WHITEPAPER

The Trellix Approach to Effective Cloud Security

Table of Contents

The Double-Edged Sword of Cloud Security

In many ways, the cloud[1] is more secure than a traditional data center. Asset management, inventory, audit logging, two-factor access controls, connectivity redundancy and firewalls are built into the cloud provider platform. Servers are easier to patch and won't become outdated within a few years; there aren't any forgotten boxes sitting in a dark corner with a note reading, "DO NOT TURN OFF." However, assets on the cloud continue to be compromised, just as those stored in traditional data centers.

Cloud Security Challenges

The cloud addresses many historical security operations pain points, but it also introduces new ones that require security practitioners to adapt. In addition to meeting previous security challenges—out-of-date software, proper firewall configuration, effective authorization policies and procedures—the cloud adds multiple tasks to security teams, such as developing new skills, tracking ephemeral assets, managing decentralized accounts ("shadow IT"), protecting data stored using cloud provider platform services instead of servers, and verifying that all platform activity is tracked and authorized.

These new security challenges introduce requirements beyond that of a traditional data center. The blind spots created as a result of using the cloud may create additional surface area for adversaries to leverage and compromise critical and sensitive customer assets. Such compromises could damage business operations and reputation. IT staff are required to learn new technology and skills to secure their cloud environments, but many lack the time and support to do so effectively.

The Anatomy of a Public Cloud Compromise

Many cloud compromises occur without any cloud hacking at all. Instead the attackers use phishing, client-side exploits or victim missteps—and sometimes all three—to acquire and use valid credentials to commit crimes.

Consider the following example of a fictional financial services company that uses analytics to detect fraudulent banking transactions.

[1] Cloud here refers to either / or a combination of public, private, hybrid or multi-cloud set-ups.

In this example, fictional thieves hatch a plot to attack the company's fraud detection directly by manipulating the analytical machine's learning models that find anomalies in transaction patterns. Their goal is to insert fake entries into the source training data so they can make large, fraudulent transactions appear normal. To accomplish this, the attackers must:

- Gain access to a cloud account capable of finding and modifying training files.
- Use the cloud credentials to create an API key.
- Use the API key in a script to enumerate storage locations.
- Search each storage location for the training data.
- Alter the training data to insert large numbers of fake events.

There are many ways for attackers to get access to credentials, from spear phishing and watering hole attacks to installing a remote access trojan (RAT). This is the Achilles heel of cloud security: your security is only as good as the procedures used to secure your access.

If the attacker succeeds when the nightly fraud analytics batch job runs – it will include the altered data with millions of fake transactions added. When the model is created and used the following day, large transfers to a suspicious account will be considered normal. The thieves can then begin issuing fraudulent transactions without the system flagging them.

The first thing to note about this attack is that no exploits are used after the credentials are initially compromised. All the activity adheres to the authorization system's policies. In other words, after the credentials are obtained, behavioral anomaly detection is the only detection method likely to work.

Examples of observables that make this activity stand out:

- Cloud console login from an unfamiliar network.
- Creation of a new API key.
- Increased use of "list" and "describe" API calls used for reconnaissance.
- Alteration of training data from a new source.
- Creation of cloud resources in the cloud provider region that the financial services company normally doesn't operate on.

On their own, these observables are not particularly interesting. They are considered weak signals and need to be aggregated to create something that a security operations center (SOC) analyst would find interesting enough to spend time investigating, this is undertaken via the following steps:

- Collecting and normalizing all relevant events.
- Performing frequency analysis, geospatial analysis, and other analytics on the data.
- Correlating the analytical findings.
- Escalating the findings to a SOC analyst for full review.

To elaborate: All these activities must not only be logged, but also reviewed. This means that SOCs need robust automation techniques for collecting these cloud audit events. Only then can machine learning be applied to help identify when multiple events working together become a pattern. With respect to the presented example, this means watching for new logins, new API keys, API activities and data set alteration. If all of that is happening in tandem, an analyst needs to be notified.

> SOCs need robust automation techniques for collecting cloud audit events. Only then can machine learning be applied to help identify when multiple events working together become a pattern.

Developing a Comprehensive Cloud Security Plan

Critical Components of Cloud Security

To ensure all cloud assets are safe, there are two high-level activities that must be continually undertaken, reviewed and improved: protecting the infrastructure and protecting against misuse of cloud assets.

Protecting the infrastructure

This originally consisted of traditional security in the form of endpoint, network and email security mechanisms. Our example showed how non-cloud email and on-premise hardware can be compromised and used in a cloud attack. Therefore, both cloud and traditional on-premise assets should be in-scope when considering the overall security posture for the cloud.

However, modern cloud security infrastructure protection must incorporate security controls native to the cloud provider's control plane and management system. This means that it's just as (or more) important to implement sound cloud infrastructure management policies for network and identity as it is for traditional host-based controls. These protections should:

- Enforce guardrails to allow developers to move quickly while ensuring mistakes won't lead to immediate compromise.
- Make complicated cloud environments simpler by consolidating management consoles to reduce the chance of neglect.
- Automate risk surface reduction tasks for activities such as network policies so that permissions start out as specific as possible, making it more difficult for an attacker to get access.

Protecting against misuse of cloud assets

A comprehensive and effective cloud security plan should include contingency capabilities for when (not if) traditional defenses are bypassed by a determined attacker. This requires the detection of misused cloud assets through analytical methods including big data, artificial intelligence and machine learning.

Collecting and Analyzing All Relevant Data

Most organizations starting a cloud security program understand the importance of collecting authentication and authorization data, but that's only half of the story. Comprehensive security means collecting usage data for visibility through various means, such as:

- Container operational logs
- Object storage read and write logs
- Policy configuration logs
- Network flow logs
- Application logs
- Load balancer logs
- Function-as-a-service and other serverless logs

Each of these logs should be collected centrally and normalized into usable data points.

After collection and normalization, teams need to perform analytics on individual types of data, such as:

- Geographically anomalous logins
- Quantitatively anomalous logins
- Quantitatively or qualitatively anomalous API calls
- Anomalous data transfers

The analytical output of these calculations must then be correlated to find intersections of importance. Failing to perform this step will result in tactically redundant information for SOC analysts.

Covering All Cloud Environments

Ensure data is collected from all cloud platforms in use (such as, Google, Microsoft, Azure, AWS), and perform analytics and correlation in a single, consolidated place. Software-as-a-service (SaaS) clouds today handle things such as human resource information systems, accounting, sales force information systems, travel systems, payroll and much more. Most major SaaS offerings have logging APIs that you can connect to your analytics solution and failing to integrate these data sources will create serious security blind spots.

Training Your Analysts for Cloud Security

Even though cloud adoption is increasing rapidly, security analysts find their capability maturity lagging. Ensure that your organization is purposefully training analysts in the latest cloud detection procedures, including how to interpret both security analysis findings and traditional security alerts.

Take advantage of training that your cloud providers offer and include that training in your standard onboarding procedures for new employees.

Building In-Cloud Security

Your engineering architects should be fluent in cloud security and the creation of solutions with built-in instrumentation, telemetry and auditing capabilities for automated security analytics. This is especially critical for container-based or serverless apps that cause problems for traditional security protection and monitoring programs.

When building new apps, there should be a security architect involved at all phases, starting with the initial planning.

Leveraging Your Cloud Provider for Built-In Data and Security

Your cloud provider will already have an array of data to collect as part of their security obligations, as well as some low-level, built-in solutions that can work with your overall cloud security program. In many cases, incorporating these native solutions may be the only way to collect certain types of data, such as DNS query information.

Be certain that your SOC and incident response team have a good line of communication with your cloud provider's help desk. This will ensure that security notifications originating from your provider will make their way to the right team members. It will also enable security staff to ask the cloud provider questions when performing incident investigations.

> Your cloud security is only as good as the procedures used to secure your access.

The Trellix Approach

Cloud security requires all the traditional security solutions that cover network, endpoint and email, enhanced with visibility and analytics-based capabilities. Trellix approaches cloud security holistically to provide protection, visibility and detection technologies alongside a comprehensive range of services to help with security assessment, staff expertise training and augmentation.

Cloudvisory

Trellix Cloudvisory is a control center for cloud security management that delivers visibility, compliance and governance to any security environment. Cloudvisory runs cloud-native microservices for asset discovery and compliance scanning to enable end-to-end automation of detection and response for complex multi-cloud environments.

Cloudvisory delivers:

- Uniform visibility into disparate, multi-cloud infrastructures through a single console
- Reduced risk of cloud security misconfiguration
- Automation for compliance reporting to keep security staff focused on advanced tasks like threat hunting instead of audit preparation

Looking Ahead

Industry trends show a substantial migration of workloads to the cloud and the rapid adoption of cloud-based software-as-a-service offerings signify that it will continue for quite some time.

As the cloud grows, so do the security threats. Credential abuse, misconfigurations and lack of visibility creates vulnerabilities for targeted attacks. A suitable strategic approach can mitigate these risks.

Cloud security through Trellix protects traditional on-premise workloads from being leveraged for cloud attacks. Our solutions natively integrate with cloud providers to add protection, detection and visibility for existing cloud workloads at scale. As environments and attackers change, our ongoing innovations help our customers meet new security challenges and prevent advanced attacks that go undetected by traditional security measures.

Trellix

Visit Trellix.com to learn more.

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.