SECURONIX™

Securing the Cloud:

Protecting Your Enterprise From an Expanding Threat Surface

www.securonix.com

Why Do You Need Cloud Security?

In the past, organizations existed within clearly defined boundaries. Security teams could protect the perimeter by securing critical data within company owned and managed data centers. But digital transformation, globalization, the cloud, and workforce mobility has spread data and users far beyond the perimeter of traditional office networks and data centers. Many business applications are cloud based, and a number of public cloud providers like Amazon Web Services, Google Cloud Platform, Oracle, and Microsoft Azure are being adopted by organizations large and small.

The benefits that cloud offers to organizations – such as the ability to scale as needs change, the reduction of operational costs, and the reduction of infrastructure overhead – are great. However, when adopting cloud solutions, many organizations fail to balance the benefits of the cloud against the threats and challenges that cloud introduces: a lack of visibility and control over assets, data privacy issues, data loss, user access controls, insecure API, denial of service (DOS or DDOS) attacks, and compliance issues. Cloud data attracts more sophisticated attackers. These attackers study the systems, find flaws, and exploit them for their benefit. According to the 2020 Verizon Data Breach Investigations Report[1], cloud assets were involved in around 24% of breaches, and 77% of cloud breaches involved compromised credentials. Combined with the increasing prevalence of cloud solutions, securing your cloud is more important than ever.

The Cost of Poor Cloud Security

Security leaders and their teams need to view data security and privacy as their highest priority when embracing the cloud. A security breach can cause more damage than just data loss, no matter if it was due to poor cloud security or not. In the Ponemon Cost of a Data Breach Report 2020[2], nearly 40% of the cost of a data breach came from business loss including customers leaving, lost revenue due to focusing on remediating the breach, and the increased cost of acquiring new customers. In the study, the average data breach cost was around $1.52 million.

Damage to Brand Reputation

A security breach impacts an organization's reputation. Loss of reputation can result in a lack of confidence among prospective buyers, users, partners, and shareholders. Loss of customer confidence can also cause customers to not renew contracts, incurring monetary losses for the organization, not to mention new business and sales that may not occur.

[1] https://enterprise.verizon.com/resources/reports/dbir/
[2] https://www.ibm.com/security/data-breach

Loss of Intellectual Property

Attackers target intellectual property such as product designs, strategies, and blueprints. Losing this proprietary technology can impact the competitiveness of your business and decrease future business' growth.

Fines and Customer Settlements

Regulatory fines may be levied in the case of a compliance violation. Organizations such as the U.S. Securities and Exchange Commission (SEC), Consumer Financial Protection Bureau (CFPB), and the EU Information Commissioner's Office (ICO) are a few examples of agencies that will fine a business for non-compliance. In fact, British Airways was fined $100 million for GDPR violations for their 2018 data breach.[3] Compensation for customers affected by the breach may also be required depending on the industry and violation.

Revenue Loss

The overall financial impact of a security breach can cost millions of dollars and has forced some organizations to go out of business. This impact is not confined to fines and cancelled contracts but may also include revenue the company misses out on while they work to isolate and remediate the attack, instead of focusing on business priorities.

Remediation and Hidden Costs

Most breached organizations hire an outside firm to investigate and remediate an attack to ensure speedy resolution. After remediating the immediate threat organizations may purchase new security solutions to detect and protect against future attacks in a more comprehensive way. In addition to the cost of incident response there are several other related costs, including legal fees, press relations, breach insurance premiums, and more.

Cloud Security Requires New Solutions

Security tools built for on-premises infrastructure does not work well against cloud threats. Rules-based threat detection was designed to protect against known threats. As threats become more sophisticated, solutions that are able to detect changes in behavior are required in order to catch insider threats and zero days. Cloud security also requires a solution that can monitor all aspects of the cloud, including cloud infrastructure, cloud data sharing applications, cloud enterprise applications, and cloud access management tools.

A cloud based SIEM empowers enterprises to detect, investigate, and respond to cyberattacks efficiently. It shortens the time needed to detect and respond to threats and gives you full visibility across your environment.

[3] https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

Important Features To Look for in a Cloud SIEM

Cloud Data Encryption

To ensure cloud data security and prevent tampering, you need to securely encrypt data at rest (data stored in the cloud) and data in motion (data in transit or being accessed), as well as use a secure channel while accessing or uploading data. For encryption to be effective, it must travel with the data, whether at rest or in transit, as well as during export and backup. Data in motion should be protected using a secure communication protocol such as HTTPS to access the data and utilizing multi-factor authentication (MFA) over VPN connections.

Data Management

One of the best ways to limit data leakage is to control access to sensitive information. This includes maintaining an inventory of sensitive information, encrypting sensitive data (as mentioned above), and limiting access to authorized cloud and email providers. Role-based access control (RBAC) and the ability to monitor privileged users is key to be able to alert on data management and access anomalies.

Enterprise application data today resides in both on-premises and cloud datastores so ensuring this data stays secure is important. Identity and access management (IAM) solutions are often the first line of defense and having poorly managed or improper identity management makes your data vulnerable to attacks. With multiple access privileges for each user across a multitude of applications to manage, organizations struggle to keep their access-related risk in check. However, with advanced analytics designed to work with IAM solutions, security teams can use context from the IAM to make dynamic, informed access decisions.

Threat Hunting

Threat hunting consists of searching iteratively on data for specific threats that may have evaded your existing security. Threat hunting may include searching on cloud and on-premises data in real time, as well as searching for threats in historical data.

Look for a cloud SIEM that can search across live and historic data, no matter where that data resides, in addition to running analytics to find possible threats on its own. Look for a SIEM that offers integrations with industry standard threat intelligence communities such as MITRE ATT&CK and Sigma.

Analytics-Based Threat Detection

Rule-based threat detection has a difficult time detecting threats in the cloud. A cloud based SIEM with integrated user and entity behavior analytics (UEBA) is able to detect advanced attacks and insider threats across your entire environment, including the cloud. By baselining user behavior and detecting anomalous, high-risk activity, behavior analytics is able to accurately uncover threats with fewer false positives than rule-based approaches.

Cloud Based /Cloud Hosted SIEM

Many on-premises SIEMs have minimal visibility and control over cloud data because they lack robust integrations. Cloud native SIEMs addresses this limitation, providing cloud security monitoring through two-way, deep integrations with cloud applications and services. Cloud native solutions can provide massive scale and high performance with an on-demand model that can ramp up or down, depending on your organization's needs.

Look for a cloud SIEM that integrates with your cloud infrastructure, so your team doesn't have to build the connections it needs.

Wider Integration With Your Environment

Beyond cloud integrations, ensure your cloud SIEM also has multiple API based connectors that enable the ingestion of data from across your entire environment. Cloud SIEMs that offer built-in integrations with a large ecosystem of security vendors will be able to provide even faster detection and response to threats.

Securing your Cloud with Securonix Cloud SIEM

Cloud Data Encryption

As explained in an earlier section, data encryption is important to ensure data integrity. All data processed and stored by the Securonix platform is encrypted while at rest using file- or disk-level encryption mechanisms as required. Data sent to and from the cloud, which includes data collected or ingested via APIs and plugins as well as interaction with the user interface, is encrypted.

Securonix customers can also take advantage of a fully managed, centralized key management system to protect your data privacy. You can encrypt your organization's cloud data with your own keys (BYOK) or AWS Key Management System (KMS), as well as manage risk, compliance, and conduct audit and forensic investigations.

Data Management

Controlling access to sensitive information is one of the best ways to limit data leakage or tampering. Securonix applies advanced behavior analytics to identity usage and access patterns in data collected from IAM solutions such as Saviynt, Okta, Ping Identity, and SailPoint. This enables the creation of risk profiles for user behaviors, which can be used by the IAM solution to make dynamic, informed access decisions. The integration delivers advanced identity analytics and intelligence capabilities, enabling several use cases that are otherwise difficult for IT security teams to manage. IAM ensures that only valid users have authorized access to corporate data, and users are only granted access as required as part of their job.

Threat Hunting

Securonix uses threat chain models that provide full attack context to help SOC analysts validate and respond quicker to threats. Securonix threat chains are based on industry standard threat modelling, including the MITRE ATT&CK framework and US-CERT Cybersecurity Framework, to stitch together related alerts.

Threat hunters need to be able to search for undetected threats on both real-time and historical data. Securonix is able to leverage its cloud native, big data architecture to decouple search and compute resources, providing organizations with quicker results. Securonix allows SOC teams to search and act on live streaming data with virtually zero latency. It also allows security teams to also perform high-performance searches on long-term data and real-time data.

Analytics-Based Threat Detection

Using a rule-based approach security teams may miss alerts for sophisticated or zero-day threats. Securonix Next-Gen SIEM, with integrated UEBA, uses patented machine learning algorithms to detect advanced and insider threats more accurately by reducing false positives. Behavioral analytics builds a comprehensive risk profile of users based on identity, employment, security violations, IT activity and access, physical access, and even phone records. All identity, activity, and access characteristics are compared to an individual's baseline, their peers' baseline, and known threat indicators in order to identify true areas of risk. Securonix comes with out of the box use cases delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time to value.

Cloud Based /Cloud Hosted SIEM

Securonix Next-Gen SIEM is built in the cloud for the cloud. Through robust integrations with major cloud applications like Salesforce, Box, and Workday, Securonix cloud connectors make threat detection faster and deliver value to security teams quicker. Securonix also provides security integrations with many major vendors such as Ping Identity, Okta, Netskope, Tanium, CarbonBlack, SentinelOne, and SkyHigh to lower your security team's overall response time. Finally, we offer tight integrations with cloud infrastructure such as AWS, Microsoft Office 365, Microsoft Azure, and Oracle.

Wider Integration With Your Environment

Securonix uses APIs to integrate with, and gain complete visibility and protection over, multiple cloud and on-premises systems. Securonix also simplifies cloud data collection and response with more than 350 built-in cloud connectors, including major cloud infrastructure and applications.

Harness the Power of Securonix Next-Gen SIEM

The adoption of cloud technology is a game changer for both organizations and hackers. The cloud provides an advantage in terms of cost, scalability, and flexibility, but at the same time cloud adoption can make enterprise data vulnerable to new attacks if not monitored properly.

When researching security solutions, remember to examine what capabilities the solutions provide for cloud data encryption, data management and access control, threat hunting, advanced analytics (beyond a rule-based approach), and cloud integrations offered out of the box.

Securonix is a great choice for small and large enterprises seeking the advantages of a cloud native SIEM. By giving our customers their choice of encryption key management, many highly regulated industries such as finance and banking are able to exercise more control over their data security. Our extensive integrations with IAM and identity governance and administration (IGA) solutions help you detect and respond quickly to privileged access management anomalies. Securonix threat chains help SOC analysts respond quicker to threats because they combine related alerts together to give the analyst a complete view of the threat utilizing the MITRE ATT&CK framework. Finally, when you purchase Securonix Next-Gen SIEM, you also receive sophisticated analytics that help you detect and respond to known and unknown cloud threats.

Want to learn more about Securonix? Ask for a demo today.

ABOUT SECURONIX

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NDR, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise, prioritizes high fidelity alerts, and detects and responds to advanced insider and cyber threats with behavioral analytics technology that pioneered the UEBA category.

CONTACT SECURONIX

www.securonix.com
info@securonix.com | (310) 641-1000

0221


SECURONIX™