5 Steps to Ransomware Defense

How to strengthen your defenses beyond the perimeter

TABLE OF CONTENTS

The rise and spread of ransomware	03
The business of ransomware will cost you	04
Stop lateral movement. Stop ransomware spread.	05
Building an iron-clad defense strategy	06
What’s happening in your network?	07
Building a ransomware defense strategy	08
The bottom line	09

Introduction

The rise and spread of ransomware

Ransomware, once simply a nuisance strain of malware used by threat actors to restrict access to files and data through encryption, has morphed into an attack method of epic proportions. While the threat of permanent data loss alone is jarring, cybercriminals and nation-state hackers have become sophisticated enough to use ransomware to penetrate and cripple large enterprises, state and local governments, global infrastructure and healthcare organizations, and more. Many of these groups are even offering their services for hire as ransomware as a service (RaaS).

Ransomware attacks are predicted to occur every two seconds by 2031 and cost $265 billion annually.

Cybercrime magazine

The business of ransomware will cost you

In 2022, a ransomware attack forced 7-Eleven to close 175 stores as they were unable to use their cash registers or accept payment. Earlier that year, a BlackCat ransomware attack on a German oil company impacted 233 gas stations, with Royal Dutch Shell having to reroute their shipments to different supply depots because of the issue. The Colonial Pipeline attack occurred in May 2021, disrupting oil and gas deliveries all along the U.S. East Coast. And in 2020, the Snake ransomware attack brought Honda's global operations to a standstill.

Today, through a mix of outdated technology, "good enough" defense strategies focused solely on perimeters and endpoints, lack of training (and poor security etiquette), and no known "silver bullet" solution, organizations of all sizes are at risk. Cybercriminals are making it their business to encrypt as much of a corporate network as possible, to extort a ransom ranging from thousands to millions of dollars.

But there is more at stake than just your bottom line. The aftermath of a ransomware attack can be detrimental: Downtime can stop business operations, disrupt productivity, and compromise your data.

Once proprietary company data is leaked or compromised, you will likely suffer damage to your brand and loss of customer loyalty. According to a 2020 survey, 80% of data breaches included personally identifiable information (PII) of customers, intellectual property was compromised in 32% of breaches, and anonymized customer data was compromised in 24% of breaches. Not to mention, threat actors can use this sensitive data against your business or to carry out other insidious acts, including selling confidential data.

With the threat of ransomware propagating quickly across networks, protecting the perimeter alone simply isn't enough.

Stop lateral movement.
Stop ransomware spread.

A ransomware attack begins with an initial breach, often enabled by a phishing email, vulnerability in the network perimeter, or brute-force attacks that create openings while distracting defenses away from the attacker's actual intent.

Once the attack has landed in a device or application, it proceeds through lateral movement across the network and multiple endpoints to maximize the infection and encryption points. Attackers will typically seize control of a domain controller, compromise credentials, then find and encrypt the backup to prevent the operator from restoring the frozen services.

Lateral movement is critical to the success of an attack. If the malware can't spread beyond its landing point, it's useless. So prevention of lateral movement is essential.

How comprehensive is your ransomware threat mitigation strategy?

Risk mitigation

Building an iron-clad defense strategy

Detecting and preventing lateral movement inside your network boils down to two main focus areas: First, **reduce the initial attack vector**, and then **limit the propagation paths**.

You can do things like limit the amount of servers that are exposed to the internet, keep up with patch management to ensure a smaller attack surface, practice ringfencing to reduce the propagation paths between applications, and back up your data so you can get back online quickly and avoid widespread data loss if an attack occurs.

Four ways to make security planning a priority

Security should be part of your organization's broader preparedness strategy, planning, and budget. This means raising awareness with C-level executives and board members, and remaining vigilant about potential risks and what you need to mitigate them.

1. Make sure you include cybersecurity in the function that manages overall risk mitigation for your organization. And ensure there is security expertise on your leadership team.
2. Don't forget to dedicate budget and resources into backup generation and network segmentation.
3. Create response plans in advance of a disaster or adverse event (like a ransomware attack). Being organized and prepared means you can react more quickly and efficiently.
4. Analyze the security impact every time you integrate, design, or develop new products and services. Ask yourself: Am I opening a new door for attackers?

What’s happening in your network?

If your organization is like many others, detecting ransomware can be a challenge. Unfortunately, this means your network is vulnerable to attack. Without strong detection capabilities, by the time you receive a ransom note, it’s already too late: Most of your network will be encrypted at the same time.

When it comes to detection, you must catch ransomware while it’s spreading. Here’s what you’ll need:

Strong visibility

If you don’t know what’s happening in your network, you can’t detect ransomware or other unwelcome cyberthreats.

Segmentation policy

Once every communication is defined and accounted for, anything outside the norm will rise to the surface, and you will be alerted.

IDS system and malware detection tools

These will detect the propagation attempts of the ransomware operators, using predefined rules and signatures for known vulnerabilities or exploits or with more general or automated anomaly detection.

Deception tools

Setting up lures, honeypots, or a distributed deception platform that can identify unauthorized lateral movement can be an effective way to discover an active breach in progress with high-fidelity incidents.

Building a ransomware defense strategy

Despite the best perimeter defenses, breaches are inevitable. This is why you must have a defense strategy in place that minimizes the effectiveness of an attack and stops the spread within your network. Find a vendor that offers a comprehensive security solution that detects threats in east-west data center traffic and blocks lateral movement.

Prepare

Find a solution that allows you to identify every application and asset running in your IT environment. This level of granular visibility will allow you to quickly map critical assets, data, and backups, and to identify vulnerabilities and risks. By having a complete picture of your network environment, you'll be able to respond and quickly activate rules during a breach.

Prevent

Your solution should enable you to create rules to block common ransomware propagation techniques. By using software-defined segmentation, you can create Zero Trust microperimeters around critical applications, backups, file servers, and databases. You can also create segmentation policies that restrict traffic between users, applications, and devices, ultimately blocking lateral movement attempts.

Detect

Implement a solution that alerts you to any attempts to gain access to segmented applications and backups. These blocked access attempts are indicators of lateral movement. Also, you should incorporate reputation-based detection that alerts to the presence of known malicious domains and processes. By enabling fast discovery of attacks that have successfully breached the perimeter, you can minimize dwell time and catch attackers before they can move past the landing point.

Remediate

Automatic initiation of threat containment and quarantine measures when an attack is detected is critical. Apply isolation rules that allow the rapid disconnection of affected areas of the network, while segmentation policies block access to critical applications and system backups.

Recover

Finally, you need visualization capabilities that support phased recovery strategies in which connectivity is gradually restored as different areas of the network are validated as "all clear."

Conclusion

The bottom line

Are you confident in your existing defense strategy?

Ransomware isn't going away. In fact, ransomware affected 66% of organizations in 2021, an increase of 78% over 2020, and that number does not seem to be dropping. This means the world will continue to experience a higher frequency of attacks, larger and higher-value targets, and more costly ransom demands — all with dire consequences for your business. Now more than ever, you need advance planning and risk mitigation strategies that go beyond a perimeter-only approach.

Stop the lateral movement of ransomware in your network. Let Akamai show you how.

Please visit akamai.com/guardicore for more information.