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. In 2019, ransom demands grew by 184% from Q1 to Q2, and experts estimate that the average cost per incident in 2020 was $283,800. Since 2018, ransomware-related incidents have increased by 41%, with the total cost to businesses in 2019 hitting $170 billion, according to some estimates. If these trends continue, the March 2019 attack on Norsk Hydro, which cost the company at least $40 million, might become 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 easy

One of the first examples of RaaS was GandCrab, which in its heyday in 2018 was responsible for more than half of all ransomware infections around the world. Over the course of its illustrious run, GandCrab generated more than $2 billion in profit, with $150 million going right to the creators and the rest spread out among its many affiliates.

Some go even further and have highly developed affiliate programs that vet applicants for compatibility. The currently spreading REvil/Sodinokibi ransomware was first spotted in mid-2019 and quickly rose to prominence thanks to its affiliate program, whereby creators allow only certain high-yield groups to use their RaaS program. Forget the stereotype of hoodie-wearing malefactors in dark rooms; this is a sophisticated network comparable to any corporate partner program.

2

It has a rapid ROI

Another reason that ransomware is so attractive is that once it makes its way inside a system, typically via email attachments, malicious URLs, insecure Remote Desktop Protocols, or malvertising, it moves fast. It scans the network to locate files, then encrypts the content and demands a ransom. Unfortunately, once the encryption process starts, there's not much you can do to undo it.

And in an alarming trend, a new methodology has arisen by which attackers steal data before encrypting it. In April, Fortune 500 computer giant Cognizant was hit by a Maze ransomware attack. Maze, which has been making the rounds since mid-2019, first steals data and then threatens victims that if the ransom isn't paid, the creators will release the data publicly. This strategy eliminates any notion of avoiding payment by way of a strong disaster recovery plan.

So it's hardly a shock that attackers continue to pursue this vector. It's lucrative and easy to pull off, and people keep on paying.

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.

I'm sure that many readers are 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 hyperrestrictive security policies that get in the way of people actually doing their jobs, that lapse in judgement is all it takes.

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® 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. 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 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.

Figure 1) Cloud secure dashboard showing user activity.

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.