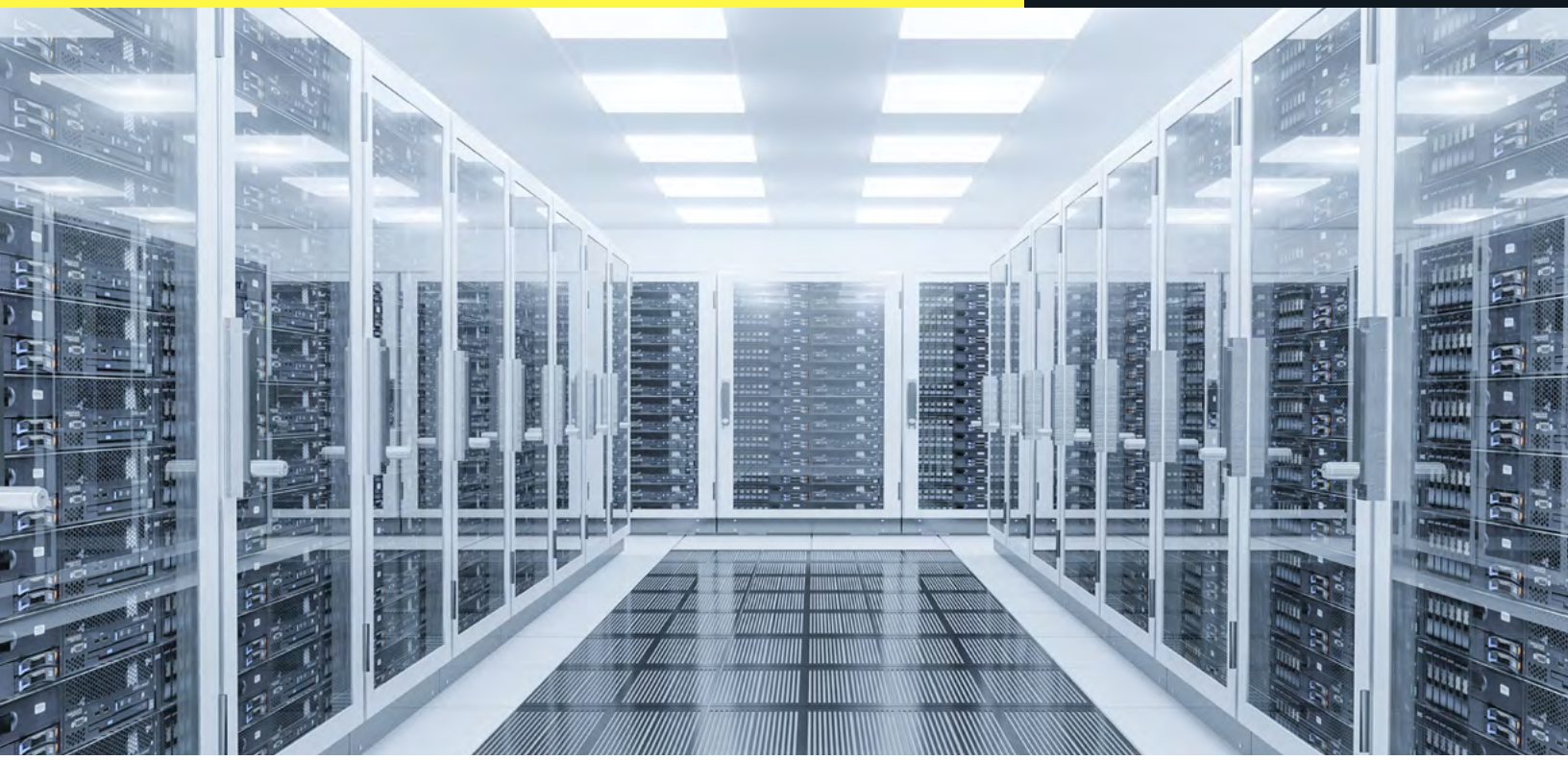
DATASHEET

NetApp Cloud Insights—Cloud Secure

Providing ransomware detection and recovery to NetApp BlueXP



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

Why you should care

The threat from a ransomware attack is very real. Currently, an attack occurs every 11 seconds[1] and is forecast to increase to every 2 seconds by 2031. Every attack has the potential to negatively impact your business and your brand. A cyber-attack study shows the average unplanned downtime is 14 hours[2] at a cost of $200K per hour. Furthermore, 80% of affected businesses suffered a loss of business/revenue. Data security is necessary since attacks on the cloud have been increasing as organizations migrate more business applications.

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 Insights is the ideal reporting tool.

NetApp Cloud Secure - Ransomware protection on BlueXP

The Cloud Secure ransomware feature is available as a standalone part of Cloud Insights. It's also integrated into the NetApp BlueXP™ control plane protection service, along with other integrated NetApp capabilities. Cloud Secure analyzes data access patterns to identify risks from ransomware attacks and 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, and the data is used to automatically identify the working communities of all users. The ability to audit all documents helps 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's activity across on-premises and AWS 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 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. In addition, Cloud Insights integrates ransomware alerts generated by ONTAP storage software to enrich the behavior analytics to further reduce this noise.

Key benefits

- Detect ransomware attacks 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

- **Detect anomalies and identify potential attacks**

Today's ransomware and malware are sophisticated, using random extensions and file names that make 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**

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

- **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.

Summary

Cloud secure provides a simple turnkey solution to ransomware detection on AWS 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.

Figure 1: Cloud Secure dashboard showing user activity.

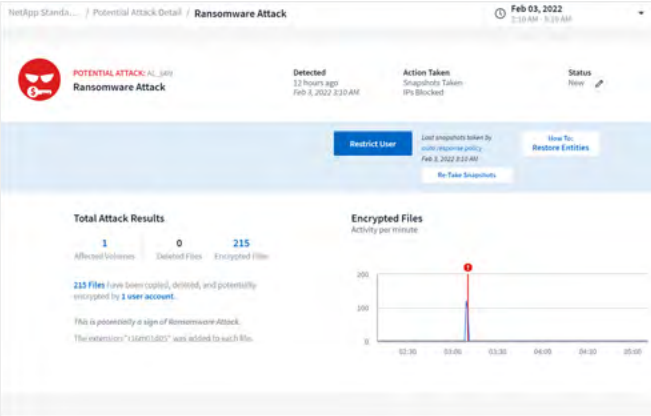


Figure 2: Cloud Secure ransomware incident.

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

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

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

AWS Marketplace simplifies software provisioning by combining elastic consumption and contract models with flexible software build and delivery models. Visit NetApp in AWS Marketplace.

To learn more, visit: www.netapp.com/aws

1 CyberSecurity Ventures, "2022 Cybersecurity Almanac," June 2, 2022
2 Splunk, "The State of Security 2022," April 4, 2022

NetApp

+1 877 263 8277

© 2022 NetApp, Inc. All Rights Reserved. NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners. DS-4223-1122

aws marketplace