Guardicore

RISK MITIGATION, PREVENTION AND CUTTING THE KILLCHAIN

STOP THE IMPACT OF RANSOMWARE WITH GUARDICORE CENTRA

WHITE PAPER

OVERVIEW

Ransomware, once simply a nuisance strain of malware used by cybercriminals 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, federal governments, global infrastructure and healthcare organizations.

In 2020, the Snake ransomware attack brought Honda global operations to a **standstill**. That same week, Snake, a form of file-encrypting malware, also hit South American energy-distribution company, Enel Argentina. In 2019, **hackers froze** the computer networks of Pemex, Mexico's state-owned gas and oil conglomerate, demanding $5 million to restore service. And in 2017, the WannaCry cryptoworm hit **230,000** computers globally by exploiting a vulnerability in Microsoft Windows.

Today, through a mix of outdated technology, "good enough" defense strategies focused solely on perimeters and endpoints, lack of training (and poor security etiquette), and no known "silver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. Especially as cybercriminals are making it their business to encrypt as many computer systems on the corporate network as possible in order to extort a ransom ranging from thousands to **millions** of dollars. In fact, ransomware attacks are **predicted** to occur every eleven seconds in 2021 at a global cost of $20 billion.

Close The Fire Doors On Lateral Movement

"Worms such as WannaCry and NotPetya rely on lateral movement to escalate a containable nuisance to a cataclysmic attack. Microsegmentation and focused granular internal controls mitigate this problem and must be deployed as part of a Zero Trust strategy."

-**Forrester,** Mitigating Ransomware With Zero Trust, June 8, 2020

IT STARTS WITH LATERAL MOVEMENT

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 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.

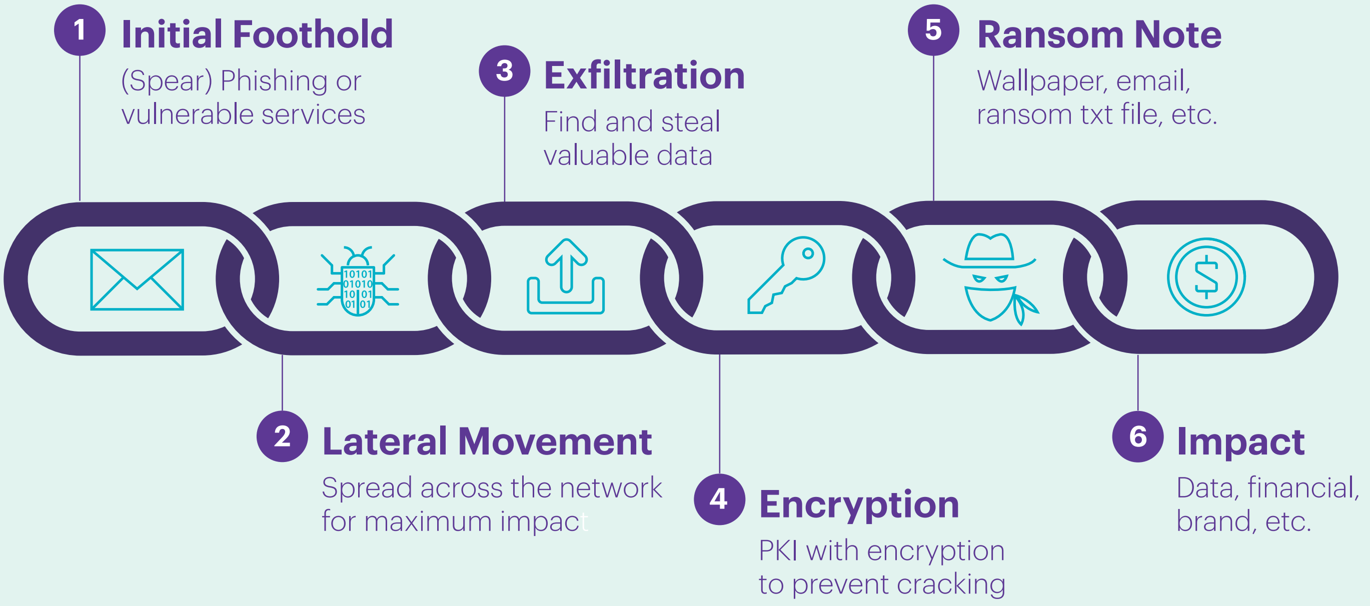
Lateral movement is critical to the success of an attack. If the malware can't spread beyond its landing point, it's useless. So, prevention of lateral movement is essential. The visibility and segmentation features in Guardicore Centra enable you to set up policies to prevent and contain an initial 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 KILLCHAIN: RISK MITIGATION AND PREVENTION

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

Because ransomware is a multi-faceted 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 Killchain



1 **Initial Foothold**
(Spear) Phishing or vulnerable services

2 **Lateral Movement**
Spread across the network for maximum impact

3 **Exfiltration**
Find and steal valuable data

4 **Encryption**
PKI with encryption to prevent cracking

5 **Ransom Note**
Wallpaper, email, ransom txt file, etc.

6 **Impact**
Data, financial, brand, etc.

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.

By using Guardicore Reveal, you can 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 Guardicore Insight).
- Unwanted Exposed Services (Databases, Domain Controllers, Internal web or file servers).

Cutting the Killchain 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 and 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:

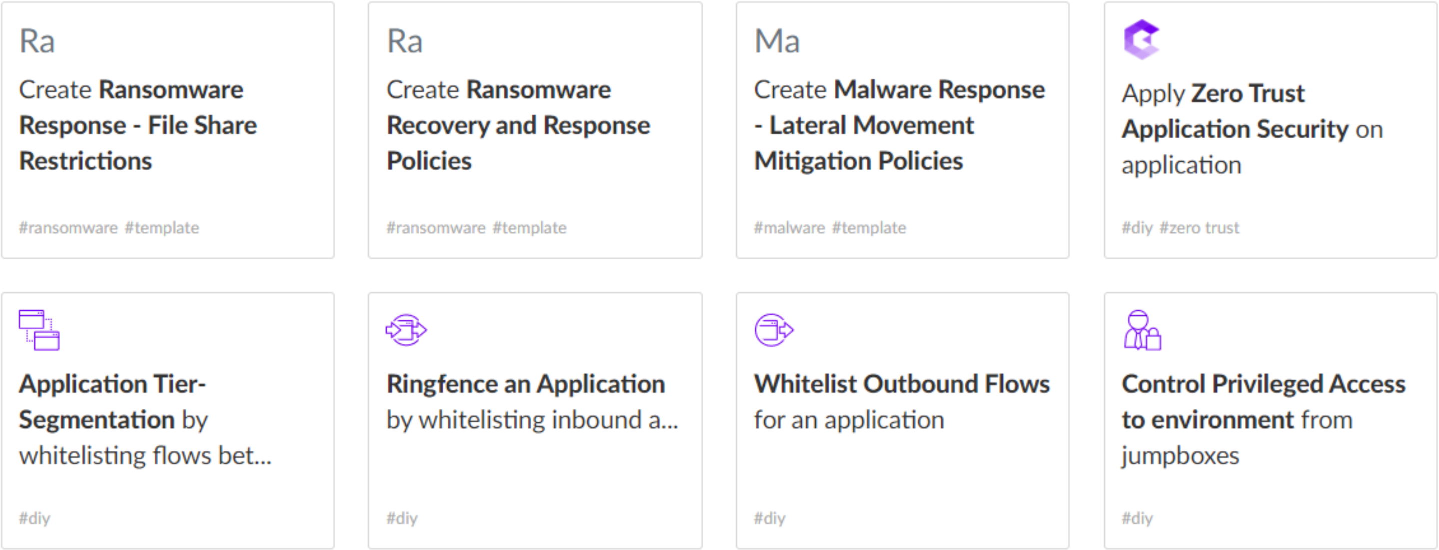
- Block any communication between laptops/workstations.
- Block communication from processes running with "powerful" domain user privileges, like Domain Administrators.
- Limit users that can execute processes on your servers.
- Limit access from laptops/workstations to datacenter servers and cloud instances.

Guardicore makes it easy to secure your network against ransomware. Using the templates available in Guardicore Centra, 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 e-commerce application assets you are seeking to ringfence, all active directory workloads in the datacenter, or the endpoints to protect against ransomware spread. This step, in many cases, is achieved automatically by Guardicore AI labeling.

3. **Protect assets by creating policies.** Guardicore'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.



Ra

Create **Ransomware Response - File Share Restrictions**

#ransomware #template

Ra

Create **Ransomware Recovery and Response Policies**

#ransomware #template

Ma

Create **Malware Response - Lateral Movement Mitigation Policies**

#malware #template

Apply **Zero Trust Application Security** on application

#diy #zero trust

Application Tier-Segmentation by whitelisting flows bet...

#diy

Ringfence an Application by whitelisting inbound a...

#diy

Whitelist Outbound Flows for an application

#diy

Control Privileged Access to environment from jumpboxes

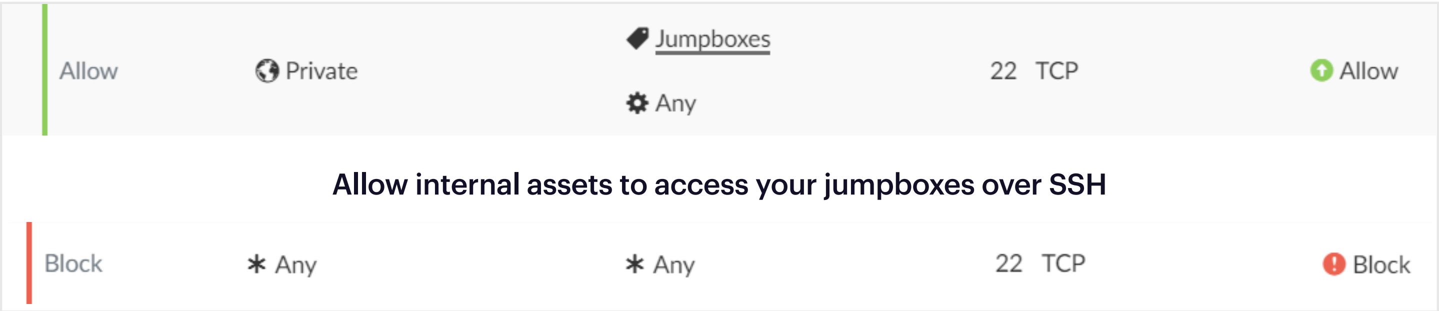
#diy

Example: Guardicore Centra 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, some of these protocols should be restricted with care. Guardicore Reveal enables 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 jumpboxes for authorized users.



Allow	Private	Jumpboxes Any	22 TCP	Allow

Allow internal assets to access your jumpboxes over SSH

Block	* Any	* Any	22 TCP	Block

Rules created in Guardicore Centra

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 Guardicore Centra to limit access to your backup servers, databases and file servers. And 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 Guardicore Centra 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. Guardicore Centra has capabilities that can help you with both threat detection and response.

Threat Detection with Guardicore Centra

Incidents

Guardicore Centra raises alerts in the form of incidents, which could indicate an attack is happening or that there is a threat to your network.

Incidents can include:

- **Deception** – 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 inside a network. They use network scans as a reconnaissance method to detect open ports or services that other servers are listening for. Guardicore Centra 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.

Guardicore Insight

Guardicore provides visibility into individual assets by leveraging osquery. Centra uses this querying framework to quickly detect anomalous activity, such as detecting Volume Shadow Copy, ransomware's most common pre-encryption action. Centra can also detect trojans used to deliver ransomware by searching for a common hollowing technique that hides malware under svchost.exe, which is a legitimate Windows process.

Threat Hunting

Guardicore's Threat Hunting service alerts users to any anomalous behaviour 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

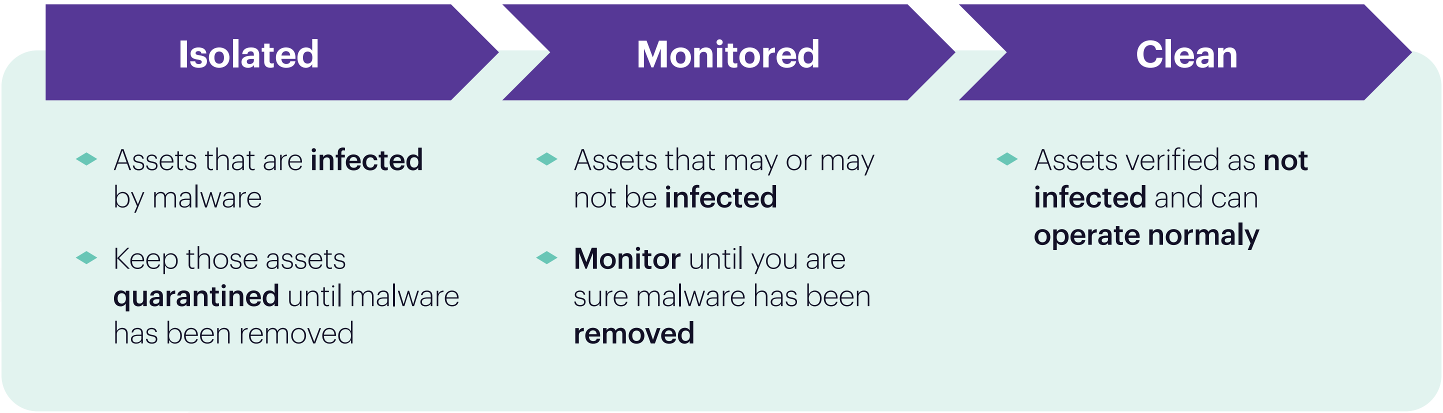
Once you've detected a threat, such as ransomware, inside your network, use Guardicore Centra to quickly deploy mitigation measures by applying policies at the process- and user-levels to actively deny and isolate malicious activity from occurring.

Incremental Infection Visibility

With your initial lead or indicator of compromise, you can start looking for additional indicators, such as communication patterns, processes, ports used, infected assets and more. Use Guardicore Reveal to 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 within the Guardicore Reveal 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**

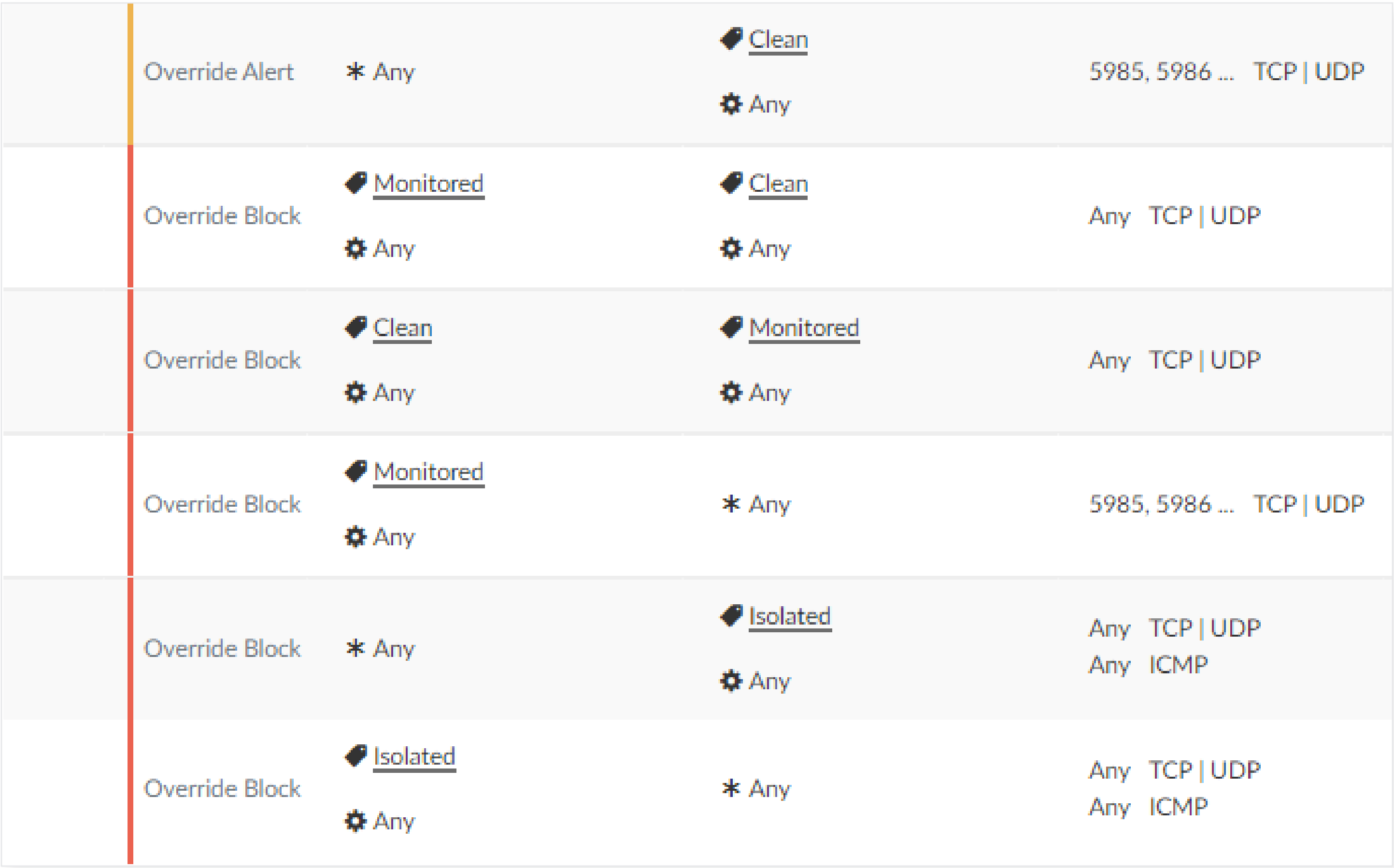
Clean

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

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.



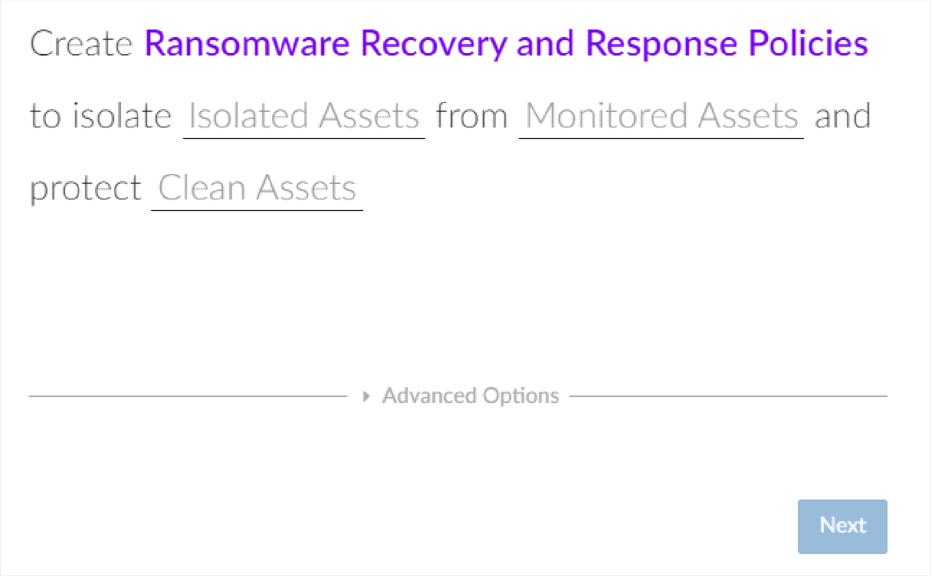
Override Alert	✱ Any	Clean ⚙ Any	5985, 5986 ...	TCP | UDP
Override Block	Monitored ⚙ Any	Clean ⚙ Any	Any	TCP | UDP
Override Block	Clean ⚙ Any	Monitored ⚙ Any	Any	TCP | UDP
Override Block	Monitored ⚙ Any	✱ Any	5985, 5986 ...	TCP | UDP
Override Block	✱ Any	Isolated ⚙ Any	Any Any	TCP | UDP ICMP
Override Block	Isolated ⚙ Any	✱ Any	Any Any	TCP | UDP ICMP

Block and alert rules in Guardicore Centra

Ransomware Recovery and Response Template

The Ransomware Recovery and Response Policies Template included in Guardicore Centra provides you with an easy-to-use, prebuilt 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 risk of (re)infection from **Isolated** machines.



Create Ransomware Recovery and Response Policies to isolate Isolated Assets from Monitored Assets and protect Clean Assets

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. Guardicore Centra can help you detect threats in east-west data center traffic and block lateral movement.

FIVE STEPS TO MITIGATE THE IMPACT OF A RANSOMWARE ATTACK WITH GUARDICORE CENTRA

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.

www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.