Three Secrets to Stopping Ransomware Cold

For over thirty years,[1] cybercriminals have been leveraging ransomware to threaten and extort businesses for potentially massive profits. Ransomware continues to dominate headlines around the world, as legacy approaches to protecting the enterprise haven't kept pace with adversaries' constantly evolving tactics.

In order to bypass security controls, cybercriminals are now crafting attacks uniquely designed for each target—essentially making each organization a new patient-zero. In light of these recent, more targeted attacks, it has become increasingly apparent that legacy solutions are inadequate to prevent them. In fact, in 2020 alone, it is estimated that ransomware inflicted damages of over $20 billion worldwide, translating to roughly $8,500 per hour of downtime. [2]

So, is there a secret to stopping ransomware? Actually, there are three, and they start with taking a fundamentally new approach to your overall cybersecurity posture that is built in the cloud from the ground-up to protect users, applications, and sensitive data from potentially devastating ransomware attacks.

SECRET #1

AI-DRIVEN SANDBOX QUARANTINE

The rise of custom crafted ransomware attacks requires the ability to constantly detect and prevent never-before-seen threats before they can cause harm. Traditional approaches rely on out-of-band malware analysis that pass never-before-seen files on to the user while they are being analyzed, resulting in potential infections that will encrypt systems and bring the business to a halt. Receiving an alert after the fact is too little, too late, especially with ransomware.To stop these critical attacks, a better sandboxing approach is needed.

What does Zscaler™ recommend?

The key to successfully stopping ransomware is built on a cloud-native approach to malware analysis that unifies best-of-breed threat detection and AI-driven quarantine to hold suspicious content, maximizing protection while minimizing user impact.

As the industry's leading sandbox built on a cloud native proxy architecture, files can be quarantined and fully analyzed before delivery, which prevents the risk of patient-zero infections. Unlike passthrough approaches, suspicious files or those never seen before are guaranteed to be held for analysis and will not reach your environment.

Moreover, with a solution like Zscaler Cloud Sandbox, you have complete control over quarantine actions with a granular policy defined by groups, users, and content type. Additionally, because Zscaler Cloud Sandbox leverages machine learning and is part of the Zero Trust Exchange™—the world's largest security platform built for the cloud—you get near-real-time verdicts of unknown files sourced from a global community, while users get faster file downloads as any dangerous files are marked for quarantine.

SECRET #2

INSPECT ALL SSL TRAFFIC

According to Google,[3] more than 90 percent of all traffic is now encrypted, and attackers often leverage encryption to hide their attacks, including ransomware. Therefore, inspecting all traffic is a must for drastically reducing risk when squaring up against ransomware. However, full SSL inspection can be a challenge. Decrypting, inspecting, and re-encrypting traffic is compute-intensive, and legacy security approaches, such as next-generation firewalls, have limited processing power. It doesn't matter if the legacy solution is an appliance or a VM in the cloud; both solutions take noticeable hits to performance when inspecting SSL traffic.

What does Zscaler recommend?

Unlike legacy approaches, a cloud-centric proxy architecture enables you to deliver top-to-bottom SSL inspection.

A cloud-native proxy allows organizations to successfully perform SSL inspection at scale, without dips in performance or the need to expand the processing capacity of costly appliances.

Because the massively scalable Zscaler cloud is globally distributed across more than 150 data centers, it can inspect all your SSL traffic with no hit to performance. This ease of scalability allows you to inspect as much traffic per user as needed, even if user bandwidth dramatically increases, without incurring any additional costs. All of this combines to eliminate any security gaps caused by the difficulty of analyzing ransomware hidden in encrypted traffic.

SECRET #3

FOLLOW OFF-NETWORK CONNECTIONS

Always-on security is another challenge organizations struggle with when it comes to ransomware. With legacy approaches anchored in the data center, what happens as users drop off the VPN and your network? Unfortunately, with the rise in remote work, adversaries have upped their game and are delivering ransomware knowing that many users are operating outside of your security controls and protections, connecting over their home networks and public Wi-Fi and often using unmanaged devices.

What does Zscaler recommend?

Achieving always-on protection starts with a ubiquitous cloud-delivered platform.

With Zscaler, the first two secrets—AI-driven sandbox quarantine and unlimited SSL inspection—can be delivered to your users no matter where they are. Every connection over any network gets identical protection, including full inspection to uncover new and unknown threats. This always-on protection ensures that your organization remains safe from ransomware threats and patient-zero infections.

This comprehensive approach to tackling ransomware begins with every user connection being secured through the Zscaler Zero Trust Exchange. Off-net users simply add Zscaler Client Connector, our lightweight endpoint agent, to their laptops or mobile devices to get the same security, policy enforcement, and access controls as if they were in your headquarters. Moreover, because Zscaler is distributed across 150 data centers globally, users always get a fast connection through the nearest data center without the inconvenience of repeated VPN logins—or VPN latency.

Say goodbye to ransomware

As research and headlines show, ransomware isn't going anywhere. Legacy tools cannot keep up with the demands of inspecting all traffic, quarantining threats at scale without decimating performance, and delivering the always-on protection needed to stave off patient-zero attacks. Zscaler, however, has already helped thousands of customers prevent ransomware and countless other security attacks from reaching their networks with unparalleled scalability and superb user experiences.

If you'd like to know how your defenses stack up against ransomware and other advanced threats, try analyzing your security with our Internet Threat Exposure Analysis tool. It's free, safe, and it quickly identifies the common gaps in your security posture that advanced threats exploit.

Test your Security

[1] https://www.zdnet.com/article/30-years-of-ransomware-how-one-bizarre-attack-laid-the-foundations-for-the-malware-taking-over-the-world/

[2] https://purplesec.us/resources/cyber-security-statistics/ransomware/

[3] https://transparencyreport.google.com/https/overview?hl=en

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.

zscaler™