



Risk Mitigation, Prevention, and Cutting the Kill Chain

Minimize the impact of ransomware with
Akamai Guardicore Segmentation

Overview

Ransomware, once simply a nuisance strain of malware used by cybercriminals to restrict access to files and data through encryption, has morphed into something far worse. 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, federal governments, global infrastructure, and healthcare organizations.

The 2017 WannaCry cryptoworm, which hit 230,000 computers globally by exploiting a vulnerability in Microsoft Windows, served as a high-profile marker of the threats ransomware presents. Since then, attackers have only become more sophisticated and attacks more pervasive. This includes the emergence of ransomware as a service (RaaS), in which hackers sell their service. [Akamai's Ransomware Threat Report, H1 2022](#), evaluated the attack patterns of Conti, a notorious RaaS group that was first detected in 2020 and appears to be based in Russia. The analysis hints at the need for strong protections against lateral movement and the critical role those protections can play in defending against ransomware. What's more, it found that the overwhelming majority of Conti victims are businesses with US\$10 million to US\$250 million in revenue.

Microsegmentation reduces the implicit trust in the network by allowing only connectivity explicitly defined by policy, thereby enforcing least-privilege access across applications for machine-to-machine traffic.

– Forrester, [Best Practices For Zero Trust Microsegmentation, June 27, 2022](#)

It's a clear sign that organizations of all sizes are at risk due to a mix of outdated technology, "good enough" defense strategies focused solely on perimeters and endpoints, a lack of training (and poor security etiquette), and no known "silver bullet" solution. In fact, the [Cybersecurity Ventures Who's Who In Ransomware: 2023 Report](#) predicts that by 2031, ransomware is expected to attack a business, consumer, or device every two seconds.





It depends on lateral movement

A ransomware attack begins with an initial breach, often enabled by a phishing email, a vulnerability in the network perimeter, or a brute-force attack that creates openings while distracting defenses away from the attacker's actual intent. Once the malware has landed in a device or application, it proceeds through privilege escalation and 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; therefore, prevention of lateral movement is essential. The visibility and segmentation features in a solution like Akamai Guardicore Segmentation enable you to quickly set up policies that prevent and contain an initial breach. You'll also be alerted to lateral movement and other suspicious behaviors to help detect malware early, so you can react right away.

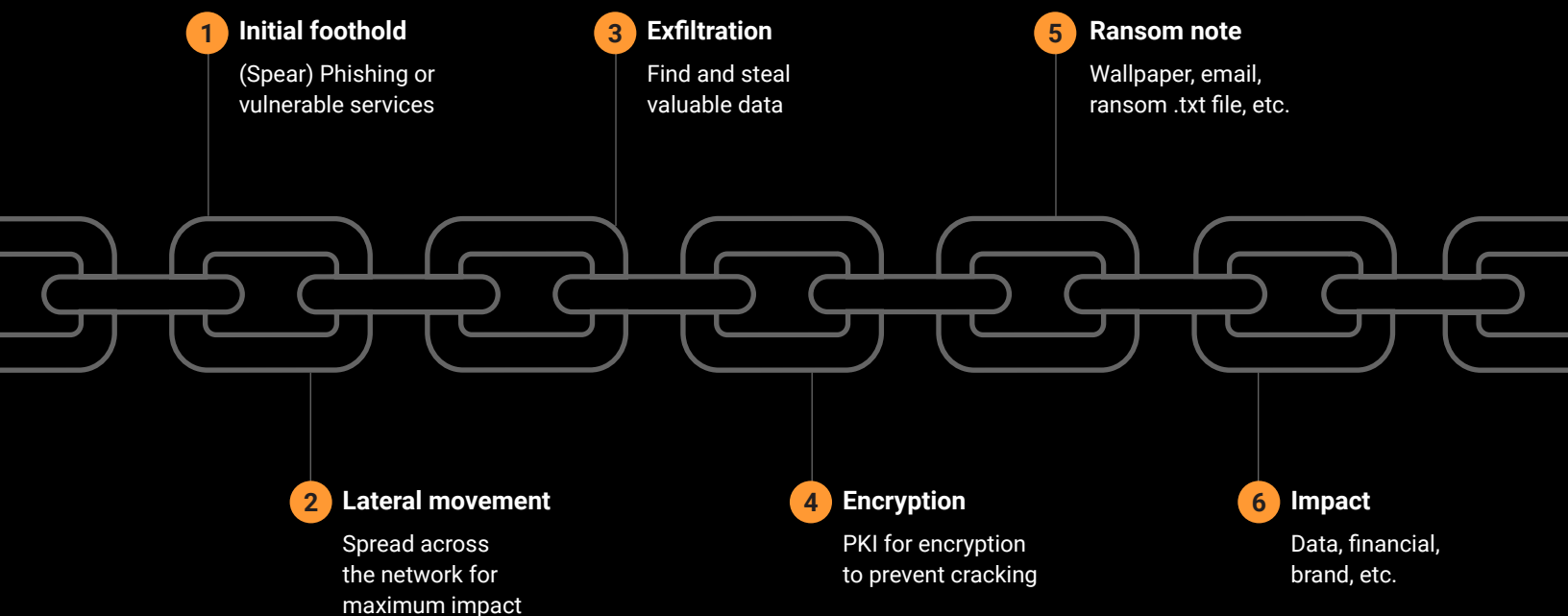


Part 1: Cutting the ransomware kill chain – risk mitigation and prevention

Ransomware doesn't spread by breaching a single machine or device. Cybercriminals use ransomware to encrypt as many systems on a network as possible to ensure a ransom gets paid.

Because ransomware is a multifaceted attack, implementing multiple layers of defense can help prevent widespread damage, data loss, and downtime. The first layer of defense is to attempt to prevent the initial ransomware infection.

The ransomware kill chain



Prevent initial infection

The first vulnerable spots for any network are its points of contact with the internet. While many ransomware attacks rely on spear phishing, nothing prevents them from breaching your internet-exposed services.

The visibility features in Akamai Guardicore Segmentation allow you to monitor services exposed to the internet and limit their exposure through policies for:

- Remote access services (RDP, SSH, TeamViewer, AnyDesk, VPNs)
- Potentially vulnerable services (Apache, IIS, Nginx)
- Potentially vulnerable machines (detect machines with an unpatched operating system using the additional Insight feature)
- Unwanted exposed services (databases, domain controllers, internal web or file servers)

Cutting the kill chain with segmentation

It's inevitable that a network will be breached at some point. This could be caused by things like spear phishing, human error, or a server running a vulnerable service that was not mitigated properly. This is why it's critical to have proper risk mitigation strategies in place.

Once a machine is breached, you want to limit the propagation inside your network. This can be done in three ways:

1. Segmentation by application ringfencing

You want to separate the network into operational segments — by application, usage, or environment — and not allow unnecessary connections between and within those segments.






Here are four segmentation guidelines to consider:

- Block any communication between laptops/workstations.
- Block communication from processes running with “powerful” domain user privileges, like domain administrators.
- Limit users that can execute processes on your servers.
- Limit access from laptops/workstations to data center servers and cloud instances.



Akamai Guardicore Segmentation makes it easy to secure your network against ransomware. Using pre-built templates, you can mitigate attacks by setting policies in three simple steps:

1. **Select your goal**, like ringfencing a critical application, creating ransomware mitigation policies, or securing an active directory.
2. **Identify the relevant assets to protect**, like the ecommerce application assets you are seeking to ringfence, all active directory workloads in the data center, or the endpoints to protect against ransomware spread. This step, in many cases, is achieved automatically with Akamai's AI labeling.
3. **Protect assets by creating policies**. Akamai Guardicore Segmentation's AI automatically suggests and recommends policies based on real traffic in the environment, and learns the communication patterns of applications across hundreds of networks.

<p>Ra</p> <p>Create Ransomware Response - File Share Restrictions</p> <p>#ransomware #template</p>	<p>Ra</p> <p>Create Ransomware Recovery and Response Policies</p> <p>#ransomware #template</p>	<p>Ma</p> <p>Create Malware Response - Lateral Movement Mitigation Policies</p> <p>#malware #template</p>	 <p>Apply Zero Trust Application Security on application</p> <p>#diy #zero trust</p>
 <p>Application Tier-Segmentation by whitelisting flows bet...</p> <p>#diy</p>	 <p>Ringfence an Application by whitelisting inbound a...</p> <p>#diy</p>	 <p>Whitelist Outbound Flows for an application</p> <p>#diy</p>	 <p>Control Privileged Access to environment from jumpboxes</p> <p>#diy</p>

Example: Akamai Guardicore Segmentation Templates



2. Preventing lateral movement with protocol-restricting rules

There are general guidelines for specific protocols and behaviors. Due to some protocols' inherent usage in normal day-to-day operations, they should be restricted with care. Akamai Guardicore Segmentation creates a visualization of all traffic to create the most accurate rules for your environment around high-risk protocols such as WinRM, SMB, RPC, RDP, SSH, and others.

For example, while SSH is useful for remote administration, and also serves to make other protocols secure (like sFTP), it's also a tool used by attackers to breach machines and propagate the network. You'll want to restrict network-wide SSH as much as possible by creating jump boxes for authorized users.

Allow	Private	Jumpboxes	22 TCP	Allow
		Any		
Allow internal assets to access your jumpboxes over SSH				
Block	* Any	* Any	22 TCP	Block

Rules created in Akamai Guardicore Segmentation

3. Protecting backups and critical data services

To maximize damage, ransomware attacks usually target the organization's backup servers in order to encrypt the stored data. Similarly, data services and file servers are targets for ransomware.

Use Akamai Guardicore Segmentation to limit access to your backup servers, databases, and file servers, as well as to limit access from outside the network, and from regions in your network that don't need access. To minimize communication to and from the critical backup servers, you can use Akamai Guardicore Segmentation to ringfence applications, and lock down communication to and from an application down to process and user levels. Limiting your data services' exposure to only the operational minimum will reduce the risk factor to those services and mitigate ransomware exposure and propagation paths.

Part 2: Ransomware detection and response

When it comes to dealing with cyberthreats such as ransomware, advanced planning and vigilance are critical. By reacting quickly to a breach, you can minimize the damage to your network. Akamai Guardicore Segmentation has capabilities that can help you with both threat detection and response.

Threat detection with Akamai Guardicore Segmentation

Incidents can include:

- **Deception** – This detects and intercepts suspicious lateral movement attempts and redirects them to dynamic honeypots so their actions can be monitored and analyzed. Deception incidents are high fidelity, providing detailed data on malicious activity and the cybercriminal's next phase of attack.
- **Network scans** – Cybercriminals gather intelligence once they are inside a network. They use network scans as a reconnaissance method to detect open ports or services that other servers are listening for. Akamai Guardicore Segmentation automatically detects network scans and alerts users immediately.
- **Policy-based detection** – Security policies at the network and process levels enable instant recognition of unauthorized communications and noncompliant traffic.

Akamai Guardicore Segmentation presents Insight feature

Akamai Guardicore Segmentation can provide visibility into individual assets by leveraging an additional feature based on osquery. The querying framework that it provides can quickly detect anomalous activity, such as Volume Shadow Copy, ransomware's most common pre-encryption action. It can also detect Trojans used to deliver ransomware by searching for a common hollowing technique that hides malware under svchost.exe, a legitimate Windows process.

Managed threat hunting

The Akamai Hunt managed threat hunting service alerts users to any anomalous behavior inside their network. This is done through techniques like analyzing incoming and outgoing internet connections and their associated GeoIP, looking for new executables that have increasing network presence that can indicate propagation, and analyzing asset connections to find indications of lateral movement through neighbor-count anomalies.

Immediate response

Once you've detected a threat such as ransomware inside your network, you can quickly deploy mitigation measures by applying policies at the process and user levels to actively deny and isolate malicious activity from occurring.



Incremental infection visibility

With your initial lead or indicator of compromise (IOC), you can start looking for additional indicators, such as communication patterns, processes, ports used, infected assets, and more. Akamai Guardicore Segmentation can help find all assets with this indicator (all assets communicating to the C2, all assets communicating to a unique port, or all assets running a malicious process). And with a visual map of your environment, you can look for other similarities across infected machines or traces of propagation.

Part 3: Disinfection and recovery

Once you have a list of all infected machines and IOCs, you can start disinfecting. Divide your machines into three label groups: **Isolated**, **Monitored**, and **Clean**.

Isolated

- Assets that are **infected** by malware
- Keep those assets **quarantined** until malware has been removed

Monitored

- Assets that may or may not be **infected**
- **Monitor** until you are sure malware has been **removed**

Clean

- Assets verified as **not infected** and can **operate normally**

Segmentation guidelines for recovery

After setting the three label groups, you can begin adding policies to segment your network by creating four communication tiers:

- **Block** all incoming and outgoing communications from **Isolated** machines.
- **Block** remote management protocol communication to and from **Monitored** machines.
- **Alert** on any remote management protocol communication to **Clean** machines.
- **Block** all communications between the label groups.

Override Alert	* Any	<u>Clean</u>	5985, 5986 ... TCP UDP
Override Block	<u>Monitored</u>	<u>Clean</u>	Any TCP UDP
Override Block	<u>Clean</u>	<u>Monitored</u>	Any TCP UDP
Override Block	<u>Monitored</u>	* Any	5985, 5986 ... TCP UDP
Override Block	* Any	<u>Isolated</u>	Any TCP UDP Any ICMP
Override Block	<u>Isolated</u>	* Any	Any TCP UDP Any ICMP

Block and alert rules in Akamai Guardicore Segmentation

Ransomware recovery and response template

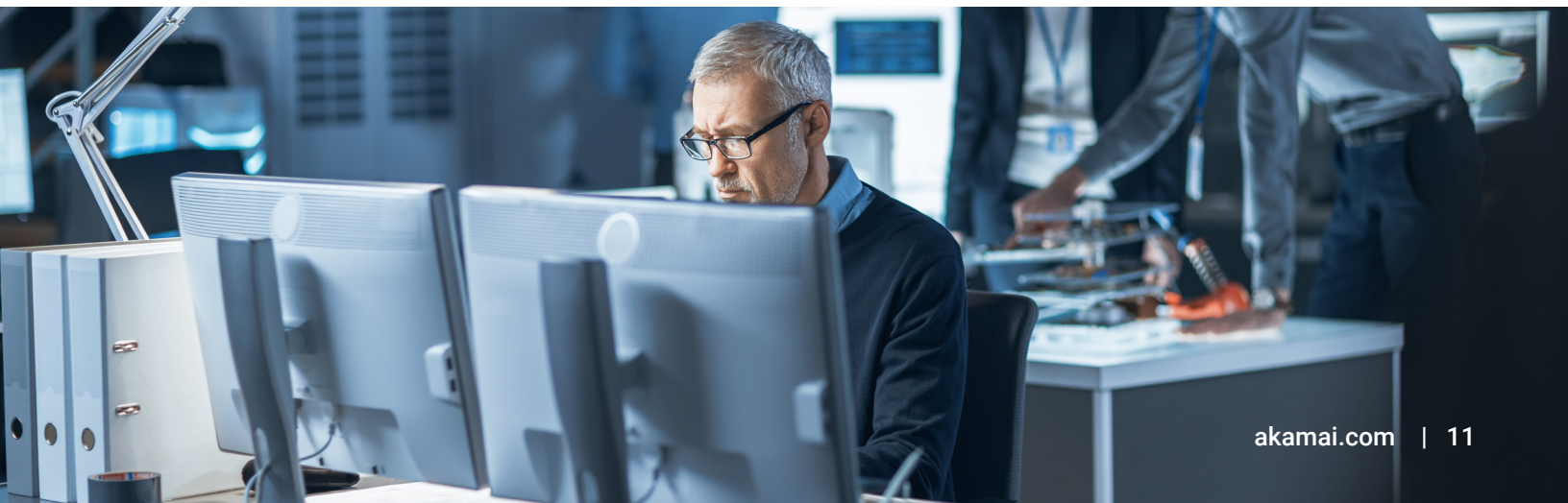
The Ransomware Recovery and Response Policies template included in Akamai Guardicore Segmentation provides you with an easy-to-use, pre-built policy to restrict access across the labels **Isolated**, **Monitored**, and **Clean**.

This template will allow you to easily maintain operational continuity of **Clean** machines without fearing (re)infection from **Isolated** machines.



Conclusion

If you still rely on legacy firewalls or perimeter-only defense, you can't stop ransomware from spreading across your network and locking down critical applications and infrastructure. The reality is, breaches are inevitable – and you need to be prepared. Akamai Guardicore Segmentation can help you detect the threats in east-west data center traffic, and block the lateral movement that ransomware depends on to encrypt and ransom your most critical assets.





Five steps to mitigate the impact of a ransomware attack with Akamai Guardicore Segmentation



Prepare by identifying every application and asset running in your IT environment.



Prevent by creating rules to block common ransomware propagation techniques.



Detect by receiving alerts to any attempts to gain access to segmented applications and backups.



Remediate by initiating threat containment and quarantine measures when an attack is detected.



Recover with visualization capabilities that support phased recovery strategies.

Stop the lateral movement of ransomware in your network.
Don't believe us? See it for yourself. akamai.com/guardicore



Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's security, compute, and delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on [Twitter](https://twitter.com/Akamai) and [LinkedIn](https://www.linkedin.com/company/akamai). Published 05/23.