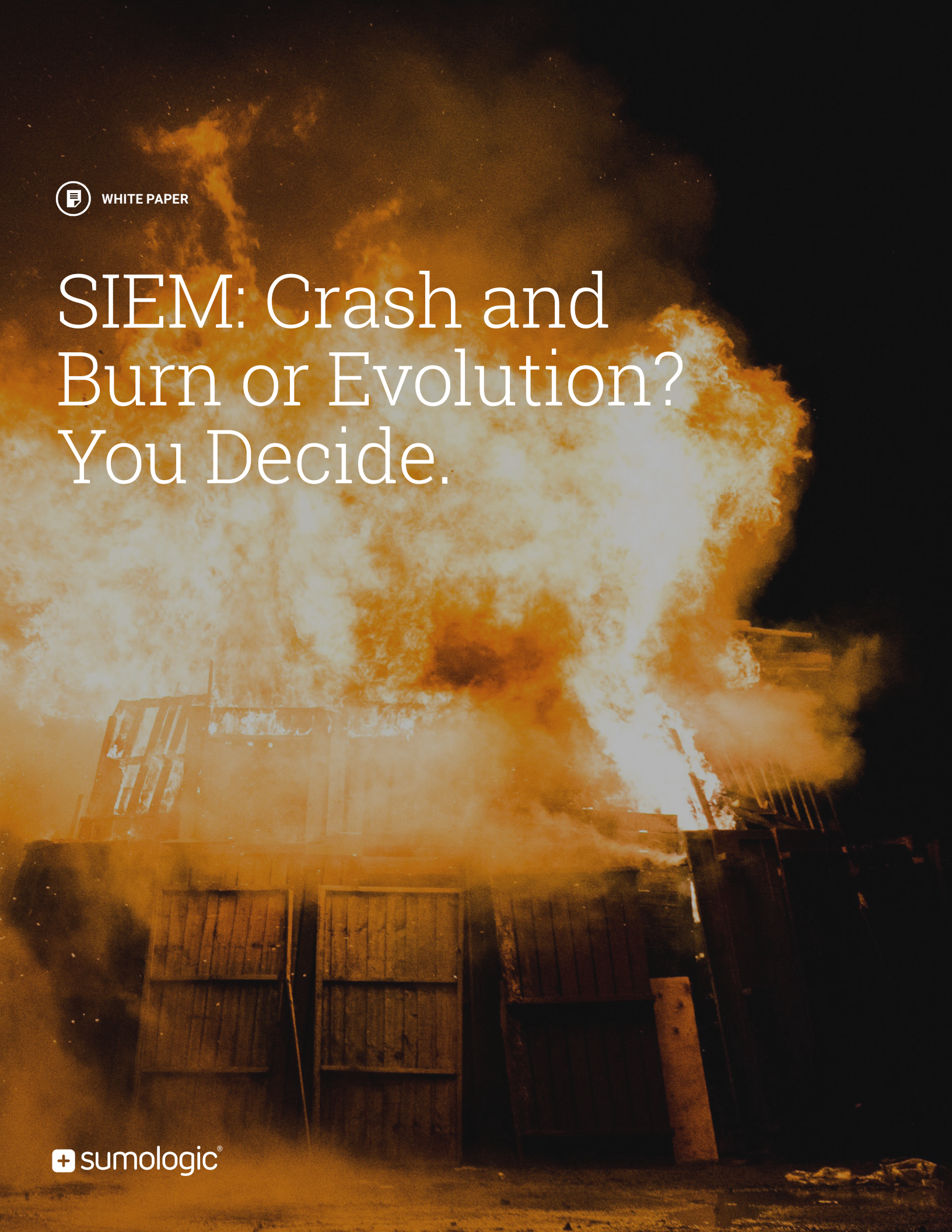


WHITE PAPER

SIEM: Crash and Burn or Evolution? You Decide.

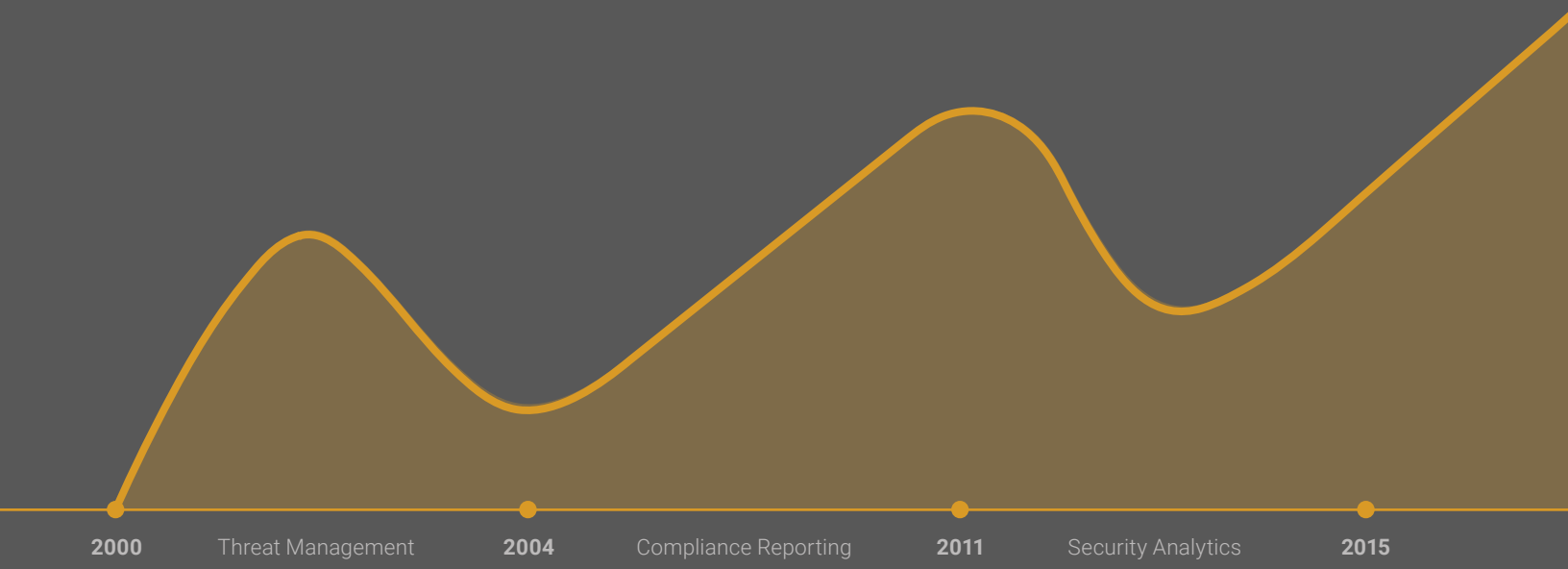
sumologic®

SIEM stands for Security information and event management and these solutions have been around since 2000. They were developed with the goal of helping organizations in the early detection of targeted attacks and data breaches.

But SIEMs have struggled to keep pace with the security needs of modern enterprises, especially as the volume, variety and velocity of data has grown. As well, SIEMs have struggled to keep pace with the sophistication of modern day threats. Malware 15 years ago was static and predictable. But today's threats are stealthy, and polymorphic.

"Often times when presenting at conferences, people will ask "Is SIEM Dead"? Such a great question! Has the technology reached its end of life? Has SIEM really crashed and burned?

I think the answer to that question is NO. SIEM is not dead, it has just evolved.[1]



The Evolution of SIEM - Transitioning to Security Analytics. Source: Forrester Research, Inc.

In speaking with hundreds of customers, and prospects, the reality is that few enterprises have the resources to dedicate to the upkeep of SIEM and the use of the technology to address threat management has become less effective and waned. Gartner Analyst Oliver Rochford famously wrote, "Implementing SIEMs continues to be fraught with difficulties, with failed and stalled deployments common".[2]

In Greek mythology, a phoenix (Greek: φοῖνιξ phoinix; Latin: phoenix, phœnix, fenix) is a long-lived bird that is cyclically regenerated or reborn. Associated with the sun, a phoenix obtains new life by arising from the ashes of its predecessor.

The SIEM ashes are omnipresent and Security Analytics are emerging as the primary system for detection and response.

Deconstructing SIEM

Although we use the term SIEM to describe this market, SIEM is really made up of two distinct areas:

1. SIM or Security Information Management (SIM) deals with the storage, analysis and reporting of log data. SIM ingests data from host systems, applications, network and security devices.
2. SEM on the other hand, or Security Event Management (SEM), processes **event** data from security devices, network devices, systems, and applications in real time. This is dealing with the monitoring, correlating, and notification of security events that are generated across the IT infrastructure and application stack.

Although folks generally do not distinguish between these two areas anymore, and just use "SIEM" to describe the market category, one should really take note of what they are trying to accomplish and what problems they are trying to solve by bringing about these kids of solutions.

Why Do We Care About SIEM?

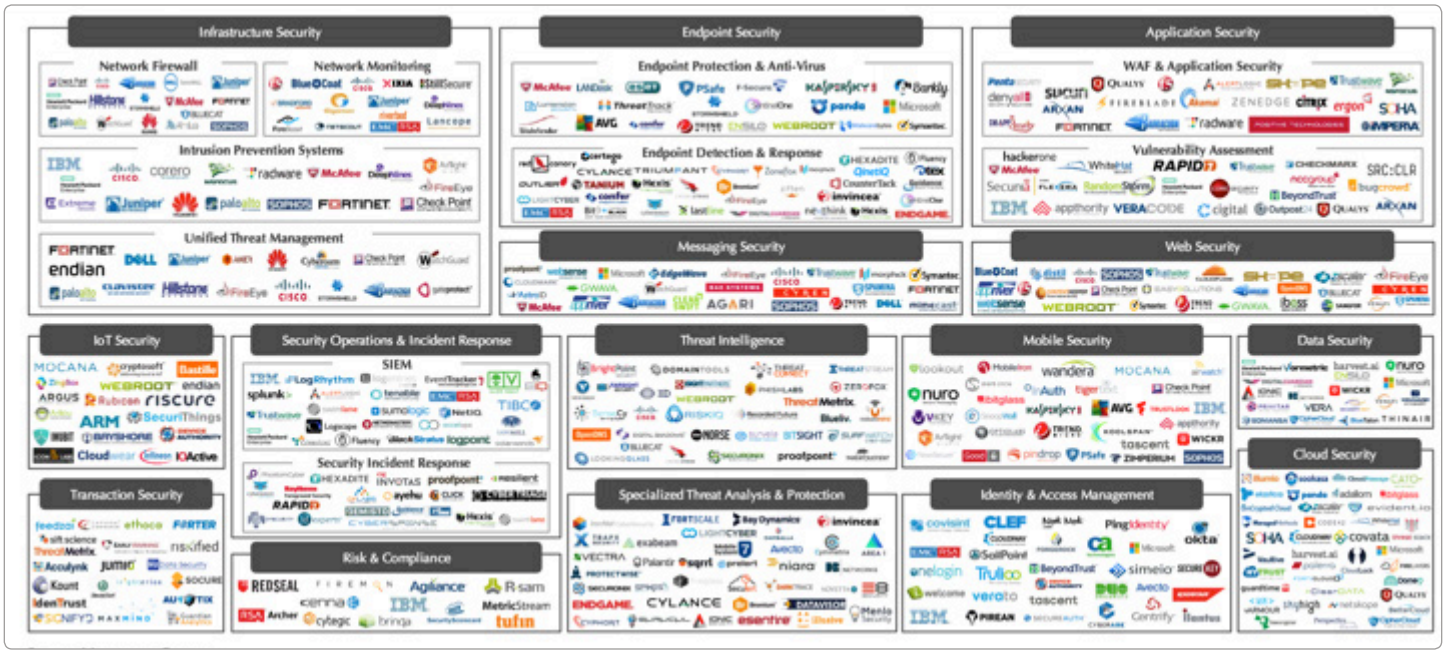
One could easily dismiss these solutions outright, but the security market is huge - $21.4B in 201 according to our friends at Gartner. And the SIEM piece alone reached $1.6B last year.

According to 451 Research the security market has around 1,500-1,800 vendors broken down into 7-8 main categories across

“There are two types of companies, those who have been hacked and those who have no clue.”

Executive Chairman and former CEO
Cisco Systems

The Security Sector is Dynamic and Vast. We are Ceaseless & Vigilant in Our Coverage.



Source: Momentum Partners.

IAM, EPP, SIEM, SMG, SWG, DLP, Encryption, Cloud Security, etc. And within each of these main categories, there are numerous sub categories.

And despite the billions of dollars invested, current security and SIEM solutions are struggling to keep the bad guys out. Whether cyber criminals, corporate spies, or others, these bad actors are getting through.

The Executive Chairman and former CEO of Cisco Systems famously said, "There are two types of companies, those who have been hacked and those who have no clue." Consider for a moment that the median # days before a breach is detected is over 6 ½ months and that the % of victims notified by external 3rd parties is almost 70%.[3] People indeed have no clue! Something different is clearly needed.

SIEM and Security Analytics: Head to Head

SIEMS were a great technology when we were dealing with protecting the known, with fixed perimeters and signature-based security. But is this reflective of today's dynamic threat landscape, with a porous perimeter and workloads moving to the cloud?

When I graduated university back in the late 80's, I was a computer programmer for a large insurance company, working on IBM mainframe applications (IMS DB/DC and CICS DB2). These were large monolithic applications, self-contained, with long development, testing and delivery cycles that took 12-18 months. We sat down with users, collected requirements, built prototypes, and went through unit, regression and QA testing before rolling things into production – OLD SCHOOL.

Think about modern digital companies that are successful today – Airbnb, Netflix, Uber, Amazon, Skype, Twitter, LinkedIn to name a few. These companies – in order to drive continuous innovation and continue to be relevant to their customers - are leveraging micro services, containers like Docker, configuration management tools like Chef and Puppet. They are driving continuous delivery initiatives weekly, even daily, at a pace we have not seen before. And to support this rapid pace, organizations are looking to leverage modern, advanced IT infrastructure for a majority of these workloads such as from public cloud providers like AWS or Azure.

So when you think about the CI/CD lifecycle, and the cloud-based infrastructures these modern applications are running on, we are

dealing with a lot of layered components - OS, Applications, NW devices, Storage devices, servers and workstations, etc. - and all this infrastructure produces a lot of data, siloed data. When you consider the volume, variety and velocity of the data streams, it becomes extremely challenging – leveraging SIEMs - to ingest this capacity and extract answers and insights in a timely fashion. The SIEM architecture was becoming their Achilles heel and maybe, more appropriately, a ball and chain around their ankle.

Additionally, as organizations move into this digital world, developing modern applications, leveraging mobile, social, information and cloud to deliver new and disruptive experiences to their customers, the predictability of workload volumes is less certain. Think about what happens to Airbnb during Thanksgiving travel season? Or Target during the Xmas shopping season? And how requests for Uber rides spike during a major sporting like the super bowl? This capacity has to be planned for, the hardware and software need to be provisioned, the people allocated, and so on. This takes time, money and foresight. Wouldn't a secure, highly elastic, cloud-native, analytics service that bursts automatically as needed be a lot easier than over provisioning servers to handle spike volumes, but that sit well below capacity for the majority of the year?

To truly be rid of this ball and chain, one needs to move beyond the rigid, fixed correlation rules that generate so much alert fatigue among InfoSec teams, that they are generally ignored. These rules were great at surfacing up known events, but what about the unknown events? What happens when you do not even know the questions to ask? With millions of event and log data being generated daily, finding these indicators of compromise (IOCs) are like trying to find the needle in the haystack. It becomes humanely impossible.

This is where Security Analytics solutions steps in. By leveraging machine learning algorithms and data science, they are able to identify abstract relationships, anomalies and trends and surface up problems automatically. Security analytics solutions look at the data more holistically, providing full-stack visibility across on hybrid infrastructures.

To summarize, below are the six takeaways on the SIEM vs. Security Analytics debate that I've pulled together based on industry analysts' and thought leaders' feedback. Use them as a guide for your future security solution investments.

Six Takeaways on the SIEM vs. Security Analytics Debate

1. Security data is unmanageable with legacy SIEM tools
2. Advanced analytics are being integrated into security markets after rule and signature based prevention systems and tuning processes struggled to detect or stop most serious breaches over the past few years.

	SIEM	Security Analytics
Application	Monolithic Applications, Static, Long development and release cycles, Mode 1	Modern Applications, Dynamic, Microservices, DevOps, Mode 2
Infrastructure	On Prem	Cloud
Execution Environment	Plan for capacity growth (HW, SW, FTE)	Elastic, Multi-tenant, Secure
Time to Deploy	15 months (avg.)	Up and running in hours
Cost	$1.4M (HW, SW, People)	$1,000 for 1GB daily ingest
Protection Capabilities	Protect the Known – Perimeter-based security using a defined signature approach	Protect the Unknown – Distributed cloud/ hybrid cloud model using behavioral-based & continuous monitoring methodologies (across users, applications, NW, data)
Protection Approach	Fixed-Rule Set (connect the dots)	Machine Learning to identify abstract data relationships, anomalies, trends, and fraudulent behavioral patterns
Visibility	Islands of Security / Limited view / Chokepoints / Port Mirroring	Holistic, Integrated, Risk-Based, Enterprise Wide View / APIs & Native Services

SIEM vs. Security Analytics comparison.

3. Security and risk professionals must evolve their tool set and capabilities to keep up with the maturing threat landscape
4. Consider threats that are already inside the enterprise: SIEM tools are typically deployed to look at the perimeter of the network, yet this mentality can expose organizations to great risk
5. Machine-learning algorithms and analysis techniques have advanced far beyond the capabilities of what was available in the commercial markets only two to three years ago. They also address the issue dubbed "We don't know what we don't know;
6. Security analytics' core function is to monitor and collect vast amounts of information from the environment to identify threats that indicate elevated risk and ultimately prevent lateral spread of those threats and data exfiltration. To succeed in this endeavor, the analytics platform performs the identification of threats and prioritization of threats without the requirement for the administrators and analysts to create policies or rules.

This is truly a transformative shift that we see once a decade. Are you ready to join the ride or are you content with the status quo?

Additional Resources

Find out how Sumo Logic helps deliver advanced security analytics without the pain of SIEM

Sign up for a free trial of Sumo Logic. It's quick and easy. Within just a few clicks you can configure streaming data, and start gaining security insights into your data in seconds.

Mark Bloom runs Product Marketing for Compliance & Security at Sumo Logic. You can reach him on LinkedIn or on Twitter @bloom_mark.

About Sumo Logic

Sumo Logic is a secure, cloud-native, machine data analytics service, delivering real-time, continuous intelligence from structured, semi-structured and unstructured data across the entire application lifecycle and stack. More than 1,000 customers around the globe rely on Sumo Logic for the analytics and insights to build, run and secure their modern applications and cloud infrastructures. With Sumo Logic, customers gain a multi-tenant, service-model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value and growth.

Sources:

[1] Forrester: Evolution of SIEM graph, taken from Security Analytics is the Cornerstone of Modern Detection and Response, December 2015

[2] Gartner: Overcoming Common Causes for SIEM Deployment Failures by Oliver Rochford 21 Aug 2014

[3] Mandiant mTrends Reports

sumologic®

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 9460

www.sumologic.com