

It’s closing time for ransomware

Ransomware is costly. It’s dangerous. It’s like that unruly customer at last call.

The aftermath isn’t cheap either.

- \$1.8–5 million:**
The average cost to remediate an attack in 2021 (up from \$768,106 in 2020)
- 10X the average ransomware payment:**
The cost of downtime and recovery time after an attack

Don’t let uninvited guests stay long enough to wreck the place.



40%

of all enterprises by 2025 will require storage products to have integrated ransomware defense mechanisms*

If it looks suspicious, we show it the door.

When it comes to ransomware protection, being proactive is the most effective way to detect and stop attacks before it’s too late. And it all starts with NetApp Cloud Insights featuring Cloud Secure and its AI-driven anomalous behavior detection.



“Is everything alright over here?”

To accurately identify a possible breach, all user activity is monitored, captured, and analyzed.

“Can I help you with something?”

The moment strange behavior is noticed, Cloud Secure steps into action.

“Please come with me.”

Cloud Secure can detect anomalies in user behavior thanks to its behavioral models built for each user.

“It’s time for you to go.”

Cloud Secure’s advanced machine learning algorithms uncover unusual data activity, detect potential attacks, and put a stop to it.

Take it back

Once risky behavior is detected, Cloud Secure takes control of the situation:

- An alert is sent, and a data snapshot is automatically taken for faster recovery
- Users are automatically blocked

Protect your enterprise now with 24-hour surveillance. And it all starts with a 30-day free trial of Cloud Insights. Plus, you’ll receive \$500 in AWS credits with trial. Sign-up through December 2022.

Start your free trial today

