DATASHEET

NetApp Cloud Insights—Cloud Secure

A feature of Cloud Insights for ransomware detection and user data access auditing

NetApp

Why you should care

The threat from ransomware attack is very real. The frequency of ransomware attacks increased 41% in 2019, and an attack is forecast to occur every 11 seconds in 2020. Every attack has the potential to cost your company business and damage your brand. Furthermore, the average recovery time from an attack is 16 days, and 67% of businesses hit by an attack permanently lost all or part of their data.

Additionally, if your company is required to comply with standards like HIPAA/HITECH, GDPR, CIPA, and CJIS, you need a way to provide data usage reporting to satisfy auditing requirements for security compliance.

NetApp Cloud Secure

NetApp® Cloud Secure, a feature of NetApp Cloud Insights, analyzes data access patterns to identify risks from ransomware attacks. It reports access activity from insiders, outsiders, ransomware attacks, and rogue users. Advanced reporting and auditing make it easy to identify violators and possible threats. Unlike perimeter security tools, which assume that insiders are trusted, Cloud Secure assumes zero trust for everyone. All activities on the supervised shares are monitored in real time. The data is used to automatically identify the working communities of all users. The ability to audit all documents access helps you to ensure compliance with regulatory requirements.

How Cloud Secure works

Cloud Secure does not assume a trusted internal network; it takes a trust no one approach. It inspects and analyzes all data access activity in real time to detect malicious behaviors.

Cloud Secure performs four major functions:

- **Monitor user activity**

To accurately identify breaches, every user activity across on-premises and hybrid cloud environments is captured and analyzed. The data is collected using a lightweight, stateless data collector agent installed on a VM in the customer's environment. This data also includes user data from Active Directory and LDAP servers and user file activity from NetApp ONTAP® and Cloud Volumes ONTAP.

Key benefits

- Detect ransomware attacks before it's too late
- Minimize the impact of an attack with automatic data backup
- Gain visibility into malicious user activity and identify potential policy risks
- Easily satisfy audit reporting requirements, saving time and money
- Simple SaaS solution, quick time to value, no upgrades, scalable from single departments to global enterprises

Cloud Secure detects anomalies in user behavior by building a behavioral model for each user. From that behavioral model it detects abnormal changes in user activity and analyzes those behavior patterns to determine whether the threat is ransomware or a malicious user. Using this behavioral model reduces false positive noise.

- **Detect anomalies and identify potential attacks**

Today's ransomware and malware are sophisticated, using random extensions and file names which makes detection by signature-based (blocked list) solutions ineffective.

Cloud Secure uses advanced machine learning algorithms to uncover unusual data activity and detect a potential attack. This approach provides dynamic and accurate detection and reduces false detection noise.

- **Automated response policies**

Cloud Secure alerts you and automatically takes a data snapshot when it detects risky behavior, making sure that your data is backed up so that you can recover quickly.

- **Forensics and user audit reporting**

Cloud Secure provides a graphical interface to slice and dice activity data to perform data breach investigations and generate user data access audit reports. It allows multiple views of file data activities by user, time, activity type, and file attributes.

These capabilities make it easy to generate user data access audit reports and conduct data breach and security incident investigations. Data is kept for 13 months, to allow continuing forensic analysis.

> **"We recently experienced a ransomware event, and when we saw what Cloud Insights ransomware detection provides, we were sold."**
>
> Director of IT, Transportation Company

Summary

Cloud Secure provides a simple turnkey solution to ransomware detection and user data access auditing. It requires minimal effort to start and delivers quick time to value, requiring no manual rules configuration and no professional services to set up.

Cloud Secure provides automatic anomaly detection based on artificial intelligence and machine learning. Because it is offered as SaaS, it requires no manual upgrades or maintenance. And it's scalable from single departments to global enterprises.

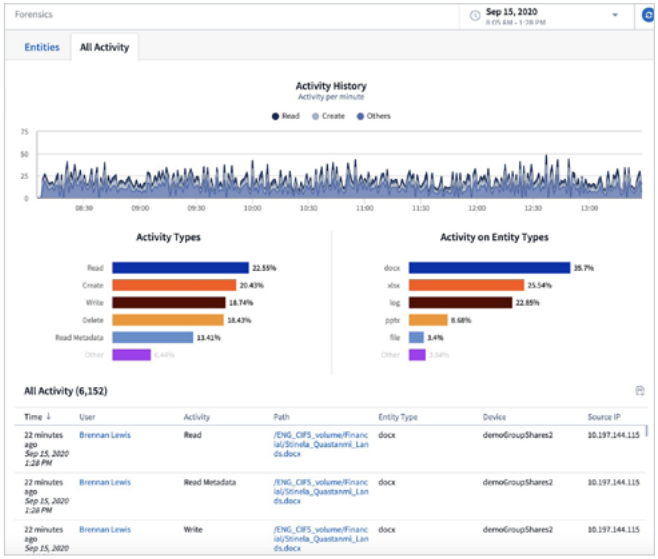
Learn more and sign up for the 30-day free trial.

Cloud Secure dashboard showing user activity.

About NetApp

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services and applications to the right people—anytime, anywhere.



Cloud Secure dashboard showing user activity.

NetApp