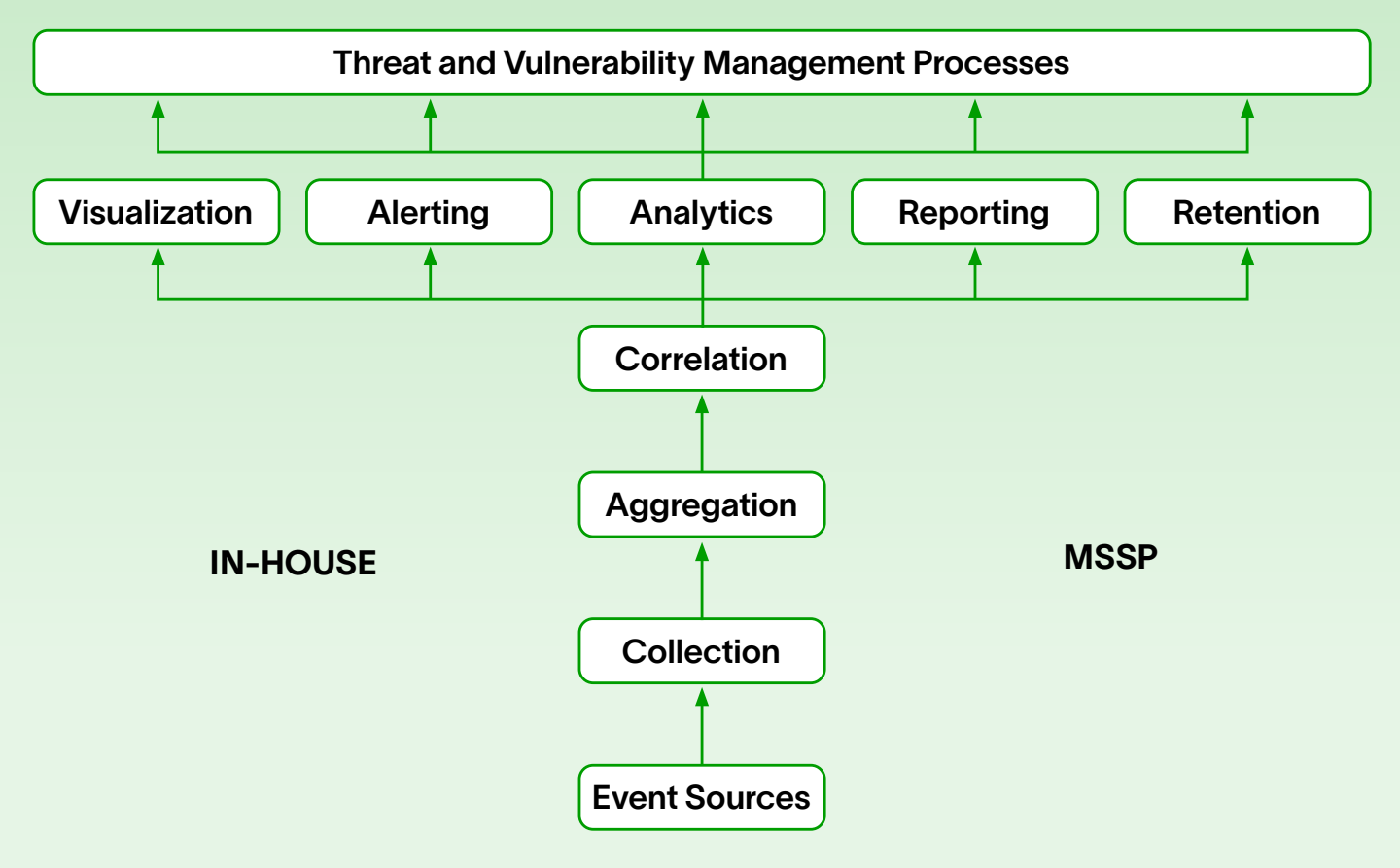


This model splits responsibility between your internal team and a trusted MSSP. Your organization hosts the platform and maintains infrastructure, while the MSSP helps manage detection content, event collection, and operational workflows.

You handle: Infrastructure purchase and ownership

MSSP and your team jointly manage: Collection, correlation, alerting, and dashboards

SIEM as a Service



In this fully managed model, your SIEM is delivered as a service. The vendor or MSSP manages infrastructure, data collection, threat detection, and reporting, allowing your team to focus on decision making and response.

Vendor/MSSP handles: Everything from ingestion to detection

You handle: Tuning inputs, reviewing alerts, and responding to threats

How to Choose

Consider the following when evaluating which model fits your needs:

- **Do you have existing SIEM infrastructure?**
  If you've already invested in hardware and software, a self-hosted or hybrid-managed model may make sense.
- **Can your organization move data off-premises?**
  If yes, a cloud-hosted or fully managed model reduces infrastructure burden and accelerates deployment.
- **Do you have trained SIEM staff?**
  If not, consider hybrid or fully managed models that provide expert support without the need to build in-house expertise.

Cloud-Native SIEM and International Regulation Compliance

Meeting regulatory obligations is a critical part of security operations, but many organizations still rely on fragmented tools and manual processes to prepare for audits. This approach increases the risk of non-compliance, fines, and reputational damage.

Modern cloud-native SIEM solutions help streamline compliance by offering prebuilt content aligned to common regulatory frameworks, such as:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act (SOX)

With preconfigured dashboards, reports, and detection rules, cloud-native SIEM can demonstrate that key controls are in place and function as expected. These capabilities reduce audit preparation time and improve confidence in compliance posture.

Data Residency and Privacy

Cloud-native SIEM solutions are typically deployed in global cloud infrastructure, giving organizations flexibility to meet data residency and sovereignty requirements. Leading providers offer support for regional hosting, multi-tenant isolation, and role-based access controls to help protect sensitive data.

If your organization must retain or process data in specific regions, choose a cloud-native SIEM that supports configurable data residency, encryption in transit and at rest, and compliance with jurisdiction-specific privacy laws.

Focus on Threat-Centric Use Cases

Migrating from an on-premises SIEM to a cloud-native platform affects multiple stakeholders across the organization. It's essential to engage business and technical leaders early in the process, especially those responsible for protecting critical assets, ensuring compliance, and driving IT-enabled outcomes.

PCI DSS Compliance

PCI DSS outlines security requirements for organizations that store, process, or transmit credit card data. Cloud-native SIEM supports PCI compliance by monitoring access, correlating security events, and simplifying reporting.

How cloud-native SIEM helps:

1. **Perimeter security:** Detect unauthorized network connections, monitor insecure protocols, and track activity across the DMZ.
2. **User identities:** Monitor changes to credentials and detect activity from terminated users.
3. **Real-time threat detection:** Analyze antivirus logs, detect insecure services, and enrich with threat intelligence.
4. **Production systems monitoring:** Identify use of default credentials or development/test systems in production environments
5. **Audit-ready reporting:** Collect and audit logs in formats that support PCI requirements and simplify report generation.

GDPR Compliance

GDPR governs how organizations collect, process, and protect the personal data of EU citizens. Cloud-native SIEM provides visibility and traceability across data systems, helping teams detect breaches and demonstrate compliance.

How cloud-native SIEM helps:

1. **Data protection by design:** Audit and verify security controls applied to personal data.
2. **Visibility into log data:** Provide clear visibility into logs and data processing activities
3. **GDPR-specific auditing:** Track credential changes, security group access, and systems storing personally identifiable information (PII).
4. **Breach detection and notification:** Detect and report data breaches with timelines and detailed summaries
5. **Data processing records:** Identify and report on data handling activities across systems.

Note: Log data may contain PII. Under GDPR Article 6, log retention is allowed for "legitimate interest," such as security operations. Always consult legal counsel and ensure your SIEM provider supports data masking and role-based access.

HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) sets data privacy and security requirements for healthcare organizations. Cloud-native SIEM supports HIPAA compliance by automating monitoring, detecting violations, and documenting system access and activity.

How cloud-native SIEM helps:

1. **Asset discovery and risk analysis:** Identify new systems and access to critical health data.
2. **Access monitoring:** Track logins, especially from terminated users or privileged accounts.
3. **Account management:** Monitor privilege escalation and user modifications.
4. **Vulnerability detection:** Identify systems lacking antivirus or showing signs of compromise
5. **Incident response:** Detect, prioritize, and automate threat response.
6. **Access control enforcement:** Track changes to credentials, timeouts, and encryption settings.
7. **Audit controls:** Monitor DLP events, file integrity, and policy changes.
8. **Data integrity:** Detect unauthorized modifications to health records.
9. **Transmission security:** Identify unauthorized data transfers or system tampering.

SOX Compliance

SOX requires U.S. public companies to maintain strict data access and accountability standards. Cloud-native SIEM helps demonstrate internal control over IT systems by tracking user activity, access controls, and data changes.

How cloud-native SIEM helps:

1. **Policy and standards monitoring:** Track violations of security policies or IT standards in real time.
2. **Access and identity auditing:** Monitor account creation, change requests, and activity from terminated users.
3. **Network security monitoring:** Detect known threats and suspicious activity across network devices.
4. **Log monitoring and alerting:** Aggregate events and alert on risky behaviors such as failed logins and privilege escalation.
5. **Enforcing segregation of duties:** Ensure appropriate access controls and separation of responsibilities in critical workflows.

Using SIEM to Detect Insider and Trusted Entity Threats

Threats from trusted users and systems remain some of the hardest to detect. Whether intentional, negligent, or the result of compromised credentials, insider activity often falls outside the scope of traditional detection methods that rely on static rules or signatures.

Insider Threats

- **Malicious insiders:** Individuals who intentionally misuse their access to steal data, sabotage systems, or cause harm
- **Negligent insiders:** Employees or contractors who unintentionally expose sensitive data or systems through carelessness or lack of training
- **Compromised insiders:** Legitimate users whose accounts or devices have been taken over by an attacker to move undetected through the environment

Modern SIEM solutions help detect these threats by applying behavioral analytics to user and entity activity. By establishing baselines of normal behavior and continuously evaluating deviations, these systems can surface high-risk actions, such as unusual access times, abnormal privilege escalation, or atypical data movement, which may indicate an insider threat.

Rather than relying solely on predefined rules, these systems use dynamic risk scoring and behavior modeling to prioritize the most relevant threats, helping analysts focus their time on the incidents most likely to cause harm.

Six Ways Cloud-Native SIEM Can Help Mitigate Insider Threats

1. **Detecting compromised credentials:** Behavioral baselining helps detect when a legitimate account is used in unexpected ways like logging in at unusual hours, from new locations, or accessing unfamiliar systems. These deviations often indicate compromised credentials, even when no alerts are triggered by traditional tools.
2. **Identify privilege escalation:** Unauthorized or suspicious changes to account privileges—especially on sensitive systems—can signal internal misuse or preparation for broader access. Cloud-native SIEM platforms track baseline privilege behavior and alert on anomalies.
3. **Spot command and control activity:** By correlating outbound traffic with known IoCs, a cloud-native SIEM can flag covert communication between internal systems and external infrastructure controlled by attackers. This is often the first clue that an insider account has been compromised.
4. **Detect data exfiltration attempts:** Indicators of data theft, such as unusual file downloads, USB device use, unauthorized cloud storage access, or excessive printing, often appear unrelated in isolation. Behavioral analytics link these low-level signals to expose a broader exfiltration pattern.
5. **Stop rapid encryption:** High-volume file encryption is a common sign of ransomware, which often enters through compromised insider accounts. Real-time anomaly detection can flag this behavior early and trigger response workflows to contain the threat.
6. **Trace lateral movement:** Insiders moving across systems, accounts, or network segments may be exploring or staging an attack. By correlating sessions across users, devices, and IP addresses, cloud-native SIEM tools can detect and visualize lateral movement before damage occurs.

Next-Gen SIEM: Behavior Intelligence Built In

Traditional SIEM tools are limited by their reliance on manually created rules and predefined correlation logic. These approaches struggle to detect advanced threats that don't follow known patterns—particularly credential-based attacks, lateral movement, and insider misuse.

Next-generation SIEM platforms incorporate behavioral analytics, machine learning, and automated investigation capabilities to address these gaps. These platforms:

- Build dynamic baselines to understand normal user and system behavior, allowing them to detect deviations in real time.
- Apply risk scoring to prioritize alerts based on context, frequency, severity, and the role or sensitivity of the affected asset.
- Automate threat timelines and evidence collection, reducing manual effort and accelerating the investigation process.
- Adapt over time, using self-tuning detection models that evolve as the environment and behaviors change.

This combination of behavioral insight, automation, and contextual analysis enables more accurate detection and faster response, especially for threats that don't trigger obvious alerts in traditional tools.

Privileged Access Abuse

Privileged access abuse is one of the most dangerous and difficult to detect insider threat scenarios. It often stems from excessive or unmonitored access rights, leaving organizations vulnerable to misuse, error, or compromise. Cloud-native SIEM platforms help reduce this risk by continuously monitoring behavior, surfacing anomalies, and alerting on potential abuse.

Five Ways Cloud-Native SIEM Can Help Stop Privileged Access Abuse

1. Suspicious access to sensitive data: Monitor and alert on access attempts that fall outside a user's typical behavior, such as viewing confidential files, accessing restricted systems, or running privileged commands.
2. Third-party violations: Track activity by vendors, contractors, or partners with elevated access. Behavioral analytics help identify unauthorized escalation or unusual patterns that may signal misuse.
3. Terminated or inactive account activity: Detect and flag any actions taken by accounts that should no longer be in use, especially accounts belonging to former employees or service accounts that typically remain idle.
4. Risky or unintended changes: Spot anomalous behavior that could indicate a critical error, such as mass file deletion, unexpected configuration changes, or sudden system modifications.
5. Overexposure and access drift: Identify users whose access has grown beyond their role. Behavioral monitoring helps detect when someone begins interacting with systems or data outside their normal scope of activity

Trusted Host and Entity Compromise

Attackers often operate undetected by compromising trusted user accounts, servers, or network infrastructure, sometimes for months at a time. Detecting this kind of long-term, low-and-slow activity requires continuous behavioral monitoring and context-aware analysis. Cloud-native SIEM platforms alert security teams to subtle anomalies that may indicate compromise early before damage is done.

Four Ways Cloud-based SIEM Can Help Detect and Stop Trusted Entity Compromise

1. **User accounts:** Identify anomalies in login behavior, access patterns, or privilege use that may indicate a compromised account. See high-risk events and provide investigators with a full timeline of user activity for faster triage and response.
2. **Servers:** Establish baselines for normal server behavior and alert on deviations like unexpected processes, unapproved access, or off-hours activity, which may signal attacker presence.
3. **Network devices:** Monitor network traffic over time to detect unusual patterns, spikes, or communication with known bad IPs. Identify the use of insecure protocols, unexpected lateral movement, or access attempts from non-trusted sources.
4. **Endpoint and antivirus monitoring:** Track changes across endpoint protection systems, including alerts when antivirus is disabled, removed, or out of date. Correlate these signals with other events to determine if a host has been intentionally weakened or compromised.

Using Cloud-Native SIEM For Advanced Security Threat Detection

Threat Hunting

Threat hunting is the practice of proactively searching for threats that evade automated detection. While some hunts begin after an incident, others are initiated based on suspicion, intelligence, or known vulnerabilities. Effective threat hunting requires broad access to security data, fast search performance, and contextual analysis—all strengths of cloud-native SIEM.

Seven Ways Cloud-Native SIEM Can Help With Threat Hunting

1. **Alert-driven investigation:** Get actionable alerts enriched with context and risk scores, letting analysts pivot quickly into deeper investigation.
2. **Environmental anomalies:** Detect deviations from established behavioral baselines and correlate unusual patterns across users, systems, and network traffic.
3. **Vulnerability-centered analysis:** Organize activity around newly disclosed vulnerabilities by identifying affected assets, timelines of exposure, and potential exploitation.
4. **External tips and threat reports:** Search historical logs for tactics, techniques, or indicators associated with peer-reported breaches or high-profile attack campaigns.
5. **Integrated threat intelligence:** Enrich log data with threat intelligence feeds to detect known IoCs and identify patterns consistent with known adversaries.
6. **Hypothesis testing:** Support structured hunting by allowing analysts to frame and test hypotheses, for example, "Has this behavior happened before in this subnet or region?"
7. **Incident pattern matching:** Compare new activity to known incidents by searching for repeat patterns or similar behavior across time, users, or systems.

Data Exfiltration Detection

Data exfiltration occurs when sensitive information is transferred outside of an organization's control, whether intentionally or not. This can happen manually through unauthorized uploads, USB transfers, or email forwarding, or automatically through malware and command-and-control activity. Cloud-native SIEM platforms help detect early signs of exfiltration by correlating signals across users, endpoints, networks, and cloud services.

Six Ways Cloud-Native SIEM Can Help Prevent Data Exfiltration

1. **Backdoors, rootkits and botnets:** Monitor outbound traffic for connections to known command-and-control infrastructure or suspicious destinations. Identify anomalies in communication patterns that may indicate data leakage from infected systems.
2. **FTP and cloud storage usage:** Track activity over high-volume data transfer protocols like FTP, SCP, or public cloud storage services, and alert on unusual file types, volumes, or destinations not associated with normal workflows.
3. **Web application activity:** Analyze interactions with internal and external web applications, detecting unapproved downloads, sensitive data exposure, or browser-based access from unexpected locations or identities.
4. **Unauthorized email forwarding:** Alert on emails sent or forwarded to unrecognized domains, including automatic forwarding rules that could be used to bypass traditional DLP controls.
5. **Lateral movement before exfiltration:** Identify behaviors associated with reconnaissance and staging, such as access across multiple systems or privilege escalation, which may indicate preparation for large-scale data theft.
6. **Mobile device misuse:** Monitor activity from mobile endpoints, including remote access behavior, unusual data transfers, or geographic anomalies that may suggest information leakage through mobile channels.

IoT Security

As more organizations rely on connected devices to power operations across industries like healthcare, manufacturing, energy, and critical infrastructure, the security risks associated with IoT continue to grow. Many IoT devices lack built-in security controls, run outdated firmware, and are difficult to patch once deployed. Monitoring these systems through a cloud-native SIEM helps detect threats early and enforce control over high-risk behavior.

Six Ways Cloud-Native SIEM Can Help Mitigate IoT Threats

1. **Denial-of-service (DoS) attacks:** Detect abnormal traffic patterns originating from IoT devices that may be participating in or targeted by a DoS attack. Apply automated responses to block or contain the behavior based on defined thresholds or risk conditions.
2. **IoT vulnerability exposure:** Identify outdated operating systems, unpatched firmware, or insecure protocols in use on IoT devices. Highlight gaps in patch coverage that increase the attack surface.
3. **Access control violations:** Monitor login activity and connectivity to and from IoT systems. Alert on access attempts from unrecognized sources or when devices connect to unknown or high-risk destinations.Unusual data flows: Track inbound and outbound data movement to detect unexpected communication between IoT devices and other systems, especially large transfers or communication to the public internet.
4. **At-risk devices:** Identify devices with access to sensitive data, control functions, or safety-critical systems. Prioritize these assets for monitoring based on their risk profile and operational importance.
5. **Compromised behavior:** Detect deviations from normal device activity, including spikes in network use, unauthorized commands, or behavioral patterns that may indicate compromise or misuse.

Migrating to a Cloud-Native SIEM

Migrating from an on-premises SIEM to a cloud-native platform affects multiple stakeholders across the organization. It's essential to engage business and technical leaders early in the process, especially those responsible for protecting critical assets, ensuring compliance, and driving IT-enabled outcomes.

Migrating to a Cloud-Native SIEM

Identify and Prioritize Critical Assets and Use Cases

Begin by identifying the data, systems, and processes that are essential to your business. These typically include:

- Intellectual property (IP)
- Customer and financial records
- Employee data
- Core business applications
- Network infrastructure
- Security and monitoring tools

Your organization's risk management framework should guide the prioritization of assets and use cases during migration. Compliance obligations—such as GDPR, HIPAA, PCI DSS, or SOX—may also dictate which components need to be addressed first.

Involve senior stakeholders early in the process. Their responsibilities often tie directly to business continuity, regulatory alignment, and data protection, making their input critical to a successful transition plan.

Migration Doesn't Mean Starting Over

A full replacement of your existing SIEM isn't always necessary. Many organizations begin by augmenting their current platform with cloud-native capabilities such as behavioral analytics, automated threat detection, or faster investigation workflows. Others take a phased approach, running the new SIEM alongside their legacy system before a full cutover. Timing considerations like contract renewals, infrastructure refresh cycles, or audit schedules can help determine the right path.

Plan for Your Destination

Whether you're moving to a SaaS SIEM, public cloud deployment, hybrid model, or managed service, it's important to define the target environment early. Each option brings tradeoffs in cost, scalability, control, and support. Consider how your team will manage data flow, retention, and access in the new model.

Cloud-to-cloud migrations are also becoming more common as teams move away from first-generation cloud-hosted SIEM or log management tools toward modern platforms that offer improved scalability and integrated threat detection. These migrations often focus on gaining access to advanced capabilities—like UEBA, machine learning, or automated response—while reducing operational overhead.

Key steps may include:

- Reconnecting cloud-native data sources (for example, AWS, Azure, Google Workspace)
- Recreating correlation rules, dashboards, and alerts
- Migrating to a modern data lake architecture for long-term search and retention

Project Plan

Set Clear Expectations and Project Scope

Before beginning the transition, your security operations team should review current requirements, including supported log sources, use cases, access controls, and reporting needs. Transition timeframes vary by environment, but many organizations complete initial migrations in seven to eight weeks.

Factors that may affect your timeline include:

- Unsupported or legacy log formats
- Scope of custom detections or reporting
- Staffing availability and resource planning

Thoughtful preparation will help avoid gaps in visibility, coverage, or compliance and ensure a smoother path to operationalizing your new SIEM.

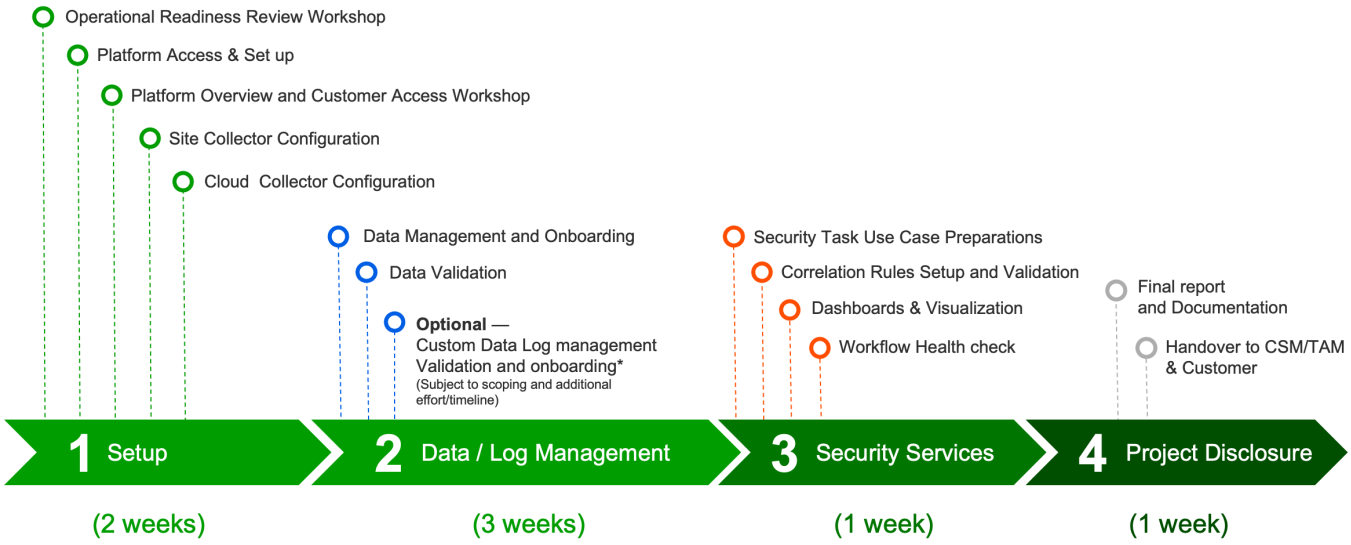


Figure 1. A typical cloud-native SIEM implementation includes four phases and takes 7–8 weeks.

Transition Steps

Step 1: Setup

(Estimated Duration: Two Weeks)

Operational Readiness Review (ORR)

Begin the transition with an operational readiness review to align your security goals with specific platform capabilities and use cases. This step validates the scope of the deployment, confirms technical requirements, and ensures all stakeholders understand the intended outcomes. The ORR also surfaces critical organizational details, such as compliance needs, integration dependencies, and user roles, that guide adoption and configuration efforts.

Platform Access and Environment Preparation

Once access is granted, your deployment engineer or implementation team will verify that licensed features are available and functioning. This typically includes provisioning tenant environments, confirming permissions, and walking through the basic platform interface and navigation with your security team.

Collector Configuration

Configure cloud or site-based log collectors to begin ingesting data from your prioritized SaaS, cloud, and on-premises sources. Common integrations may include:

- **Cloud platforms:** AWS, Azure, GCP
- **Collaboration and file sharing:** Office 365, Google Workspace, Box, Dropbox
- **Identity providers:** Okta, Duo, OneLogin
- **Security tools:** Cisco AMP, CrowdStrike, Proofpoint
- **Business systems:** Salesforce, ServiceNow, GitHub

Collector setup ensures security events and log data are normalized and available for detection, investigation, and reporting from day one.

Step 2: Data and Log Management

(Estimated Duration: Three Weeks)

Data Onboarding and Validation

In this phase, scoped data sources are connected, and logs begin flowing into the platform. Your implementation team should validate the ingestion pipeline to ensure that:

- Log sources are active and generating events as expected
- Parsed fields are correctly extracted and mapped
- The platform's data pipeline is functioning reliably and at scale

Successful onboarding includes confirming that each source aligns with the defined detection use cases and compliance requirements. Consistent data normalization at this stage is critical to enable accurate detection, efficient investigations, and reliable reporting later in the deployment.

Step 3: Security Services

(Estimated Duration: One Week)

This phase focuses on aligning detection, visibility, and investigation workflows with your organization's priorities as defined during the ORR.

Correlation Rule Implementation and Validation

Configure and validate prebuilt and custom correlation rules to support priority use cases such as malware detection, credential compromise, or unauthorized access. This helps your security operations team understand how detections are triggered, what actions follow, and how alerts are prioritized within the platform.

Dashboard and Visualization Setup

Verify that default dashboards and visualizations are operational and providing value to security analysts. Most cloud-native SIEM platforms support customization and export functionality, enabling teams to tailor dashboards for specific roles or reporting requirements and share findings in PDF format as needed.

Workflow Health Check

Confirm that security alerts and correlation outcomes are flowing through the system as expected. Ensure they appear in the appropriate dashboards, queues, or case management areas, so analysts can act on them efficiently.

Step 4: Project Closure

(Estimated Duration: One Week)

Final Report and Documentation

To formally close the deployment project, the implementation team should deliver a final report outlining the completed activities, key configurations, and any outstanding items. This documentation typically includes:

- Summary of deployment phases and milestones
- Configured data sources, collectors, and correlation rules
- Dashboards and reports implemented
- Validation outcomes and system health status
- Recommendations for next steps or ongoing optimization

The report should be reviewed in a closure meeting with stakeholders to confirm alignment, answer final questions, and ensure a smooth transition to steady-state operations or managed services.

Post-Transition Activities

After initial deployment, several follow-up activities help validate performance, build analyst confidence, and prepare for long-term operational success.

Run in Parallel for Validation

It's recommended to operate the cloud-native SIEM alongside your existing on-premises SIEM for at least 30 days. This parallel run allows your team to compare results, verify detection accuracy, and confirm data integrity across both platforms. Any discrepancies can highlight configuration gaps, parsing issues, or detection logic that needs adjustment.

Review Case Outcomes and Use Case Coverage

At the conclusion of the implementation, review a sample of generated cases to assess alignment with your intended use cases. Look for gaps in alert quality, context, or automation that may require tuning. This is also a good time to use any available coverage analysis tools to identify weak areas and plan follow-up improvements.

Prepare Reports for Compliance and KPIs

Set up reporting workflows to meet compliance obligations and track key performance indicators (KPIs). These reports may include:

- Use case coverage and detection effectiveness
- Compliance frameworks, including PCI DSS, HIPAA, NIST, and ISO
- Vendor-specific logs such as Cisco, VPN platforms and Symantec
- SOC performance metrics like MTTD and MTTR

Ensure your reporting environment supports export, filtering, and scheduling to simplify regular reviews and audit preparation.

Transition Detection Rules and Build Search Proficiency

As your team shifts to the new platform, analysts will begin crafting searches and writing queries for threat hunting, investigations, and reporting. This often requires familiarity with:

- The platform's query language and syntax
- Logical operators and search structure
- Relevant data sources and how they are parsed
- Mapped use cases and expected outcomes
- Where to find documentation or support resources

Providing hands-on training or structured query examples can reduce the learning curve and help analysts build confidence more quickly.

Additional Considerations When Evaluating Cloud-Native SIEM

Choosing a cloud-native SIEM involves more than assessing core functionality. It's important to evaluate how the platform aligns with your organization's operational, security, and compliance requirements—both during onboarding and over the long term.

When evaluating potential solutions, consider asking the following:

1. **Deployment and Data Residency**
   - Where is the platform hosted and where will your data reside?
   - Can the vendor meet your organization's data residency or sovereignty requirements?
2. **Data Protection and Privacy**
   - How is your data protected in transit and at rest?
   - What encryption and access control mechanisms are in place?
3. **Scalability and SaaS Delivery**
   - Does the solution offer true SaaS benefits such as elastic scaling and reduced administrative burden?
   - How easy is it to manage data ingestion and retention?
4. **Data Collection and Transport**
   - How is data collected from on-premises, cloud, and third-party sources?
   - Are collectors lightweight, secure, and configurable to your environment?
5. **Network Impact**
   - What is the expected impact on bandwidth or internet usage, particularly during peak periods?
6. **Upgrade Cadence and Quality Assurance**
   - How frequently are new features or updates released?
   - What testing and validation processes are in place to maintain platform availability and stability?
7. **Security Technology Support**
   - How well does the vendor support integrations across identity, endpoint, cloud, and network security tools?
   - Are there prebuilt connectors and support for custom sources?
8. **Licensing and Usage Transparency**
   - Is the pricing model usage-based or tiered?
   - Can you easily monitor your consumption and adjust entitlements as needed?
9. **Platform and Source Health Monitoring**
   - How does the platform ensure availability and detect issues with log sources, collectors, or parsers?
10. **Data Ownership and Offboarding**
    - If the agreement ends, do you retain full access to your data?
    - What options exist for data export or migration?

New-Scale SIEM

New-Scale SIEM is a cloud-native SIEM built for scale, speed, and analyst productivity. It combines modern log management, behavioral analytics, and case management in a unified platform, now enhanced with agentic and generative AI through Exabeam Nova.

Key Capabilities

- **Cloud-scale log management:** Collect and enrich data from across your environment, including on-premises systems, SaaS platforms, cloud infrastructure, and security tools. Ingest, normalize, and store petabytes of data with fast search across years of logs.
- **Unified threat detection and response workbench:** A centralized, analyst-friendly interface for detection, investigation, and response. Analysts can move from alert to case in a single view, streamline workflows, and reduce time to resolution.
- **Behavioral analytics and risk scoring:** Use machine-learned behavior baselines to detect credential-based threats, lateral movement, and privilege misuse. Dynamic risk scoring prioritizes the highest-risk activity, aligned to adversary tactics in the MITRE ATT&CK® framework.
- **Automated investigations:** Exabeam Nova AI agents help analysts work faster and more effectively by generating threat timelines, summarizing case details, building visualizations, and suggesting next steps. Investigations that once took hours can now be completed in minutes.
- **Use case coverage:** Map detections to common attack techniques and frameworks to evaluate coverage and identify gaps. Outcomes Navigator helps teams align security operations with their priorities, whether that's insider threat detection, ransomware defense, or regulatory compliance.

Exabeam Nova: AI Agents by Role

Exabeam Nova is a coordinated system of six AI agents, each specialized for a specific SOC function:

Search Agent: Enables natural language querying across log sources and languages, helping analysts find relevant data without complex syntax.

Visualization Agent: Builds charts, dashboards, and visualizations based on analyst queries or case context to improve clarity and communication.

Advisor Agent: Summarizes posture, ATT&CK coverage, and outcomes in leadership-ready reports to support executive decision-making.

Threat Scoring Agent: Applies adaptive, behavior-informed risk scoring to help prioritize relevant events and reduce alert fatigue.

Investigation Agent: Automatically generates threat timelines, classifies activity, and suggests next steps—speeding up analysis and resolution.

Analyst Assistant Agent: Offers real-time, case-specific guidance during investigations to help analysts work faster and more accurately.

Together, these agents reduce manual effort, improve consistency, and facilitate faster detection, triage, and response coverage.

Cloud-Native Security Log Management

New-Scale SIEM is a cloud-native platform built to collect, normalize, and analyze log data from cloud services, on-premises infrastructure, and third-party tools. It simplifies log management while enabling real-time detection, investigation, and response.

At the core of New-Scale SIEM is Threat Center, a unified workbench that centralizes detection, search, investigation, and case management. Threat Center includes:

- Over 180 prebuilt correlation rules for identifying credential misuse, lateral movement, and other high-risk behaviors
- Integrated threat intelligence to provide enriched context
- Real-time dashboards and fast, intuitive search
- Automated evidence collection, tagging, and a built-in ticketing system designed specifically for SOC workflows

With support for more than two million events per second (EPS), New-Scale SIEM scales to meet the demands of large enterprises. Long-term storage and fast historical search enable deep forensic investigations, while embedded guidance helps teams strengthen their detection posture over time.

AI enhances the entire process. Exabeam Nova agents help analysts write queries in plain language, summarize investigations automatically, and recommend next steps without requiring manual tuning or custom scripting.

Whether you're reviewing detection coverage or investigating suspicious activity, New-Scale SIEM delivers the speed, clarity, and context your team needs to respond effectively.

Cloud-Scale Visibility

Achieving meaningful detection and response starts with complete visibility. New-Scale SIEM helps you assess data source coverage, configuration quality, and parsing accuracy so you can identify and close gaps that impact your security outcomes.

Built for security teams, not general-purpose logging, New-Scale SIEM delivers fast, scalable log management with a modern experience your analysts can use without extensive training. Built-in recommendations highlight which data sources, event streams, and parsers will improve detection coverage and response speed, removing guesswork from log onboarding and tuning.

Advanced Correlation Capabilities

New-Scale SIEM simplifies the process of building and operationalizing detections. Analysts can convert any search into a correlation rule in a single step, streamlining the path from investigation to continuous monitoring.

The Correlation Rules app allows teams to write, test, and publish custom rules to detect known threats and anomalous behavior within their environment. Rules can be assigned higher criticality based on supporting context, such as threat intelligence or behavior mapped to adversary techniques.

Analysts can monitor rule performance, fine-tune logic, and adapt detection strategies as new risks emerge, all within a centralized and easy-to-use interface.

Automation Management

Automation Management in New-Scale SIEM helps security teams streamline alert triage and accelerate response through customizable, rule-based workflows. It enables analysts to focus on high-value tasks by automating repetitive steps in the detection and investigation process.

With Automation Management, teams can:

- Ingest alerts from Exabeam and third-party tools
- Define conditions to enrich, escalate, or suppress alerts based on priority and context
- Apply tags, assign incidents, and route tasks automatically
- Guide analysts through structured, outcome-based workflows
- Integrate with ITSM and external ticketing systems through prebuilt actions and APIs

These automation rules help standardize response, improve consistency, and reduce manual effort without compromising flexibility. As new threats and requirements emerge, rules can be quickly updated to reflect changes in your environment or processes.

Behavioral Analytics

New-Scale SIEM includes advanced behavioral analytics to detect threats that bypass traditional rule- and signature-based tools. Built on the cloud-native New-Scale Security Operations Platform, it delivers full visibility into user and entity activity and applies machine learning to identify anomalies indicative of insider threats, credential compromise, and lateral movement.

Behavioral models establish baselines for normal behavior and assign dynamic risk scores to deviations, enabling early detection of high-risk activity. These detections are mapped to tactics in the ATT&CK framework and integrated directly into investigation workflows.

The platform provides real-time dashboards to monitor system health, uptime, and data flow. Actionable recommendations help teams continuously improve security posture by identifying opportunities to optimize event streams, refine parsers, and expand detection coverage over time.

Normalize Data With a Common Information Model

Security data arrives in many formats, often with inconsistent fields and structures. The Exabeam CIM standardizes how logs are parsed, stored, and interpreted, enabling reliable correlation, streamlined parser maintenance, and consistent detection logic across data sources.

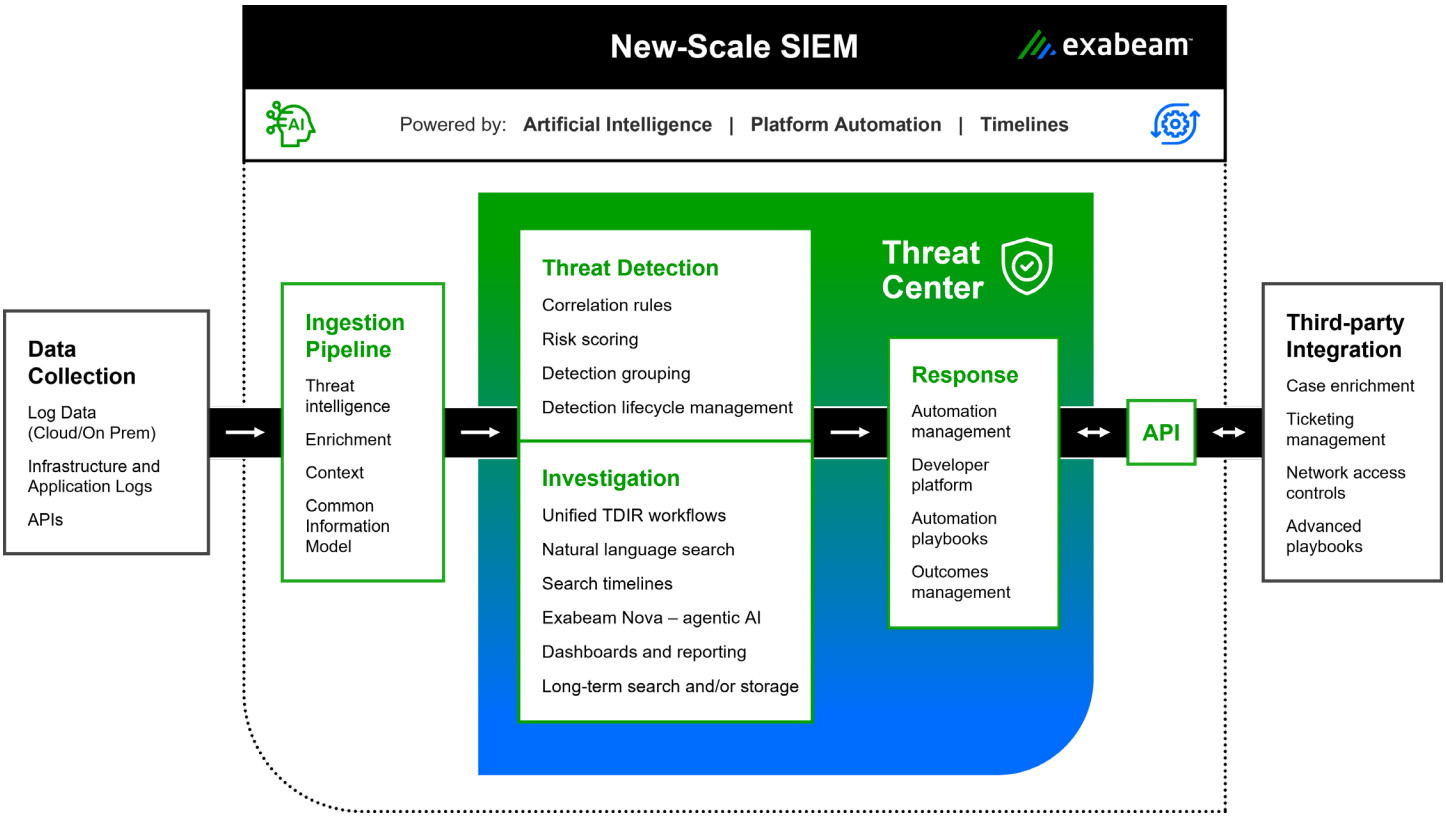


Figure 2. Exabeam Fusion, the New-Scale Security Operations Platform, powers New-Scale SIEM.

Get Started With Exabeam

Whether you're replacing a legacy SIEM or enhancing an existing deployment, the modular New-Scale Platform gives your team a faster path to stronger outcomes. Add advanced capabilities such as behavioral analytics, automation, and TDIR workflows to your current tools or as part of a full transition.

New-Scale Analytics

New-Scale Analytics is a cloud-native solution for collecting, normalizing, storing, and searching security data all within a fast, intuitive interface designed for security operations teams.

It delivers scalable, affordable log management with:

- Modern search and dashboarding that provides near-instant results, even over petabytes of data
- Cloud-native performance that eliminates the need for complex infrastructure or tuning
- Normalized data at ingestion for consistent detections and simplified parser maintenance
- Flexible, modular deployment that allows you to start with log management and expand to full TDIR capabilities

With New-Scale Analytics, your team can investigate threats, monitor system activity, and meet compliance requirements without learning complex query languages or managing infrastructure. It's the ideal starting point for organizations looking to modernize their security operations with scalable, cloud-native log management.

SIEM Replacement With New-Scale SIEM and New-Scale Fusion

Exabeam offers a modular approach to SIEM modernization, allowing organizations to replace legacy systems with cloud-native speed, scale, and automation without sacrificing flexibility.

New-Scale SIEM delivers advanced detection, investigation, and response capabilities. It includes:

- A centralized interface for detection, search, case management, and response
- Integrated threat intelligence and adaptive risk scoring
- Dynamic dashboards, automated timelines, and real-time investigation guidance
- Sustained performance at more than two million EPS

New-Scale Fusion combines New-Scale SIEM and New-Scale Analytics to form the full Exabeam New-Scale Security Operations Platform. It adds:

- Behavioral analytics to detect insider threats, credential misuse, and lateral movement
- Exabeam Nova for AI-assisted search, investigation, and response
- Automation Management to streamline alert triage and orchestrate response workflows
- Outcomes Navigator to improve detection coverage

SIEM Augmentation With New-Scale Analytics

New-Scale Analytics gives organizations the ability to enhance detection and investigation without replacing their existing SIEM. It integrates with third-party SIEMs and data lakes to provide high-performance search, machine-learned detection, and automated investigation workflows, addressing common gaps in speed, visibility, and context.

As a modular solution, New-Scale Analytics can ingest and normalize security data using the Exabeam CIM, improving detection quality and consistency. Behavioral analytics establish baselines for users and entities to detect anomalies. Each event is assigned a dynamic risk score to help analysts focus on high-impact activity.

For teams constrained by limited automation or manual processes, New-Scale Analytics also offers built-in workflows and prebuilt content aligned with common threat types such as phishing, ransomware, malware, and insider threats, making it easier to adopt TDIR best practices without overhauling existing infrastructure.

Whether augmenting a legacy SIEM or centralizing detection on a data lake, New-Scale Analytics provides an immediate, modular path to stronger outcomes.

About Exabeam

Exabeam is a leader in intelligence and automation that powers security operations for the world's smartest companies. As a global cybersecurity innovator, Exabeam provides industry-proven, security-focused, and flexible solutions for faster, more accurate threat detection, investigation, and response (TDIR).

exabeam

Learn more at www.exabeam.com →