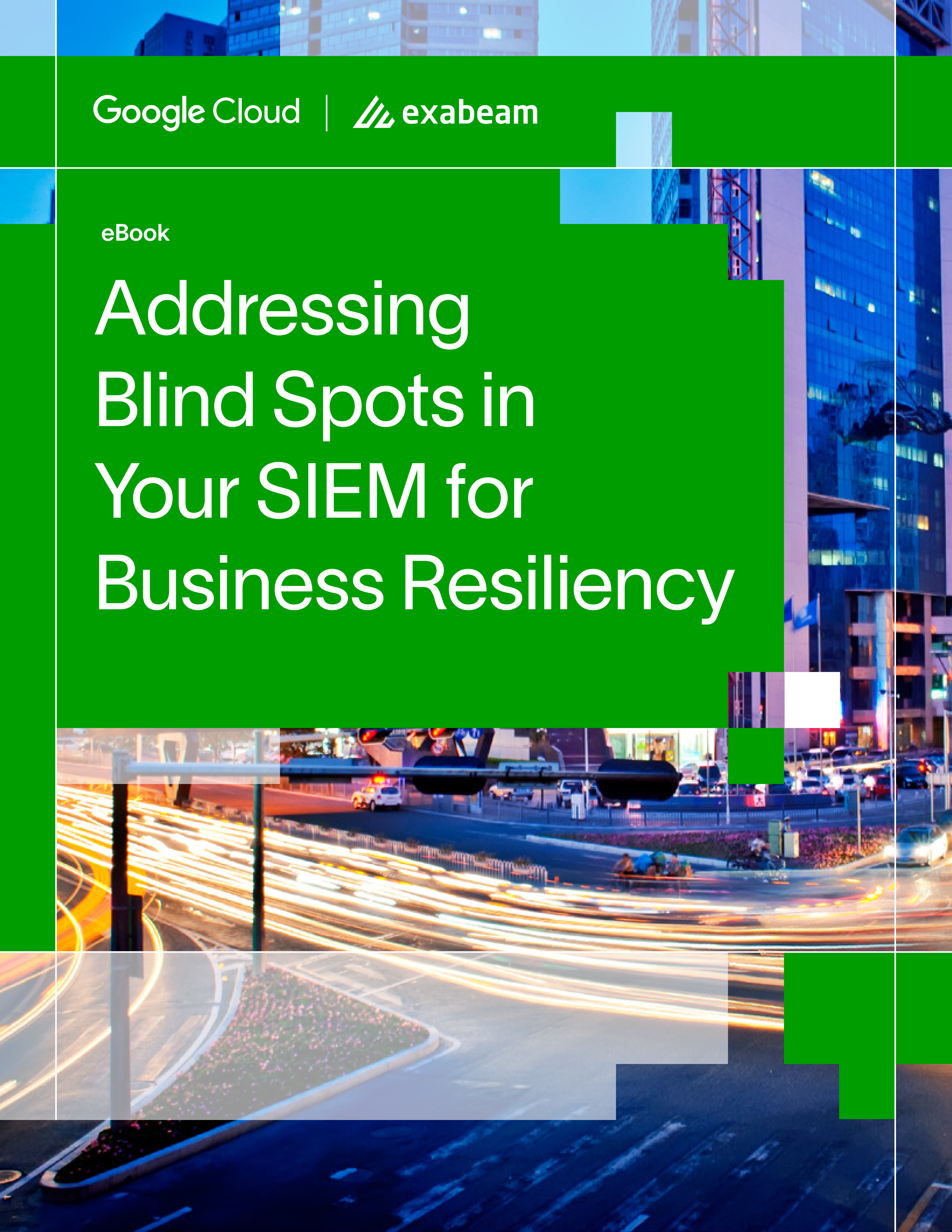
Google Cloud | exabeam

eBook

Addressing Blind Spots in Your SIEM for Business Resiliency



Contents

Introduction

The looming threat of a security breach and its impact on maintaining business operations are top concerns for organizations.

As organizations embark on more distributed and cloud-based systems, the attack surface expands, opening the exposure to more attacks and advanced security threats. Add to this, cybercriminals are more sophisticated in exploiting vulnerabilities that often lead to breaches, compromised credentials and wide scale data exfiltration.

Data breaches are more common today than ever before, and more costly. The average total cost for a data breach increased nearly 10% to $4.24 million, the highest ever recorded according to Ponemon Institute's 2021 report.

Traditional SIEM solutions struggle to protect against the advanced security threats we are witnessing due to increasingly cloud-based infrastructures, remote work, internet, and user traffic at unparalleled levels. Moreover, new tactics using machine learning and multi-phase attacks combined with a shortage of cybersecurity expertise add to the challenges of protecting your business against a security breach. Organizations need to evolve from their legacy solutions and are looking for new security solutions that deliver better outcomes.

- **Remote work due to COVID-19 increased the average data breach cost $1.07 M higher**
- **Compromised credentials caused the most breaches 20% at an average cost of 4.37M**
- **3.5M unfilled cyber security jobs globally in 2021**

Why is the threat surface so challenging to protect?

The digital era created a distributed world where data, people and business are dispersed.

The traditional notion of perimeter security has disappeared. And, new classes of cyberattacks arise as adversaries advance their approaches to target these businesses' vulnerabilities.

Threat landscape expands

More recent events, such as the shift to work from home, adoption of cloud, the emergence of the Internet-of-Things (IoT), and 5G and IPV6, are expanding the threat landscape. The attack vectors now span clouds, endpoints, networks, and even APIs.

Smarter cybercriminals

Today's cybercriminals, extremely motivated and well funded by organized crime and nation-states, are using new tactics that include machine learning and multi-phase attacks. Traditional SIEM and many security point products based on rules or search, leverage knowledge from prior attacks, making it difficult to keep up with emerging attacks.

Complex IT environments

Today's IT landscape consists of data scattered across on-premises infrastructure, public, private and hybrid clouds that all contain sensitive data. Employees are accessing critical business information using a myriad of devices. As businesses continue to innovate, a proliferation of smart devices contain and share data across other devices and systems.

Exabeam is a three-time leader in the Gartner Magic Quadrant for SIEM and positioned highest for its ability to execute in 2021.

Top 4 SIEM shortcomings for today's threats

With its genesis in 2015, SIEMs evolution of central log management (CLM) to serve as a broader threat and operational risk platform served business well when the world was a bit simpler.

Since then, the advances in technology and the complexity in protecting the IT infrastructure has made SIEM increasingly ineffective for several reasons.

Reliance on rules and signatures versus analytics

Too many alerts and false positives to track down

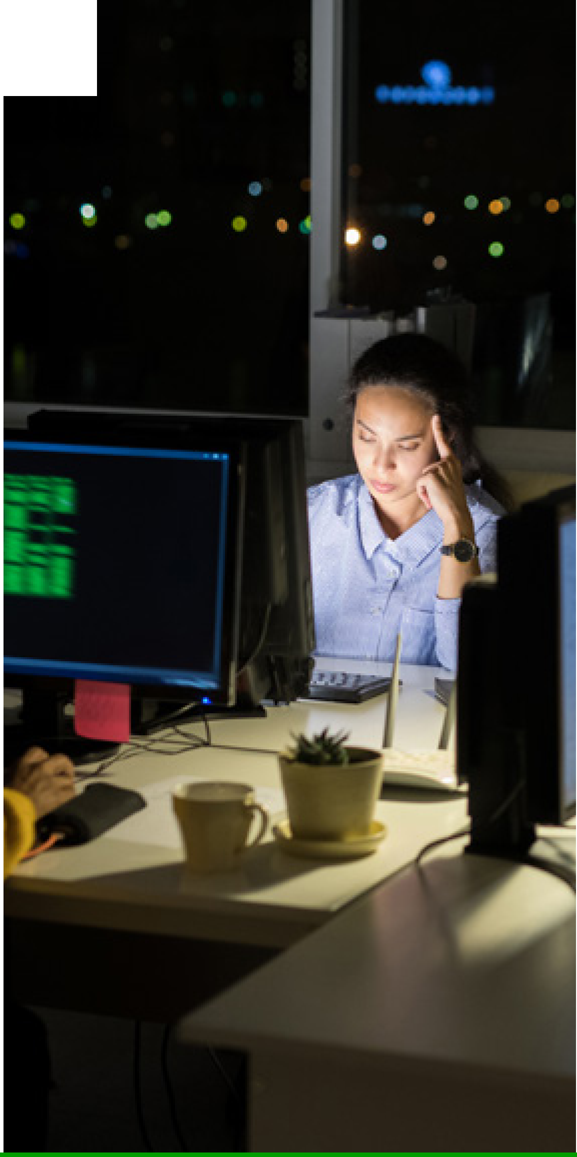
Limited data ingestion capabilities and data overload

Difficult to deploy and maintain

Gartner predicts by 2023 that data security, cloud security, and infrastructure protection are the fastest-growing areas of security spending.

A slow response is costly

The Ponemon Institute research showed that faster incident response times were associated with substantially lower costs, with a cost savings of nearly 30% if a breach was contained in less than 200 days.



How can you find threats faster?
Technology expedites an organization's ability to identify and contain security threats. Security technology augments or replaces human intervention using artificial intelligence, machine learning, analytics, and automated security orchestration. Finding incidents and intrusion attempts faster results in cost savings. The Ponemon Institute study cited artificial intelligence applied to security mitigated costs the most.

Organizations that deployed automated and security artificial intelligence (AI) solutions spent up to $3.8 million less in remediation from data breaches than organizations without.

- **The cost of mega breaches, 1M+ records, reached over $400 million**
- **The largest breaches were 50 to 65M records**
- **Customer personally identifiable information is the most frequently breached and the most expensive at $180 per record**

Protect more with behavioral analytics

Your existing security solution may not be enough to provide business resilience amid the new threat landscape.

To identify blind spots, and keep their organization protected, forward-thinking IT security departments are embracing a behavioral analytics approach.

What is behavioral analytics, and how can it bolster your security? A behavioral analytics solution continuously monitors the behavior of users and devices, establishing a baseline of what normal behavior for each of them looks like. Whenever new activities occur, your behavioral analytics solution will compare them to the baseline, and if it detects abnormalities, score them accordingly.

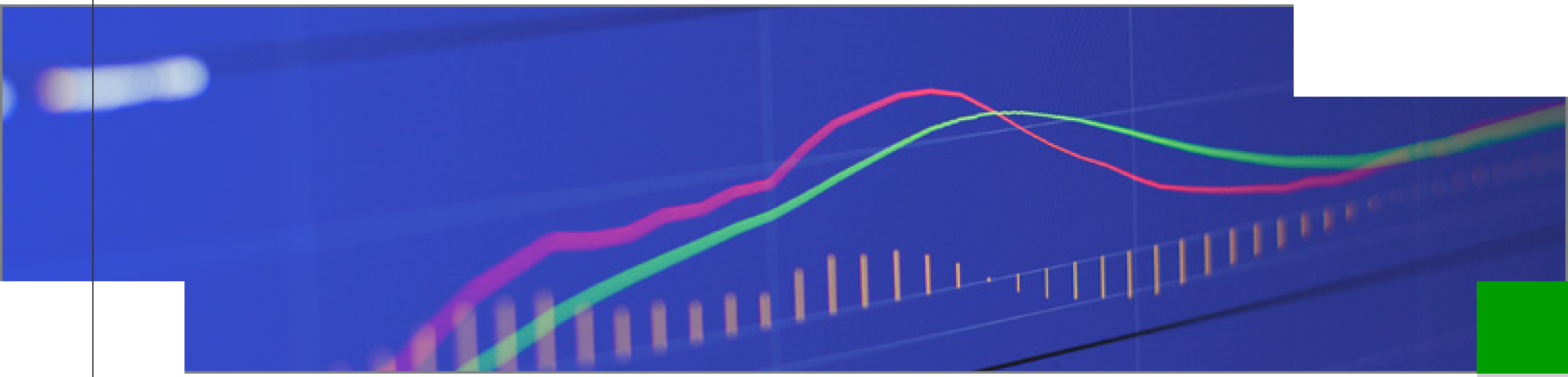
Here is how to integrate behavioral analytics in your security workflows to detect insider threats and lateral movement.

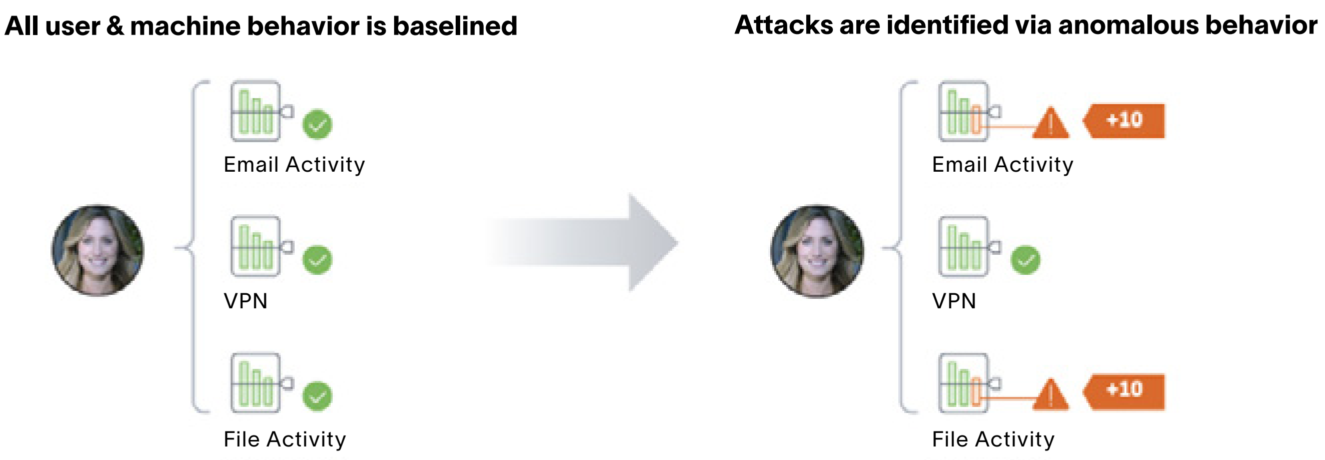
Step 1
Baseline user and machine behavior

Step 2
Aggregate all security telemetry in a single place

Step 3
Associate all events to users and machines and their peer groups and geographies

Step 4
Run analytics to find abnormalities




All user & machine behavior is baselined
Email Activity
VPN
File Activity
Attacks are identified via anomalous behavior
+10
Email Activity
VPN
+10
File Activity

Behavioral analytics works by detecting abnormal behavior, rather than being trained to recognize previous attacks (a rules-based approach).

As a result, it can help detect previously unknown threats.

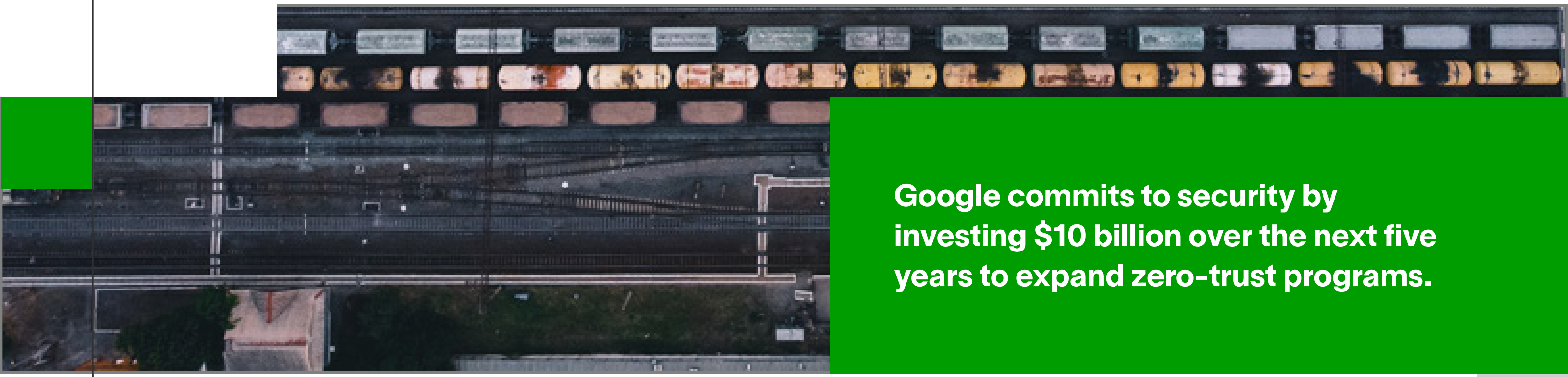
Behavioral analytics is superior for catching threats from malicious or compromised insiders, as those users who deviate from their typical behavior in order to attack.

One excellent use of behavioral analytics is to help automate triage alerts. According to Ponemon, analysts spend 36% of their time triaging alerts.

They must take the time to answer various basic questions about an alert before deciding how to proceed. Even a single alert can trigger an avalanche of questions.

Automating your triage alerts takes that time-consuming work off analysts' hands, and behavioral analytics helps you get there. Behavioral analytics can provide insightful context for triage alerts, offering information on what normal behavior looks like and how risky a particular anomaly is, enabling analysts to make a quick decision.

You can also automate investigations using the context provided by behavioral analytics, which links changes in behavior back to specific users and devices, creating the opportunity to proactively automate specific, course-correcting, next steps.



Google commits to security by investing $10 billion over the next five years to expand zero-trust programs.

Exabeam: The fastest path to a resilient security posture

Business continuity is essential, and equipping your security team with the right tools is vital. With its Next-Gen SIEM and XDR, Exabeam takes the guesswork out of detecting emerging threats.

Its native user and entity behavior analytics (UEBA) capabilities team up with automation to help security teams increase efficiency and run a modern SOC.

Despite the shortcomings of traditional SIEM, it still has its purpose as a log collector. Organizations who don't want to rip and replace their SIEM have options. Exabeam Fusion SIEM or XDR can augment a legacy SIEM and provide best-in-class analytics and automation on top of it. The legacy SIEM provides the centralized data storage and compliance reporting, while Exabeam offers Next-Gen cloud-based, threat detection, investigation and response - whether as a SIEM or XDR.

If you have decided it's time to fully modernize your SOC, consider Exabeam Fusion SIEM or XDR. With Fusion SIEM, you get centralized data storage that scales to your organization's needs, as well as compliance reporting capabilities. If long term data retention and compliance are not needed Fusion XDR is your choice. Fusion SIEM and XDR both leverage Exabeam analytics, automation and prescriptive use case content, allowing you flexible options to get proven, repeatable solutions to combat threats.

Deliver more security value with Exabeam by:

Modernizing threat protection

Quickly identify and defend against new and emerging threats and verify compliance with security regulations

Tackling rising cybercrime

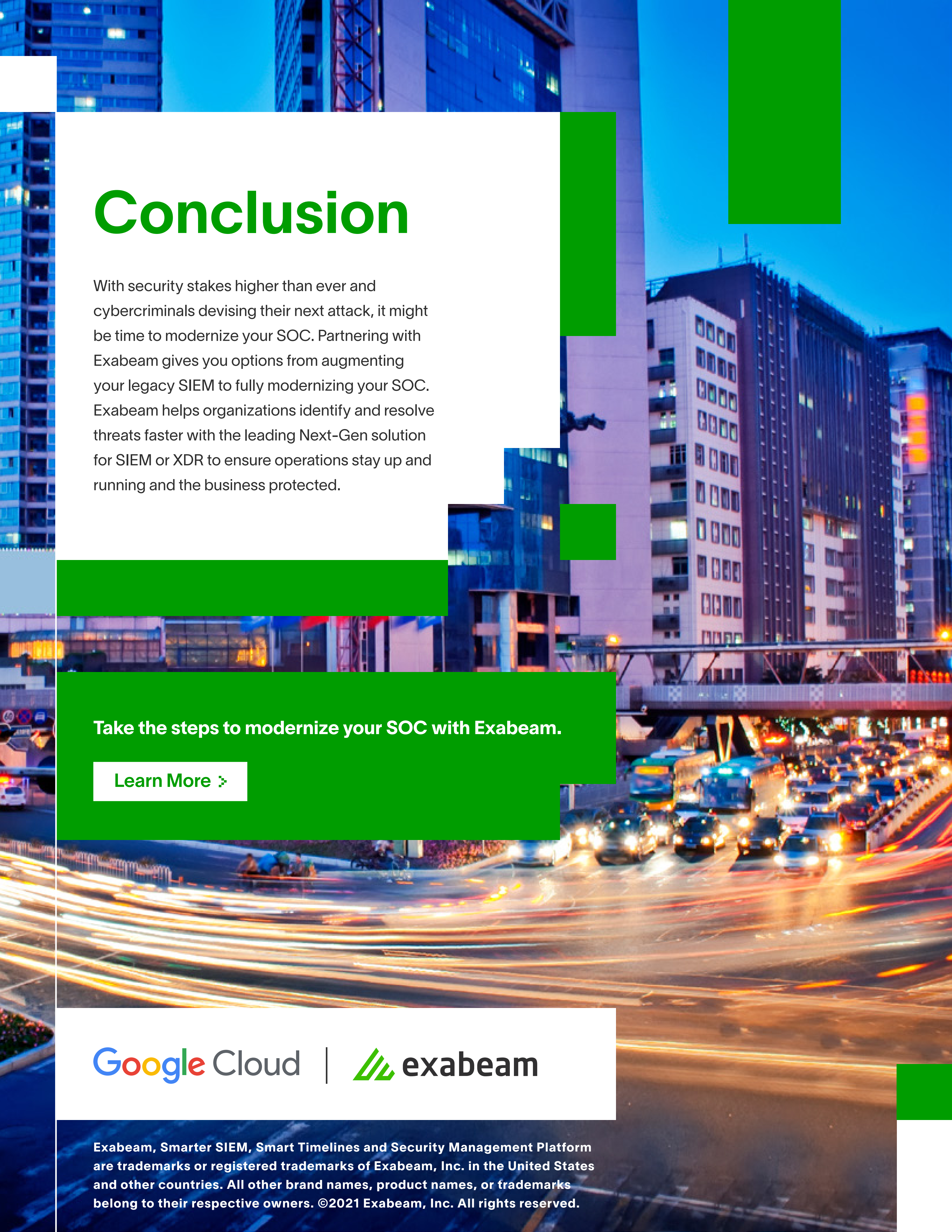
Integrate with existing cybersecurity products

and use junior level staff for

cost efficiency

Protecting against exploited network vulnerabilities

Find abnormalities as compared to baselines to detect insider threats and lateral movement



Conclusion

With security stakes higher than ever and cybercriminals devising their next attack, it might be time to modernize your SOC. Partnering with Exabeam gives you options from augmenting your legacy SIEM to fully modernizing your SOC. Exabeam helps organizations identify and resolve threats faster with the leading Next-Gen solution for SIEM or XDR to ensure operations stay up and running and the business protected.

Take the steps to modernize your SOC with Exabeam.

Learn More >

Google Cloud | exabeam

Exabeam, Smarter SIEM, Smart Timelines and Security Management Platform are trademarks or registered trademarks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. ©2021 Exabeam, Inc. All rights reserved.