DATASHEET

NetApp Cloud Insights Storage Workload Security, providing ransomware and insider threat protection

NetApp

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

Why you should care

The threat from ransomware attack is very real. Currently, an attack occurs every 11 seconds[1], and that frequency is expected to increase to every 2 seconds by 2031. Every attack has the potential to cost your company business and damage your brand. A global cyberattack study shows that the average unplanned downtime is 14 hours[2] at a cost of $200K per hour. Furthermore, 80% of businesses hit by an attack suffered a loss of business and/or revenue. Cyberattacks are increasing as organizations move more business applications to the cloud. That makes data security more important than ever.

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.

The Cloud Insights Storage Workload Security (formerly known as Cloud Secure) features are available as a part of NetApp® Cloud Insights.

Data access patterns are analyzed real-time to identify risks from ransomware attacks and reports anomalous access activity from insiders, outsiders, ransomware attacks, and internal 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, Storage Workload Security assumes zero trust for everyone. All user 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 helps you to ensure compliance with regulatory requirements.

How data security works

Even from users on a trusted internal network, Cloud Insights Storage Workload Security does not assume that all users actions are to be trusted; it takes a trust no one approach. It inspects and analyzes all user data access activity in real-time to detect malicious or anomalous behavior.

Cloud Insights Storage Workload Security performs four major functions:

1. 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.

Cloud Insights Storage Workload Security 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. In addition, Cloud Insights integrates ransomware alerts generated by ONTAP storage to enrich the behavior analytics to further reduce this noise.

Key benefits headline

- Detect ransomware and insider threats before it's too late
- Minimize the impact of an attack with automatic data backup and user restriction
- 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
- Restricts data access upon detecting potential attack

2. 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 Insights Storage Workload Security 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.

3. Automated response policies

When Cloud Insights Storage Workload Security detects unusual user behavior, it alerts you and follows automated policy actions. It takes a Snapshot™ copy of your data and makes sure that the data is rapidly backed up so that you can recover quickly and restrict data access to prevent further compromise.

4. Forensics and user audit reporting

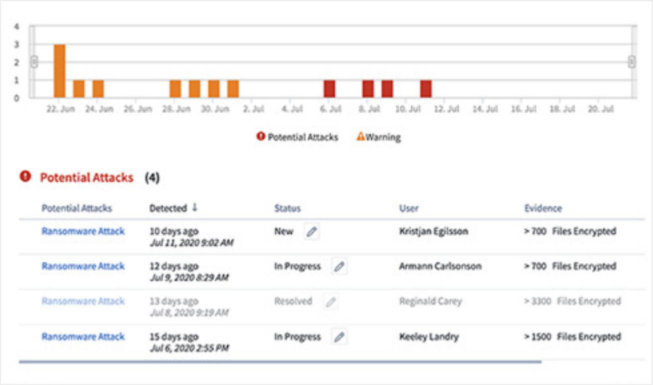
Cloud Insights Data Security provides a graphical interface to slice and dice activity data to perform data breach investigations and generate user data access audit reports. It allows multiple views of file data activities by user, time, activity type, and file attributes. These capabilities make it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

Summary

Cloud Insights Storage Workload Security offers 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 Insights Storage Workload Security 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

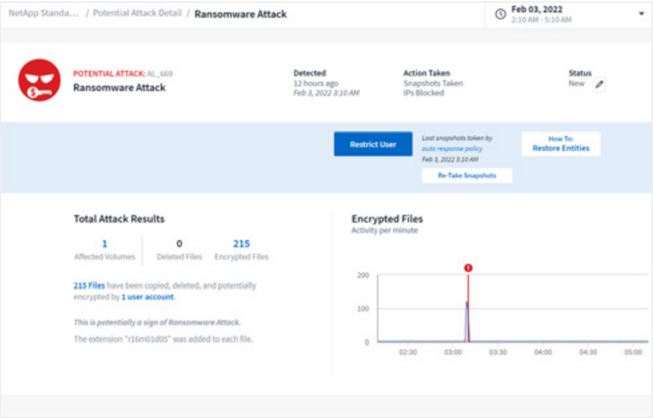
Learn more and sign up for the 30-day free trial.



Potential Attacks (4)

Potential Attacks	Detected ↓	Status	User	Evidence
Ransomware Attack	10 days ago *Jul 11, 2020 9:02 AM*	New	Kristjan Egilsson	> 700 Files Encrypted
Ransomware Attack	12 days ago *Jul 9, 2020 8:29 AM*	In Progress	Armann Carlsonson	> 700 Files Encrypted
Ransomware Attack	13 days ago *Jul 8, 2020 9:19 AM*	Resolved	Reginald Carey	> 3300 Files Encrypted
Ransomware Attack	15 days ago *Jul 6, 2020 2:55 PM*	In Progress	Keeley Landry	> 1500 Files Encrypted

Figure 1: Storage Workload Security dashboard showing user activity.



POTENTIAL ATTACK: AL_669
Ransomware Attack

Detected
12 hours ago
Feb 3, 2022 3:10 AM

Action Taken
Snapshots Taken
IPs Blocked

Status
New

Last snapshots taken by auto response policy
Feb 3, 2022 3:10 AM

Total Attack Results

1 Affected Volumes | 0 Deleted Files | 215 Encrypted Files

215 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of Ransomware Attack.

The extension "r16m01d05" was added to each file.

Encrypted Files
Activity per minute

Figure 2: Storage Workload Security ransomware incident.

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

Director of IT, Transportation Company

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. www.netapp.com

[1] CyberSecurity Ventures

[2] Splunk, State of Security 2022

+1 877 263 8277