E-BOOK

5 reasons you can’t prevent ransomware

NetApp

Contents

Given the number of high-profile ransomware attacks over the years, and the grave consequences of an infection, you might think that prevention methods should be maturing to the point that ransomware will soon be stamped out entirely.

Consider the once ubiquitous threat of exploit kits, such as the infamous Angler, a massive headache for any security team at the time. These exploit kits have all but faded from memory, thanks to the relentless effort by researchers to clamp down on them.

But ransomware is still everywhere, and total prevention of ransom-ware is effectively impossible. Let’s count down the reasons why that’s so.

5

It pays

Attackers are more motivated than ever, because successful attacks offer huge payoffs. The average ransom paid by organizations in the United States, Canada, and Europe increased from US$115,123 in 2019 to $312,493 in 2020—a 171% year-over-year increase. The average for the first fiscal quarter of 2021 came in at $850,000. Since 2019, ransomware-related incidents have increased by 65%. The attack frequency will continue to grow; instead of an attack every 11 seconds, it's estimated that an attack will occur every 2 seconds by 2031. These attacks will become increasingly commonplace. With numbers like these, it's easy to see why ransomware continues to be a favorite criminal endeavor.

And even though law enforcement agencies advise against it, organizations keep paying the ransom. It's natural for companies to want to protect their data, but the cost of the disruption to the business often eclipses the ransom itself, which means that paying up is often the most cost-effective option.

4

It’s cheap

On the flip side, the out-of-pocket costs to run a ransomware campaign are low. Today, an attacker can buy a prefab ransomware kit for a relatively paltry sum. The kit contains everything needed to deploy and monetize an attack, including encryption services, the payload dropper, and obfuscation tools. A typical ransomware-as-a-service (RaaS) subscription starts from a little over $100 per month. More complex and powerful variants can cost thousands, but the payoff potential increases as well. Support plans are also included to ensure that attackers can extract the maximum value from the service.

3

It’s proven effective

Ransomware is a profitable business. Forget the stereotype of hoodie-wearing malefactors in dark rooms; this is a sophisticated network comparable to any corporate partner program. One of the latest examples of RaaS is DarkSide, which was first found at the beginning of August 2020 and moved to a RaaS distribution model by November. Based on incidents reported, the typical demand is between $200,000 and $2 million for keys to unlock your data. Not only are DarkSide ransomware operators getting large paydays, but they’re also positioning themselves as “Robin Hoods”: taking money from large, profitable corporations and even making charitable donations from the proceeds. Reports based on the leak sites indicate that at least 90 victims have been affected by DarkSide to date. In total, more than 2TB of stolen data is currently being hosted on DarkSide sites, further demonstrating another incentive to pay up.

2

It has a rapid ROI

Another reason that ransomware is so attractive is that after it makes its way inside an organization, typically through email attachments, malicious URLs, insecure Remote Desktop Protocols, or malicious advertising (“malvertising”), it moves fast. It scans the network to locate files, and then encrypts the content and demands a ransom. Unfortunately, after the encryption process gets going, there’s little that can undo it. And in an alarming trend, a new methodology has arisen by which attackers steal data before encrypting it. In May 2021, Colonial Pipeline, supplier of 45% of the fuel for the U.S. East Coast, was hit with a ransomware attack. The attack was carried out by DarkSide or an affiliate. Besides locking Colonial Pipeline’s computer systems, DarkSide stole over 100GB of corporate data. This data theft shows that the group doubly extorts its victims. They not only ask for money to unlock the affected computers but also demand payment for the captured data, while threatening to publicly leak the stolen data if the victims don’t pay.

1

People are unreliable

So far we've covered why ransomware is so ubiquitous, but nothing about how to stop it. Although it's true that a great number of attacks could be prevented by better patching hygiene, there's one reason above all others that total prevention is impossible, and that's people.

You trust that your employees would never intentionally harm your organization. But ransomware infections still happen because employees are not hyperalert at all times to the dangers of malicious links and emails or phishing attempts.

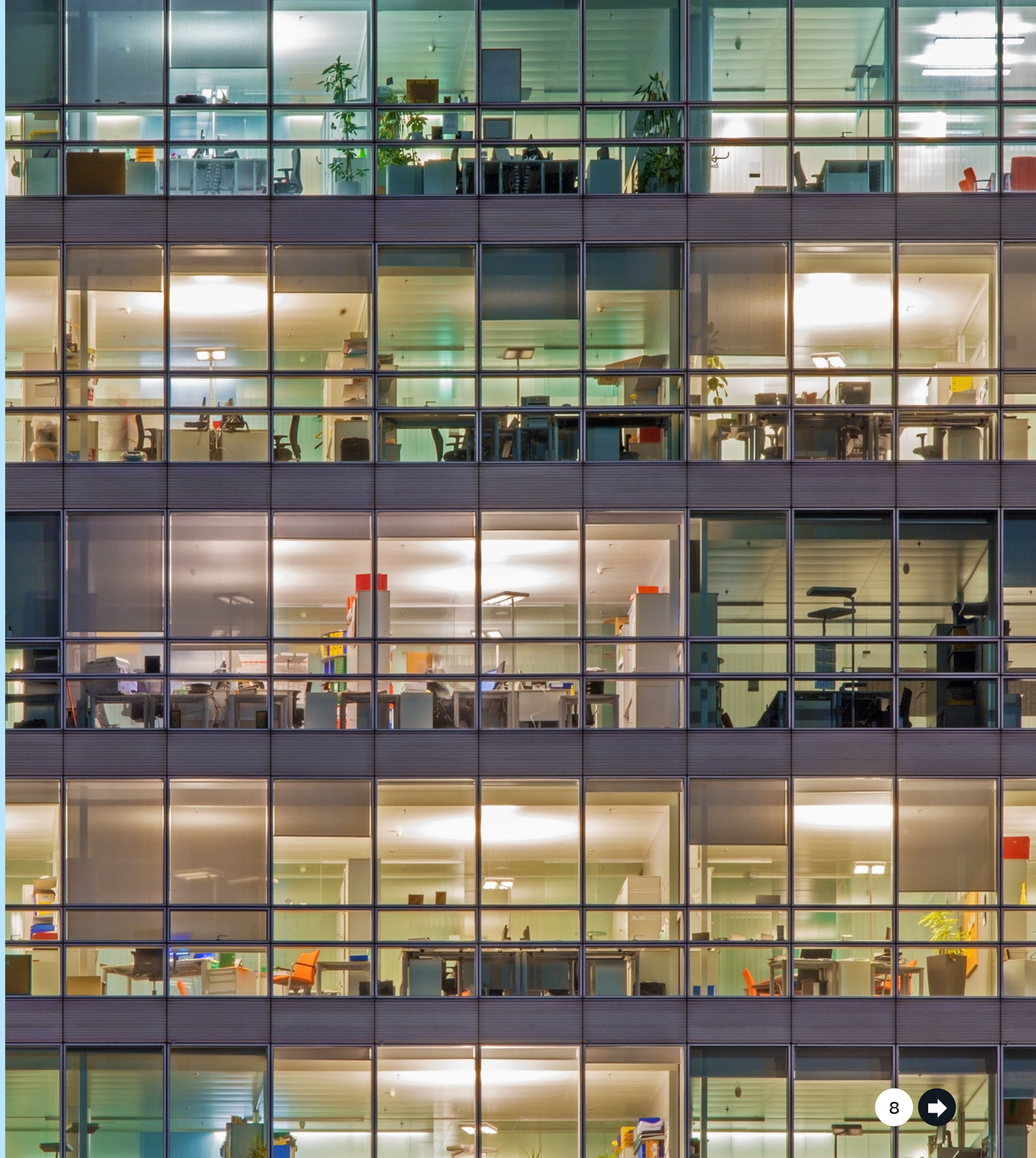
Many readers are probably familiar with regular mandatory security-awareness computer-based training. Training certainly doesn't hurt, but even your most security-aware employees can have a momentary lapse in judgment when clicking a link or opening an email. And without hyper-restrictive security policies that get in the way of people actually doing their jobs, that lapse in judgment is all it takes. Detection is needed within seconds, not minutes, hours, or longer.

Zero trust ransomware protection

If you can’t prevent ransomware, what can do to protect against it?

Your employees need access to data to do their jobs just like ransomware does, so your employees become the attack vector. Policies and roles that restrict access to data can help, but too many of them can get in the way of productivity.

The answer is early detection, user behavior analysis, and automated action when suspicious patterns occur. Within seconds.



NetApp® Cloud Insights offers just this type of detection with a feature called Cloud Secure. With Cloud Secure you can monitor activity, detect anomalies, and automate responses.

- **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® storage, either in your own data centers or in the cloud.

  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. 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.

- **Automate response policies**
  Cloud Secure alerts you to a potential ransomware attack and provides multiple automatic response policies to protect your data from the attack.

  Create a NetApp Snapshot™ copy when it detects unusual behavior. Your data is protected so that you can recover quickly, while limiting any potential for disruption from a false positive.

Block a user's ability to access data:
- When abnormal (read/write) user behavior is detected.
- When unusual file deletion behavior is detected.

Cloud Secure provides detailed access auditing, so administrators can quickly identify compromised data along with the source of the attack for quick remediation and recovery.

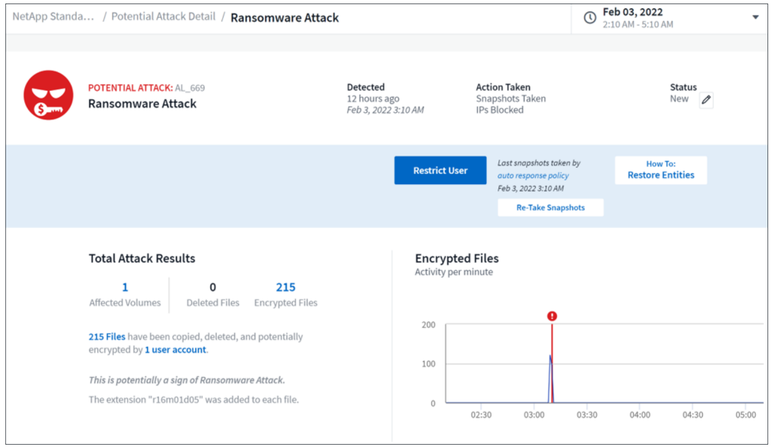


Figure 1) Cloud Secure dashboard showing ransomware attack.

If you’re interested in learning more about Cloud Secure, sign up for our 30-day free trial. **Learn more and start your 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.

NetApp