
Akamai

Ransomware Protection:

Reducing the Impact on Your Organization

Guardicore

Welcome from Akamai

Brian S. Dennis

Principal Technologist-Public Sector

Akamai Technologies

Working to make the Public Sector a Cyber-secure environment

Who are you listening to?

Michael Mikelas

Manager, Solutions Engineering
Akamai Guardicore Segmentation

- Have held various Admin, Engineer, Architect and Leadership roles across the Education, Manufacturing, Healthcare, and Chemical industries. Most recently consulted for a prominent Security Solutions Integrator before joining Guardicore.

Something Big and Different is Happening

Order of magnitude increase in the reach and impact of security incidents

By the end of 2021, Ransomware
attacked organizations every 11 seconds

Novel, large-scale attacks that are nearly impossible to anticipate

SolarWinds, Kaseya, Log4J and now PNWKIT reveal global vulnerability to sophisticated,

emerging attacks

An Effective Response to Ransomware Attacks Starts with the Fundamentals

June 2021 Open Letter to the Private Sector

1. Backup your data, system images, and configurations, regularly test them, and keep the backups offline
2. Update and patch systems promptly
3. Test your incident response plan
4. Check your security team's work
5. Segment your networks

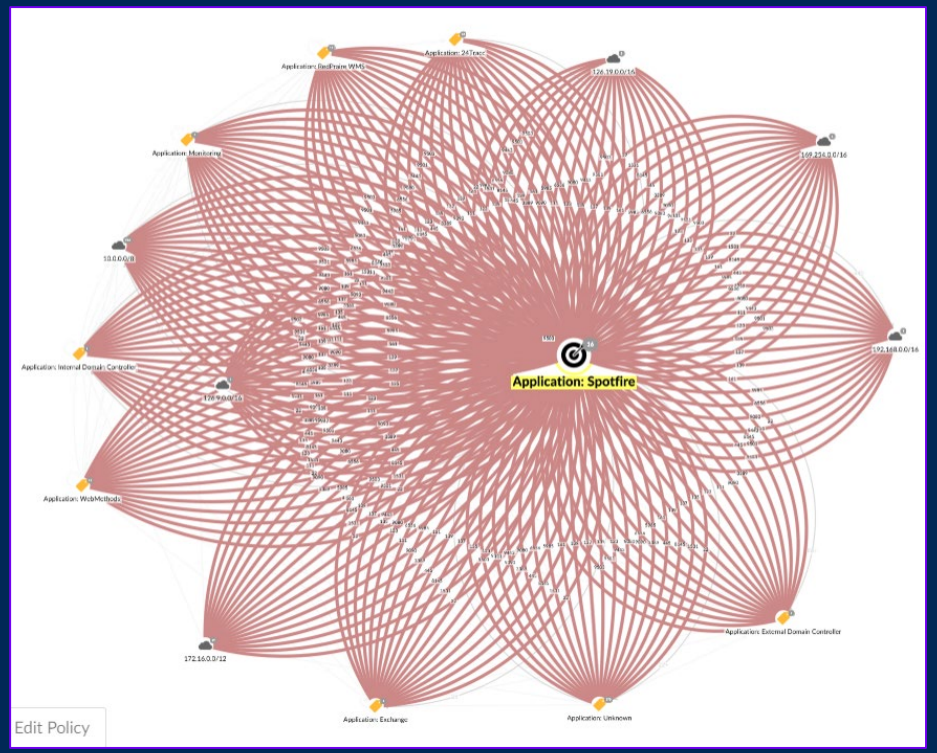
But which of these things is often considered the most daunting leap for organizations?

A Closer Look:

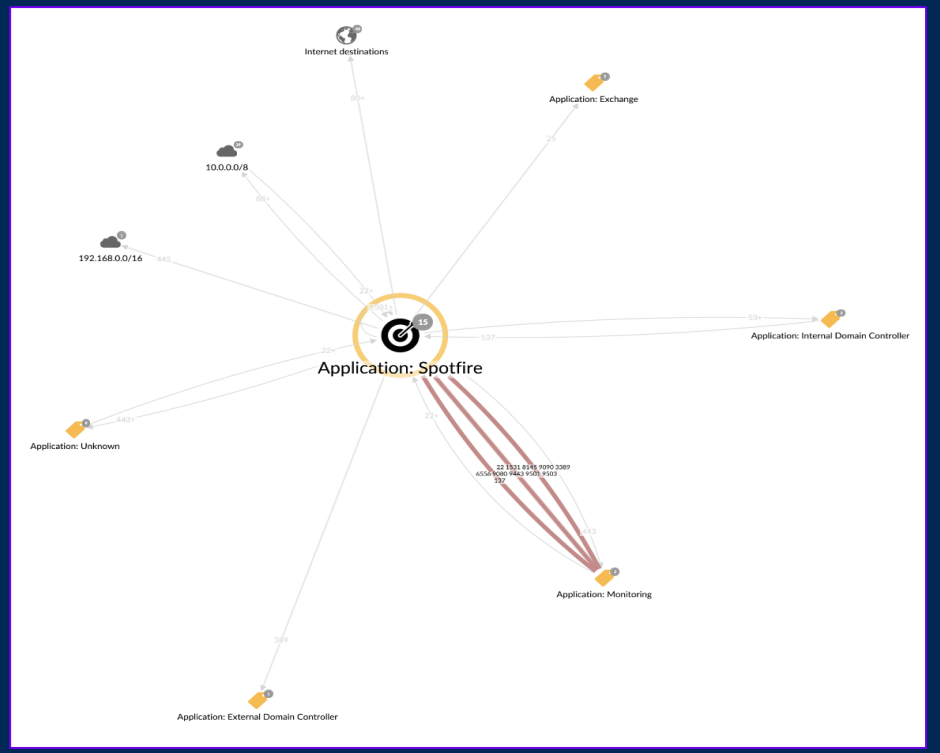
Ransomware Mitigation with Software-Based Segmentation

Segmentation - a critical control for Ransomware

Without segmentation



With segmentation



How a Typical Ransomware Attack Unfolds

- Spear-phishing emails
- Phishing attack
- Vulnerable service exploitation
- Unpatched server exploitation
- Brute-force attack

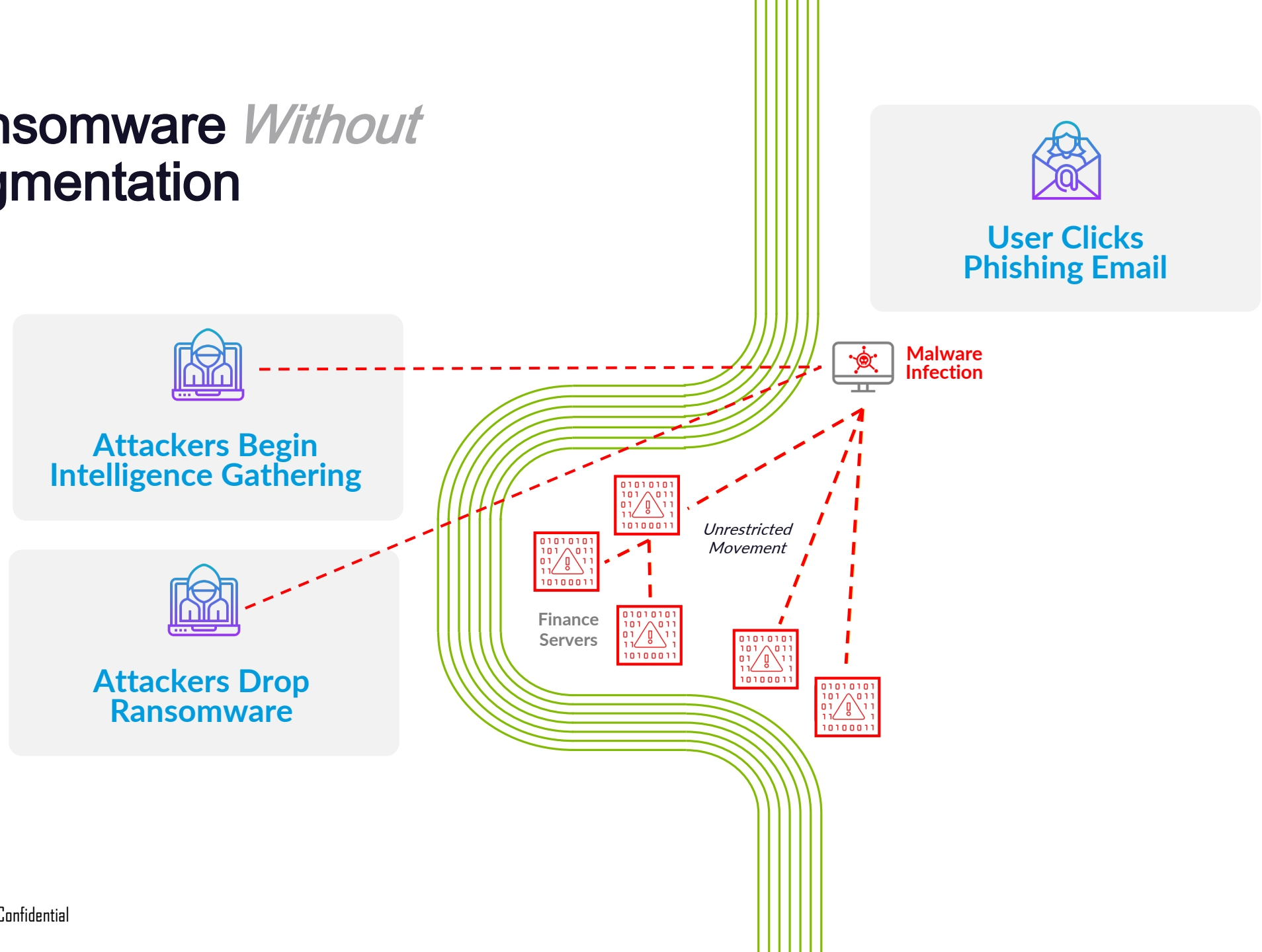
- Move laterally towards the system with privileged account
- Harvest credentials

- Encrypt the company's backup servers to rule out fast recovery

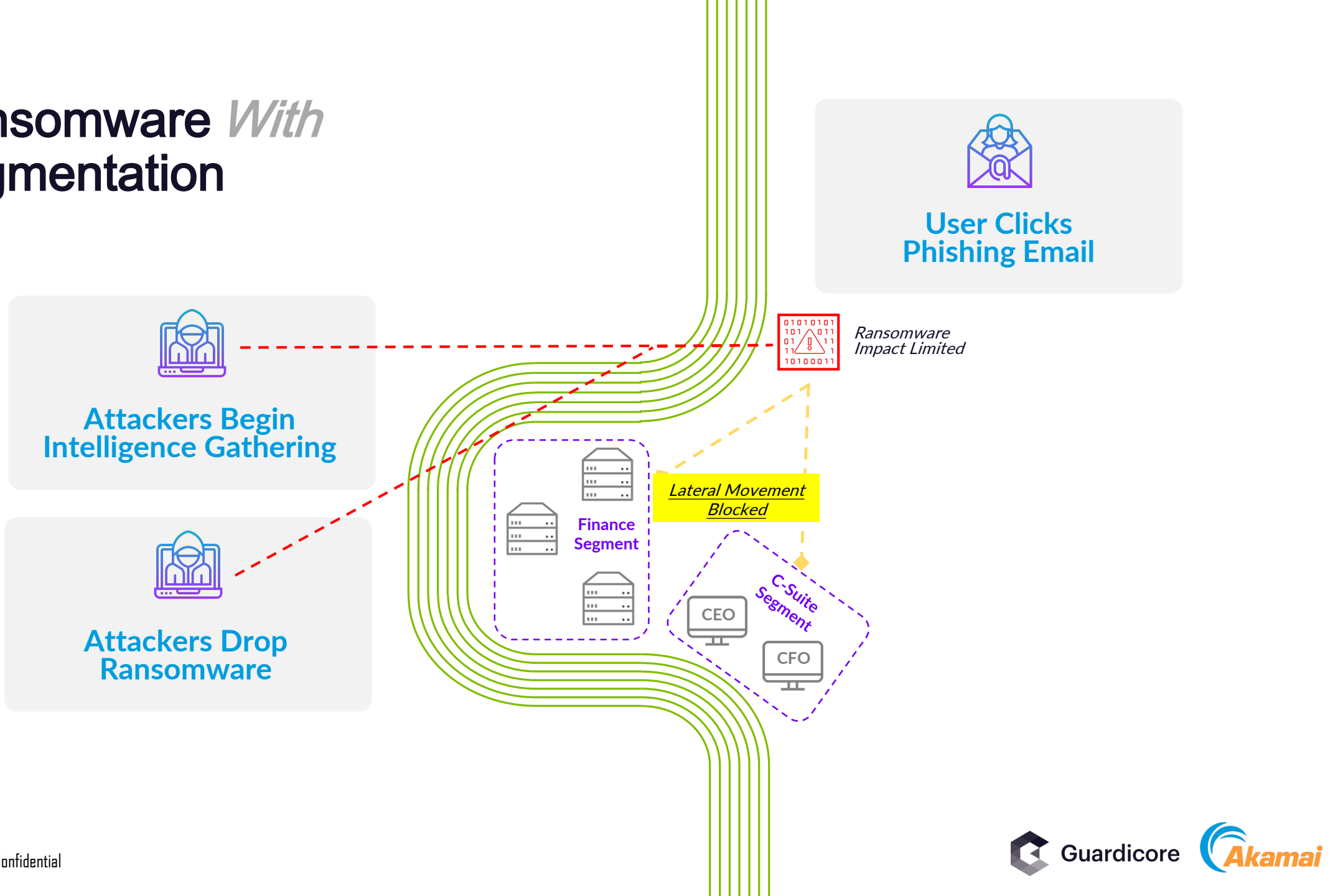
- A little as one day (e.g., EternalBlue, BlueKeep, Zerologon)
- Common target protocols: RDP, SMB, RPC, SSH, WMI

Step 5 – Exfil/Encrypt Everything/Extort x2!

Ransomware *Without* Segmentation



Ransomware *With* Segmentation



Guardicore Akamai

So Why Don't Many Organizations Excel at Segmentation?

NO VISIBILITY
into what is actually happening

DevOps driving
continuous change

Work from home:
Known and unknown endpoints connecting
from many locations

COMPLEX COORDINATION between Security and Infrastructure teams

Frequent change
windows and downtime
are untenable

Competing priorities
lead to friction and delays

The definition of a "network" is
A MOVING TARGET

Most organizations
are now hybrid cloud

Microservices and containers
communicate differently

Bottom Line:
Even though the value is clear, segmentation feels hard and risky.

Akamai Guardicore Segmentation Changes the Game

Discover

See everything, everywhere in high definition

Divide

Create software-defined Zero Trust (micro)perimeters

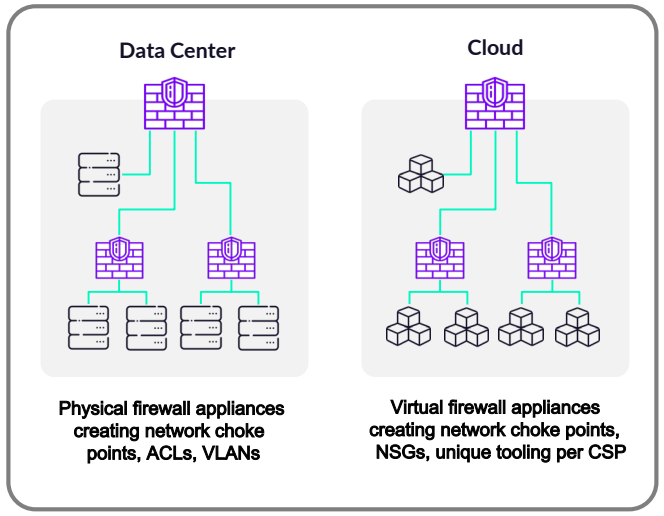
Conquer

Detect threats and respond with speed and precision

Breaches will happen, but they don’t have to be catastrophic.

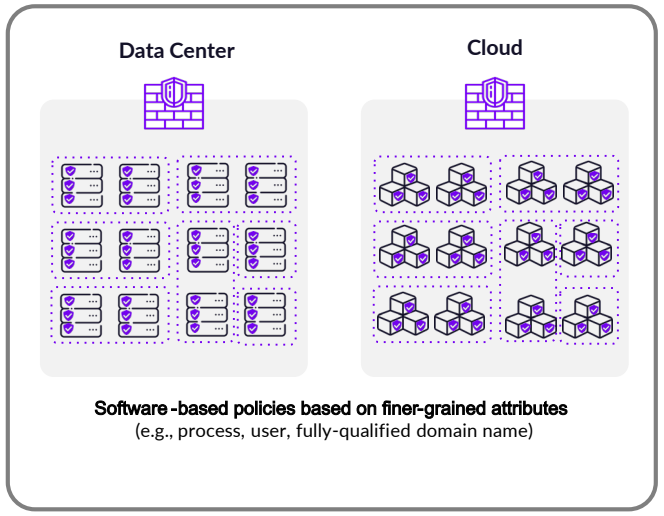
It’s Time to Rethink Segmentation

The Old Way



- Tied to environment and network
- Different approaches for different environments / technologies
- Slow and difficult to change
- Network-centric policies

The New Way



- Software-only approach
- One set of security policies that work everywhere
- Easy to visualize and change
- Workload-centric policies

Faster
Reduce Risk
Lower Costs

Minimize hardware refresh cycles and overhead

Software-Based Segmentation Versus Infrastructure-Based Segmentation

Faster

- 45 applications
- 6 weeks vs. 1.5 years
- Zero downtime

Reduce Risk

Up to 99% attack surface reduction

LowerCost

85% TCO savings over infrastructure based segmentation

High-Impact Achieved in Minutes

Operations

- Fast and non-disruptive to deploy
- Simple, AI-based policy creation
- Fast and intuitive ongoing updates
- Scales easily as needs evolve

Security

- Consistency across platforms and environments
- Protects every segment between every workload
- Based on context instead of network choke points
- Extends security to users and endpoints
- Immediately begin Threat Hunting as agents are being deployed

Demo

Akamai

Reducing Ransomware Risk with Guardicore

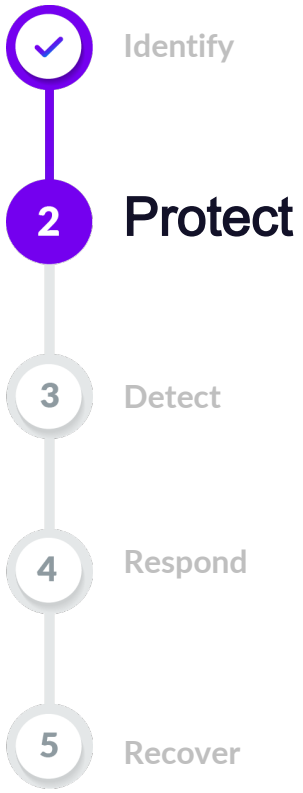
NIST Framework	Identify	Protect	Detect	Respond	Recover
	1	2	3	4	5
Guardicore Capabilities	Map your assets Identify critical data Map security gaps	Secure common ingress points Block common propagation paths Segment critical assets	Detect lateral movement Detect access to command and control	Quarantine affected networks Disconnect clean environments Block command and control access	Phased access provisioning Full visibility for clean recovery

How Software -Based Segmentation Helps

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

1. Provide full visibility into the IT landscape
2. Quickly map critical assets, critical data, backups and their risk posture
3. Create response playbooks and rules to be activated during an outbreak:
   - Disconnect backups
   - Disconnect sites
   - Etc…

How Software -Based Segmentation Helps

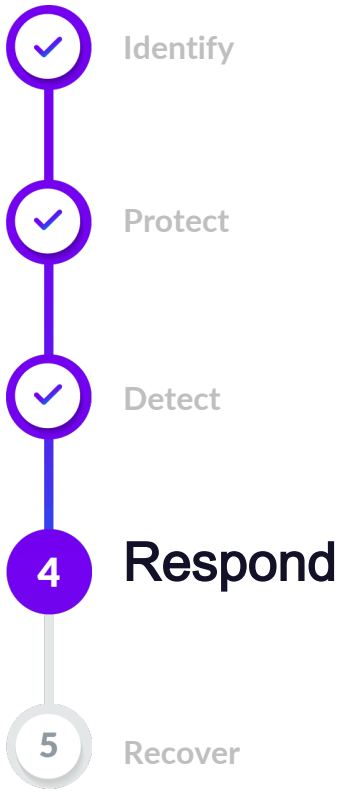


1. Introduce rules to block common ransomware propagation techniques
2. Ring-fence critical applications, backups, file servers, databases
3. Introduce Zero Trust access from users to applications
4. Restrict traffic from users to users
5. Limit blast radius with micro-segmentation

How Software -Based Segmentation Helps

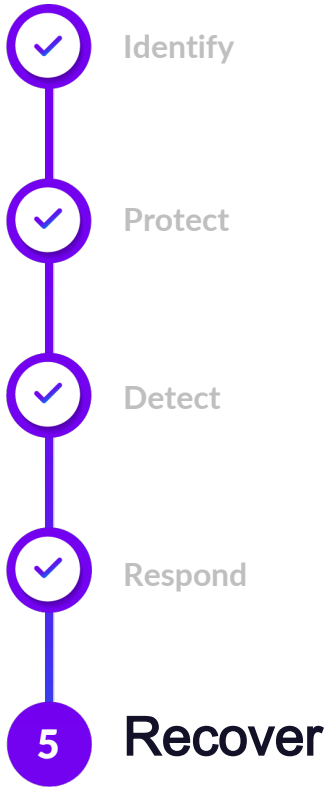
1. Alert on access violation to critical applications and backups
2. Alert on access to malicious domains or detection of known malicious processes
3. Alert on detection of network scans
4. Alert on deception incident indicating lateral movement

How Software -Based Segmentation Helps



1. Use Guardicore Reveal and Guardicore Insight to identify the scope of the breach
2. Introduce quick isolation rules to disconnect affected parts of the network
3. Enforce rules to block access to backups
4. Block access to critical applications and sites
5. Disconnect from internet
6. Introduce mitigation rules based on ransomware IOCs

How Software -Based Segmentation Helps



1. Phased secure recovery with increasing connectivity
   - Phase 0: allow connectivity only inside the app
   - Phase 1: allow access to common services
   - Phase 2: allow access to other applications
2. Verification and validation with Reveal and Insight

Success Story:

Stopping 'DarkSide' Ransomware with Software-Based Segmentation

Customer Background

- Leading communications infrastructure operator
- Highly mobile workforce with 6,000+ Windows laptops

Security Priorities

- Ransomware
- "Shadow IT" activity
- East-west traffic visibility

Problem:

- WFH employees with public IP addresses and open services to the Internet
- Indication of brute force attack originating from Russia and China
- Ultimately attributed to DarkSide (gang linked to Colonial Pipeline incident)

Solution:

- Customer enforced one rule to immediately block RDP
- DarkSide ransomware group was left with no possible points of entry

Result:
Avoided likely $1 million+ loss

Thank you for participating!

Any Questions?

Michael Mikelas
Manager, Solutions Engineering
Akamai Guardicore Segmentation

Brian S. Dennis
Principal Technologist-Public Sector
Akamai Technologies