exabeam

WHITE PAPER

SECURING THE CLOUD WITH MODERN SIEM MONITORING AND ANALYTICS

SUMMARY

MANY ENTERPRISES ARE EMBRACING THE CLOUD TO SUPERSEDE ON-PREMISES DATA CENTER RESOURCES: 86 PERCENT OF SECURITY LEADERS SAY THEY'RE MOVING THEIR OPERATIONS INTO THE CLOUD, AND 70 PERCENT SAY THEIR CLOUD SECURITY BUDGET WILL INCREASE DRAMATICALLY IN THE NEXT THREE TO FIVE YEARS.[1]

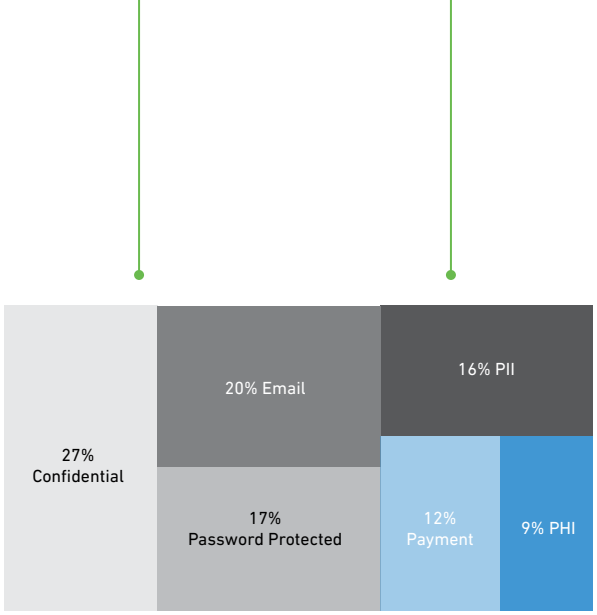
Even if an all-cloud initiative is not immediately in motion, it's likely your organization will be moving at least some operations into the cloud in the near future. Before taking this step, it's critical to assess how you will go about securing cloud operations by understanding related security and compliance issues. Fortunately, a modern security information and event management (SIEM) solution will let your analysts address enterprise cloud security with advanced monitoring and analytics. A modern SIEM automatically collects alert data from across multiple clouds, detects new and emerging threats with behavioral analytics, and helps analysts quickly respond to attacks on cloud applications and infrastructure. This white paper describes how a modern SIEM can help you combat increasingly targeted and complex attacks and insider threats. It also provides case studies to show how a modern SIEM augments other cloud security solutions like identity and access management (IAM) and cloud access security broker (CASB) to better detect, investigate and respond to cloud-based attacks while minimizing the detection of false positives.

The Need for Cloud Security

There are several approaches for moving to cloud computing. Some organizations have been slow to move to the cloud; some go cloud first via Infrastructure as a Service (IaaS) or Software as a Service (SaaS) having deployed almost everything formerly on premises into the cloud; while the vast majority of enterprises are in the middle with a hybrid model. Most "apps" are now cloud-based and used with a web browser or mobile device.

[1] SecurityIntelligence.com.

Many apps are tailored to very specific, individual roles. An audit of apps used by an enterprise often surprises stakeholders by how many cloud services they use. A large organization now uses an average of about 2,000 cloud services, a number that is increasing by double-digits year-on-year.[2] More cloud services launch every week and the percentage of cloud services that are enterprise-ready continues to increase. Leading public cloud providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform as well as cloud services like Salesforce, Office 365, Google Apps for Work and several of their security applications.



TYPES OF SENSITIVE DATA STORED IN THE CLOUD (SOURCE: MCAFEE)

With the widespread use of public cloud services, organizations increasingly store sensitive data in the cloud. According to our partner McAfee,[3] during 2018, 27 percent of all documents uploaded to cloud-based file sharing and collaboration services contain sensitive information. Of that, 5.6 percent is confidential data (e.g. financial records, business plans, source code, etc.) and 3.3 percent contains personally identifiable information (Social Security numbers, tax ID numbers, etc.). Another 2.3 percent contains payment card information and 1.8 percent contains personal health information (e.g. medical record IDs, patient diagnoses, etc.). There is a good chance if you have data in the cloud, your cloud data includes some of these sensitive data sources. Which is why securing those data and payloads operating on public clouds should be a high priority!

DEFINING THE CHALLENGE OF CLOUD SECURITY

Defining the challenge of cloud security starts by acknowledging who is responsible for what. This quest depends on how your enterprise is using the cloud. For example, a legacy IT scenario is where the enterprise hosts everything – so the enterprise is also responsible for securing everything. For a SaaS application, back-end security for apps and data is handled mainly by the SaaS provider; access security rests with the enterprise and its users. For scenarios using IaaS, a shared responsibility model is used where the cloud provider secures the back-end data centers, networking, servers, and virtualization; the enterprise is responsible for protecting cloud payloads such as operating systems, databases and applications.

Securing a hybrid scenario requires particular scrutiny. As more workflow shifts into the cloud, more data (often sensitive) is created and shared in the cloud. For example, during 2018, 48.3 percent of files in file sharing and collaboration applications – like Box, Dropbox, Google Drive and Microsoft OneDrive – are shared.[4] Many of these and other files are created in the cloud and thus never cross the corporate network. Cisco estimates that "by 2021 more than 95 percent of data center traffic will be cloud traffic."[5]

[2] Source: McAfee, Cloud Adoption and Risk Report 2019 at https://cloudsecurity.mcafee.com/cloud/en-us/forms/white-papers/wp-cloud-adoption-risk-report-2019-banner-cloud-mfe.html; see p. 3.

[3] McAfee report, pp. 5-6.

[4] McAfee report, p. 7.

Traditional network security won't be monitoring these documents.

Despite this massive exposure of sensitive data and expectation of shared responsibility by cloud service customers, only one percent of security professionals have cloud security as their primary job responsibility; just 28.5 percent say it is part of their responsibilities.[6] Clearly, there is a misalignment of expectations vs. need.

The enterprise-side task of securing its apps and data in the public cloud starts with ensuring that configurations are properly established and maintained. According to one survey, the misconfiguration of cloud platforms jumped to the top spot as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure application programming interfaces or APIs (50 percent).[7]

In addition to ensuring that configurations are secure, responsibility for securing its cloud payloads rests exclusively with the enterprise. Interestingly, while virtual cloud infrastructure is physically different from on-premises infrastructure, the threats affecting cloud workloads are exactly the same ones affecting on-premises applications and their data. Fulfilling the enterprise's responsibility for cloud security requires the use of the right tools and methodologies.

> "Through 2020, at least 99% of cloud security failures will be the customer's fault."
>
> **GARTNER, MAGIC QUADRANT FOR CLOUD ACCESS SECURITY BROKERS, 30 NOV. 2017**

Compliance is a final major challenge. Compliance requirements often relate to the deployment and use of security controls. It's important your organization's use of the cloud and associated security tools also meet related compliance requirements for data protection and privacy.

USING THE RIGHT TOOLS

Cloud security leverages the familiar concept of "defense in depth," where a range of tools complement each other to protect different aspects of cloud payloads and data. According to the Netskope report,[8] the three most effective security technologies for protecting data in the cloud are data encryption, network encryption with a virtual private network, and security information and event management.

Enterprises also deploy other security solutions for cloud-based data protection and threat protection. For example, a cloud access security broker tool is a policy-enforcement point between a cloud app's users and its provider that applies enterprise security policies as cloud-based resources. Network intrusion protection is used to monitor and detect threats in cloud network traffic, closing the security gap of workload-to-workload communication.

[5] Source: Cisco Global Cloud Index: Forecast and Methodology, 2016-2021 White Paper at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

[6] Exabeam 2018 Cyber Security Salary and Job Report, pp. 19-20 at https://www.exabeam.com/wp-content/uploads/2018/05/EXA_Salary-Survey-Report_L1R6.pdf

[7] Netskope 2018 CyberSecurity Insiders Cloud Security Report at https://resources.netskope.com/cloud-security-reports-1/2018-cloud-security-report

[8] Ibid.

Server protection for IaaS workloads is used to defend against advanced attacks. And single sign-on (SSO) tools are used to control access to cloud-based resources.

Most of these other technologies are protection oriented. They are designed to try to stop breaches. Just as with on-premises protection tools, however, attackers are sometimes able to navigate past this "virtual defense in depth" approach. For this reason, it's important to consider cloud security as being about more than just passive protection. Robust cloud security requires the enterprise to proactively protect, detect and respond to attacks in the cloud. Using a modern SIEM has become the essential fulcrum for addressing the latter requirement.

HOW A MODERN SIEM SECURES CLOUDS

A modern SIEM is uniquely capable of ingesting and behaviorally analyzing all security alert data from any cloud or on-premises data source to empower enterprises to detect, investigate and respond to cyberattacks more efficiently. To effectively function as a cloud cyber-cop, the modern SIEM needs multiple API-based connectors to enable the ingestion of alert data from any source you need to ensure cloud security. It also may ingest on-premises data sources into a hybrid multi-cloud environment. Security operations center analysts will be pleased to note that the way an enterprise uses a modern SIEM for cloud security is exactly the same process as for protecting on-premises infrastructure. Generally, this process flow is:

- Logs are ingested and centralized into a SIEM.
- An alert fires either from a security tool like FireEye or from a correlation rule in the SIEM itself.
- This triggers an investigation, where analysts review evidence gathered in their SIEM.
- Evidence is processed into an incident timeline. At this point, an analyst has an idea of what's going on, what systems and users were impacted, and what they should do about it for remediation.
- Based on the timeline, the analyst can now respond to an attack.

It is helpful to describe this process of detection, investigation and response in more detail specifically as it applies to cloud security.

MULTIPLE PATHS FOR MODERN SIEM/CLOUD INTEGRATION

Cloud-direct integration – Many public cloud services offer well-defined mechanisms for pulling activity logs into third-party systems. For example, salesforce.com offers very powerful logging to its customers. Salesforce Event Log Files (ELF) enable products such as Exabeam to collect and classify activity logs. For other applications, check that your SIEM vendor has a content team developing connectors that are critical for your environment.

Cloud-proxy integration – Some organizations also use web proxies as a means of controlling and monitoring cloud and web activity. For example, SonicWALL or Barracuda web gateways might be used to collect activity outside of the corporate data center. A modern SIEM can ingest this data.

Cloud-broker integration – The third approach to cloud monitoring is the cloud access security broker or CASB. Gartner recently recommended CASB as an approach for securing and monitoring cloud activity. A modern SIEM can ingest activity and log data from CASB products. It can also incorporate a combination of approaches described in this paper.

DETECTING THREATS WITH A SIEM

Detection comes after the ingestion of log data. The first step for data analysis is to build a baseline of normal user and device behavior. For example, how often does a user access their cloud email? What size files does the user typically send out by email or share on a cloud storage application?

Once you have baselined normal behavior, you can then add risk points for anomalous, high-risk activity. For example, detecting first-time access to a cloud service from a new country or device is a potential security issue. Other examples may include repeated failed logins; service accounts logging into a cloud service; and access during an unusual time of day. Using a modern SIEM to detect anomalous events is important because they typically flow past the radar of legacy tools.

The SIEM analyzes cloud and on-premises logs to create risk scores. If risk points add up and cross a threshold you've set, the person, device or network can be short-listed for investigation. The advantage of risk scoring is that it also helps with prioritizing what to investigate.

Legacy SIEMs typically use correlation rules, which are limited in scope. To use them, you have to know what type of attack you are looking for. On the other hand, a modern SIEM with user and entity behavior analytics (UEBA) helps address unknown attacks, insider threats, and other types of complex attacks. By baselining normal behavior, then adding risk points for anomalous, high-risk activity, UEBA is able to accurately uncover threats.

USE CASE: SIEM AUGMENTING IAM

Identity and access management (IAM) tools are used to ensure that only authorized people can access specific cloud services. Exabeam's SIEM augments IAM capabilities by placing a user's activity from a session into a timeline. In conjunction, the SIEM also detects behavioral anomalies and notes risks related to the session. The aggregation of risks in user sessions and notable sessions are automatically sent to the integrated IAM tool. The IAM uses this data to take appropriate enforcement action on the user before granting access to cloud resources.

A major benefit of UEBA is providing results with fewer false positives and maintenance inherent to static correlation rules. Its modeling is further improved when baselines take into account the behavior of groups of users like people in the same department, or that work at the same office. This granularity of analytics provides greater accuracy in spotting anomalous behavior.

INVESTIGATING INCIDENTS WITH A SIEM

We mentioned earlier that a SIEM allows you to collect both cloud and on-premises data. One of the advantages of this integration is that you can build a timeline to learn about all of the activities before, during and after an attack. Traditionally, this timeline was created by analysts who must gather evidence by querying and pivoting in their SIEM. A modern SIEM automatically combines sequence, behavior, identity, and scope into a pre-processed object. This result can be instantly retrieved whenever needed, for example while threat hunting.

Modern SIEM technologies and processes like user-device-IP mapping provide deeper visibility to help you improve cloud security by combining it with other data sources so you can build a more complete, accurate timeline. Accuracy is valuable because typical attacks include several phases. Those phases can start, traverse and/or end in the cloud. Using a modern SIEM will help identify threats in this vector.

RESPONDING TO ATTACKS WITH A SIEM

Security analysts can respond to attacks with a modern SIEM by using a corresponding playbook to address each of the constituent parts of an attack. For example, the analyst might run a phishing playbook to address phishing in cloud email, a malware playbook to address the malware it installed in the cloud and/or on-premises, and a data exfiltration playbook to identify or stop potential data loss from that malware in a cloud application.

Some SIEMs improve incident response team productivity with security orchestration, which entails pre-built connectors to IT and security infrastructure used to pull data or run actions. The real value is enabling response playbooks with full workflow automation. These playbooks can be run in a fully or semi-automated manner to perform an investigation, containment or response. None of this is provided by legacy SIEMs.

USE CASE: SIEM AUGMENTING CASB

Cloud access security broker (CASB) tools are used to ensure that only authorized people can access sanctioned cloud services. Exabeam's SIEM augments CASB by receiving its cloud events via integration. The SIEM analyzes cloud and on-premises logs to create risk scores based on location, device, cloud service, user identity, activity and other factors. The scores enable a security analyst using the SIEM to investigate incidents such as compromised credentials. The integration of SIEM scoring allows a higher degree of security for cloud services by using CASB security policies and access controls.

OTHER CLOUD USE CASES FOR SIEM

Lateral Movement

A breach through the most innocuous entry point of an organization's network may quickly become a proverbial hole in the dike with undetected lateral movement. This can be a big problem if security tools do not have visibility into a public cloud. The process of lateral movement entails systematically moving through a network in search of sensitive data and assets. Perhaps the attack began by compromising a low-level employee's account. Once inside, the hacker probes other assets for vulnerabilities in order to switch accounts, machines and IP addresses. Opportunity knocks once the attacker secures administrative privileges. Lateral movement is extremely difficult to detect by legacy security tools because parts of the attack are scattered across the IT environment, spread among different credentials, IP addresses and machines; the seemingly unrelated events all appear to be normal.

Data Leakage

Data leakage occurs when sensitive information leaves an organization without authorization. It can happen when a user transfers data over the internet or copies it to a physical device and moves it outside the premises.

A large apparel company encountered such data theft from cloud-based applications by departed employees. In this situation, Exabeam's SIEM identified anomalous GitHub access by several just-terminated employees. The SIEM used an integrated feed from the company's human resources system that flagged the individuals' employment as having been terminated. With Exabeam's SIEM, the company was able to identify the attack and stop data theft. Had the company been using only legacy network access control, it would have been unable to identify the theft because the users had valid credentials.

USE CASE: DETECTING LATERAL MOVEMENT

A global engineering firm encountered lateral movement when a malware compromised machine was performing "Pass-the-Hash" attacks to move laterally in the network. This exploit re-used a stolen (and uncracked) hashed user credential to trick an authentication system into creating a new authenticated session on the same network. Exabeam Advanced Analytics identified unusual virtual machine (VM) creation activity and anomalous naming conventions for these VMs. Combined with other anomalous activity, the machine and user were flagged as notable and escalated to analysts. The compromised machine was quarantined before it was able to exfiltrate sensitive data from the firm.

USE CASE: ENSURING COMPLIANCE

A publicly traded cyber security company used a private cloud to store sensitive customer information. It found that compliance with the SOC 2 regulation took too much time. With Exabeam's SIEM, the company was able to use machine-generated Exabeam Smart Timelines™ and out-of-the-box reporting that proved to auditors that it was able to track malicious actors. The company experienced increased productivity by SOC analysts by automating previously manual tasks involved in investigations. In addition to achieving timely SOC 2 compliance, the company's productivity gains delayed the need to hire an additional analyst.

Compliance

Maintaining compliance in the cloud can be daunting. Cloud infrastructure has more servers and instances than traditional on-premises infrastructure. Cloud assets are also ephemeral and after they are spun up, the duration of their existence can be weeks, days, hours, minutes, or even just a few seconds. Ensuring compliance requires capturing and analyzing cloud logs of all activity.

ABOUT SIEM PRICING …

The pricing model for a SIEM is important because cloud logs are chatty. The average organization today generates billions of unique transactions in cloud services each month (including user login, uploading files, editing documents).

For security, the more information you have to analyze, the better because you potentially get more clues for an investigation. One downside is that cloud services can lead to excessive logging costs as most SIEM vendors charge based on the volume of log data ingested into the tool. Security analysts refer to this issue as the so-called "Splunk tax," which is a familiar example. One impact of the volume-based pricing model is that it can also cause organizations to limit data sources, which creates blind spots for analysts.

The solution is finding a vendor that offers flat-rate pricing. An alternative pricing model, for example, may charge based on the number of users and the number of devices. The flat-pricing model also provides the benefit of greater predictability.

No matter which integration you choose (direct, proxy, broker or some combination thereof), ingested cloud logs can be combined with other types of logs. These logs may come from your network, on-premises applications, devices and other big-data stores to name a few – the combination of which provides a full picture of cloud activity used by your organization.

EXABEAM AND CLOUD SECURITY

Exabeam's modern SIEM addresses cloud security in multiple ways to ensure the protection of sensitive data, applications and infrastructure. The Exabeam Security Management Platform:

- Collects alert data by direct ingestion from dozens of cloud security tools and popular cloud-based services across multiple enterprise clouds, in addition to hundreds of other products.
- Detects new and emerging threats with behavioral analytics.
- Augments detection with the Exabeam Threat Intelligence Service, which improves threat detection accuracy with a daily updated stream of indicators of compromise (IoCs) such as malicious IP addresses and domains.
- Provides machine-built timelines to improve analyst productivity and reduce response times by automating incident investigation.
- Includes response playbooks using pre-built connectors and hundreds of actions to contain and mitigate threats.
- Can be deployed on premises, in cloud IaaS or as SaaS.
- Is licensed using flat, predictable pricing based on the number of employees.
- Augments other cloud security solutions like IAM and CASB to better detect, investigate and respond to cloud-based attacks while minimizing the detection of false positives.

exabeam

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.

SUMMARY

Wherever your organization is on its cloud journey, ensuring the use of appropriate technology and processes is critical for protecting sensitive data and applications stored, processed or transmitted in public clouds. For cloud security and compliance, the use of a modern SIEM is essential to equip your organization's analysts with the capabilities they need for 360-degree visibility of cloud-borne threats. A modern SIEM with advanced monitoring and analytics from Exabeam will automatically collect alert data from across multiple clouds, detect new and emerging threats with behavioral analytics, and help analysts quickly respond to attacks on cloud applications and infrastructure. To learn more about how Exabeam can help your organization to combat increasing targeted and complex attacks, insider threats, and augment capabilities of other security tools, please contact Exabeam for a demonstration at Exabeam.com/demo.

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit https://www.exabeam.com.