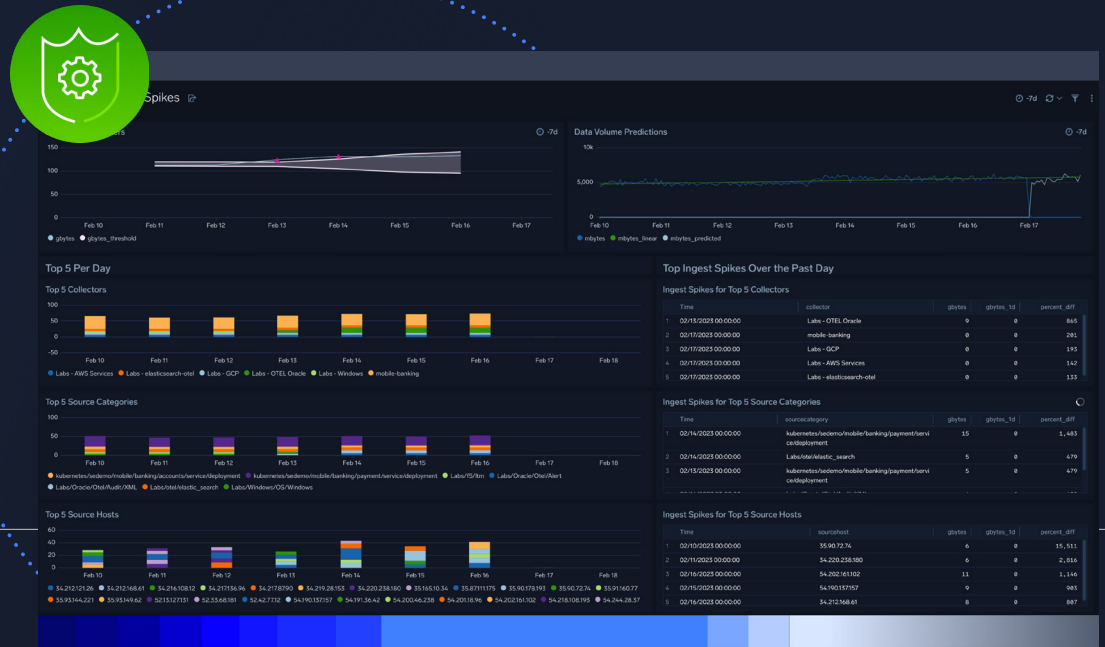


# How to take your security posture to the next level

sumo logic



# The high cost of risk

According to IBM and the Ponemon Institute's [Cost of a Data Breach Report 2022](#), the total cost of a global data breach reached \$4.35 million — up 12.7% from 2020. That number is even higher for US businesses, where the average cost of a breach exceeded \$9.4 million in 2022. In a world where 85% of organizations studied in the report experienced more than one data breach during their tenure as a company, these costs — and the potential business outcomes — are devastating.

Yet, despite these figures, many businesses do not have a cybersecurity plan. For example, [only 50% of small to medium companies](#) have a cybersecurity plan; 32% of those who have a plan have not updated it since the COVID-19 pandemic and the shift to remote work. As digital innovation and hybrid work persist, organizations must implement measures that can help them find, explore and respond to cyber threats. Threat detection and investigation tools make that possible.



**50%**

**only 50 percent of small to medium companies have a cybersecurity plan.**

## For security teams, maintaining an excellent security posture isn't just important; it's fundamental.

Healthy applications and cloud infrastructure require strong security posture to retain satisfied customers and grow revenue. Threat detection and investigation refers to identifying and exploring threats or security-related events within an asset, application or network as quickly and effectively as possible.

Today, businesses face an increasing volume of data paired with [dozens to even hundreds](#) of disparate security tools and applications to manage and monitor. That's not to mention the persistent cybersecurity talent gap (2022 illustrated a need for more than [3.4 million security professionals](#)). Businesses with small or emerging security teams can feel stuck between a rock and a hard place.

**Threat detection** identifies threats within cloud-based, hybrid and on-premises infrastructure and applications before they cause major issues for a business. The sooner security teams uncover a security-related event, the quicker they can investigate and mitigate it.

**Threat investigation** analyzes a threat or potential threat to glean more information about it. When a threat is detected, SecOps teams use behavioral, forensic and log data to investigate and uncover as much information as possible. From there, teams can respond appropriately to the threat and plan for system improvements to reduce risk in the future.

Fortunately, advanced [security analytics](#) platforms provide organizations with a one-stop shop to monitor and secure applications and infrastructure.

## What threats do emerging security teams face?

Cybersecurity is an arms race with the war waged in the cloud. On the one hand, businesses are dealing with multiple cloud environments, not to mention hybrid and on-prem infrastructure, and increasing amounts of data. By 2025, the world will need to protect [200 zettabytes of data](#) — zettabytes have 21 zeros for those doing the math.

On the other hand, you have bad actors and cyber criminals deploying evolving tactics and techniques to target businesses of all sizes and industries. Here's what you need to know about the current state of security for businesses:

- The leading cause of a security breach is credential theft, followed by phishing, exploiting vulnerabilities and botnets, according to Verizon's 2022 [Data Breach Investigation Report](#).
- When looking specifically at SMBs, the [most common form](#) of attack is malware, at 18%, followed by phishing, data breaches, website hacking, DDoS attacks and ransomware.

- 2022 saw a [13% rise in ransomware](#), a steep increase that's been rapidly rising over the past five years. Blocking the key areas discussed in the previous two bullet points can help minimize the potential for this kind of attack
- Human error cannot be overlooked, as customers, employees and vendors play a large part in security-related events. [Roughly 82% of breaches](#) involved a human element, such as social engineering attacks, misuse or other errors.
- An organization takes an average of [277 days to identify](#) and contain a data breach, but businesses that contain it faster can save money and resources. For example, organizations that resolve their issue in under 200 days stand to save about 26.5% — or roughly \$1.12 million.

How do you fend off numerous threats that target your application or network? In part, it comes down to finding a solution that grants teams visibility into their log data, security tools, infrastructure and applications.

# Security for growing fintech company

It's hard to argue that threat detection and investigation aren't business critical in a world where cyberattacks aren't a matter of if but when. But how does it combine into a holistic and successful strategy that even a startup could use? Just ask Dave.

## The challenge

Dave, a financial services organization best known for their “Banking for Humans” slogan, has achieved hypergrowth — with ten million-plus users on their mobile app. While hypergrowth is great, it brings a series of complex challenges. Chief among these challenges is clear visibility into systems to ensure their applications, environments and customer data are secure.

Dave set out to find a solution to capture vast amounts of data, including all user activities, API calls and logs, to garner insights for product interactions while keeping their systems and data secure.



# Dave landed on Sumo Logic's SaaS analytics platform as their logging and monitoring solution.

The platform offers full application and infrastructure visibility so Dave can capture and analyze all their data from disparate sources in a single location. With Sumo Logic, Dave can monitor security-related data to improve their security posture.



Configure robust alerting policies using Sumo Logic Monitors to track critical logs and get real-time notifications when changes or outliers occur.

## The results

With a powerful monitoring solution in their arsenal, the team at Dave has seen significant benefits that will support their growth for years to come.



### Understand all threats and vulnerabilities

By continuously monitoring security logs and events data, Dave improved their overall security posture.



### Incorporate easy-to-use insights

Dave can iterate and deploy releases based on user behavior, system issues and other relevant application events.



### Support compliance

By employing Sumo Logic, Dave gained access to the data monitoring, analysis and reporting necessary for compliance with GDPR, PCI DSS and SOC 2.

[Read more](#) about how Dave is using Sumo Logic to power security and observability analytics across their entire enterprise.

# Ready to dive in?

## Your step-by-step guide to getting started with threat detection and investigation

Organizations are dealing with vast amounts of data paired with the need to monitor alerts, tools, infrastructures and applications. It's a lot to manage. But with advanced threat detection and investigation tools, teams can monitor all their environments in a single location, cutting back the time and resources needed to switch between various programs. For example, with [Sumo Logic Cloud Security Analytics](#), security teams have one place to monitor, alert and analyze data in real time across all their security tools.



**Developing and implementing a threat detection and investigation process doesn't have to be challenging. The five steps on the following pages can get you started.**

---

## 1 Collect and aggregate all security data into a single, unified location

Save your security team time, money and resources by aggregating your structured and unstructured data into a single source of truth. Sumo Logic's [security data lake](#) combines secure storage with domain-agnostic analytics for more effective threat detection and investigation.

---

## 2 Use integrations to discover trends or potential threats

Sumo Logic empowers security teams to increase the velocity and accuracy of threat detection. And, with hundreds of out-of-the-box integrations, you can access pre-built queries for custom searching and monitoring.

---

## 3 Configure robust alerting policies to notify SecOps teams when changes or outliers occur

The quicker your team can get to work, the quicker investigation and mitigation can happen. With [Sumo Logic Monitors](#), teams can track and build alerts that fit their unique requirements.

---

## 4 Program and deploy automated responses to start damage mitigation

These automated responses can go a long way in controlling potential damage and restoring affected systems until you resolve the threat.

---

## 5 Perform root cause analysis to investigate the threat fully

Attacks may persist without further investigation and patches, so it's critical to find and patch any vulnerabilities as soon as possible. Sumo Logic provides powerful [search capabilities](#) so teams can perform extensive threat investigations quickly.

# Detect and investigate the risks that matter most

Sumo Logic [Cloud Security Analytics](#) empowers SecOps and DevSecOps teams to detect threats from every angle with use-case-driven queries, dashboards, alerts and more. With broad-based security functionality, you can observe, detect and investigate security threats throughout your environment.

In addition to **threat detection and investigation**, Sumo Logic Cloud Security Analytics covers other critical use cases, including:

- Security data lake — To store and manage information
- Audit and compliance — To meet security regulations and follow best practices
- Application security — To embed security throughout the application lifecycle

Your business and your customers deserve security. Sumo Logic Cloud Security Analytics provides built-in detection, integrated threat intelligence and search-based investigation to improve the security posture of your applications and infrastructure in a single platform. When you're ready to take your threat detection and investigation to the next level, [contact us](#) or start your [free 30-day trial](#).

**Sumo Logic.**  
**The infinite power of log analytics.**