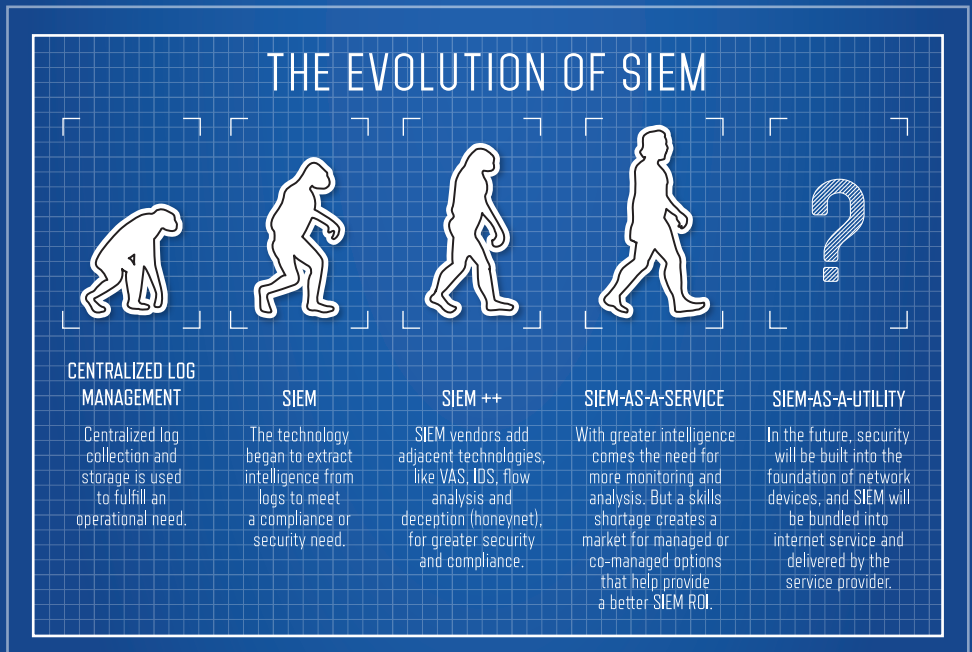# Understanding SIEM.

SIEM is a foundational technology for both securing a network from threats as well as demonstrating regulatory compliance. Security information and event management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources.

The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.

SIEM solutions have evolved quite a bit over the last 10+ years. Choosing the right SIEM for your organization is a critical decision.

EventTracker continues to be at the forefront of this evolution - building upon our leading platform, Security Center, and offering a flexible "co-managed" SIEM-as-a-Service that optimizes security and compliance for each unique organization.

## THE EVOLUTION OF SIEM

| CENTRALIZED LOG MANAGEMENT | SIEM | SIEM ++ | SIEM-AS-A-SERVICE | SIEM-AS-A-UTILITY |
|---|---|---|---|---|
| Centralized log collection and storage is used to fulfill an operational need. | The technology began to extract intelligence from logs to meet a compliance or security need. | SIEM vendors add adjacent technologies, like VAS, IDS, flow analysis and deception (honeynet), for greater security and compliance. | With greater intelligence comes the need for more monitoring and analysis. But a skills shortage creates a market for managed or co-managed options that help provide a better SIEM ROI. | In the future, security will be built into the foundation of network devices, and SIEM will be bundled into internet service and delivered by the service provider. |

continuum
IT management platform

continuum.net

# Don't settle for SIEM shelfware. Get results.

While SIEM is a critical component, due to a lack of qualified analysts for in-house SIEM, organizations have failed to achieve the results they expected, which can cause SIEM to become "shelfware". As a result, co-managed SIEM is on the rise.

Organizations have discovered that self-managing a robust SIEM solution is too expensive, arduous to maintain, and is difficult to staff for constant monitoring. Co-management is on the rise and expected to grow five-fold by 2020. Proper security management is a collaboration with our customers to deliver results and optimize your team's effectiveness.

## Why do organizations prefer co-managed SIEM?

- **REDUCE DEPLOYMENT TIME**

- **CONTROL COST AND RESOURCES**

- **SIMPLIFY CONTRACTS AND SCALABILITY**

- **MAXIMIZE SECURITY CAPABILITIES**

**"Co-managed SIEM services enable security and risk management leaders to maximize value from SIEM and enhance security monitoring capabilities, while retaining control and flexibility."**

How and When to Use Co-Managed SIEM

**Gartner.**

---

**"SIEM technology delivered as a service offers the opportunity to simplify and reduce the time to implement, administer, maintain and scale, while reducing licensing complexity, compared with on-premises versions."**

Innovation Insight for SIEM as a Service

**Gartner.**

**continuum**
IT management platform

continuum.net