
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?

Douglas Holland

Senior Solutions Engineer
Akamai Technolgies

Douglas Holland is a professional communicator of technical ideas. As a Solutions Engineer at Akamai Technologies, he is passionate about helping customers solve business challenges, enhancing digital experiences, and improving their security posture. He currently works with State, Local, and Education organizations in the United States and Canada to improve the performance and security of their online digital properties.

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**

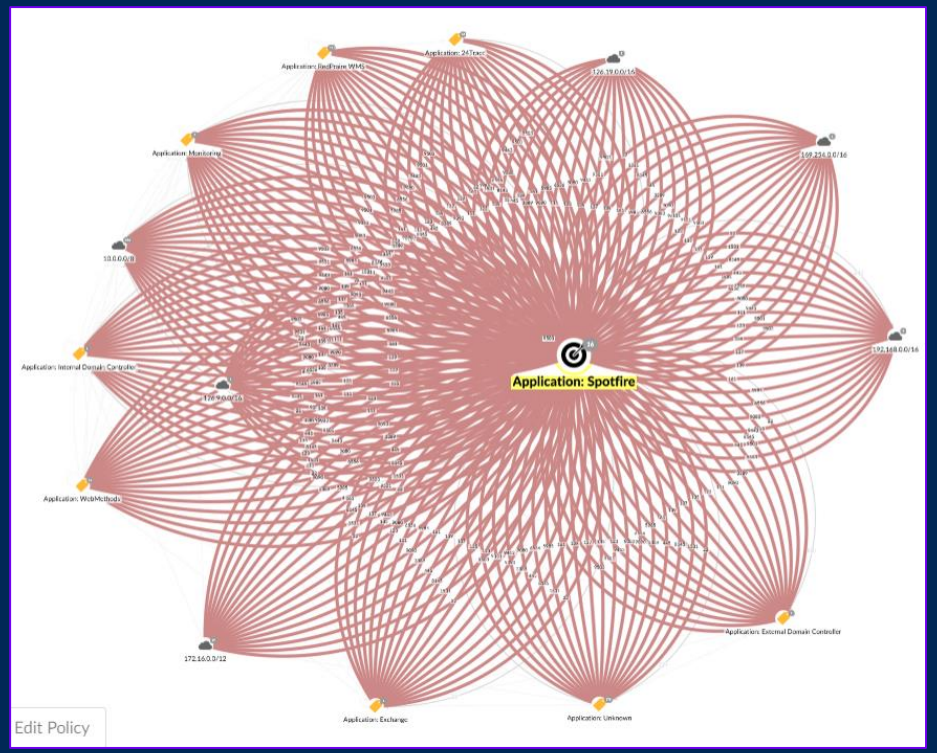
But which of these things is often considered the most daunting leap for organizations?

A Closer Look:

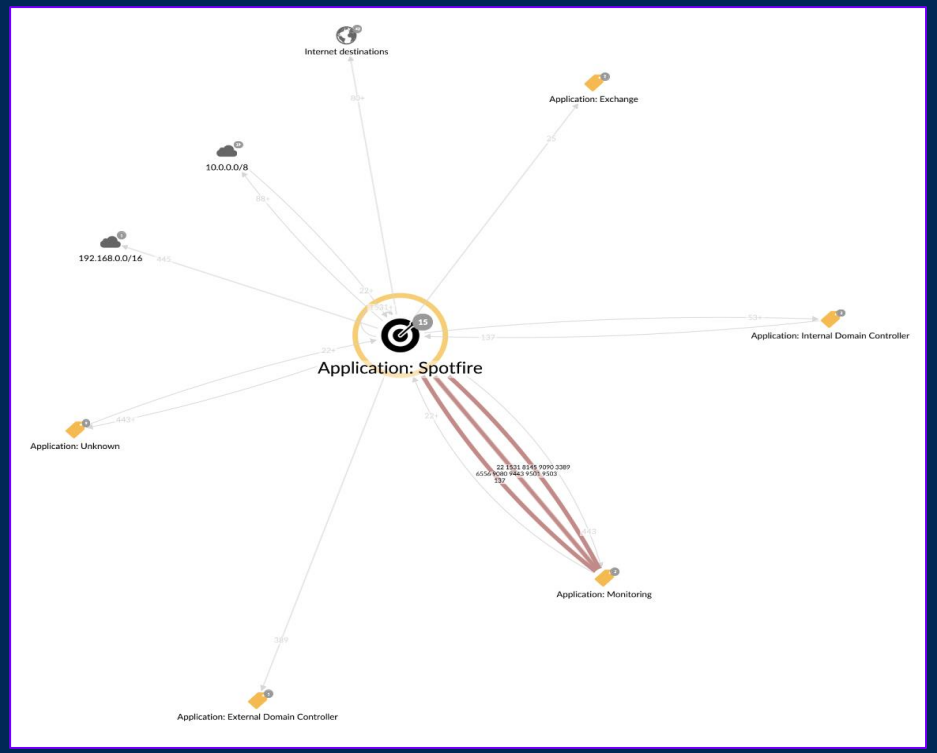
Ransomware Mitigation with Software-Based Segmentation

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

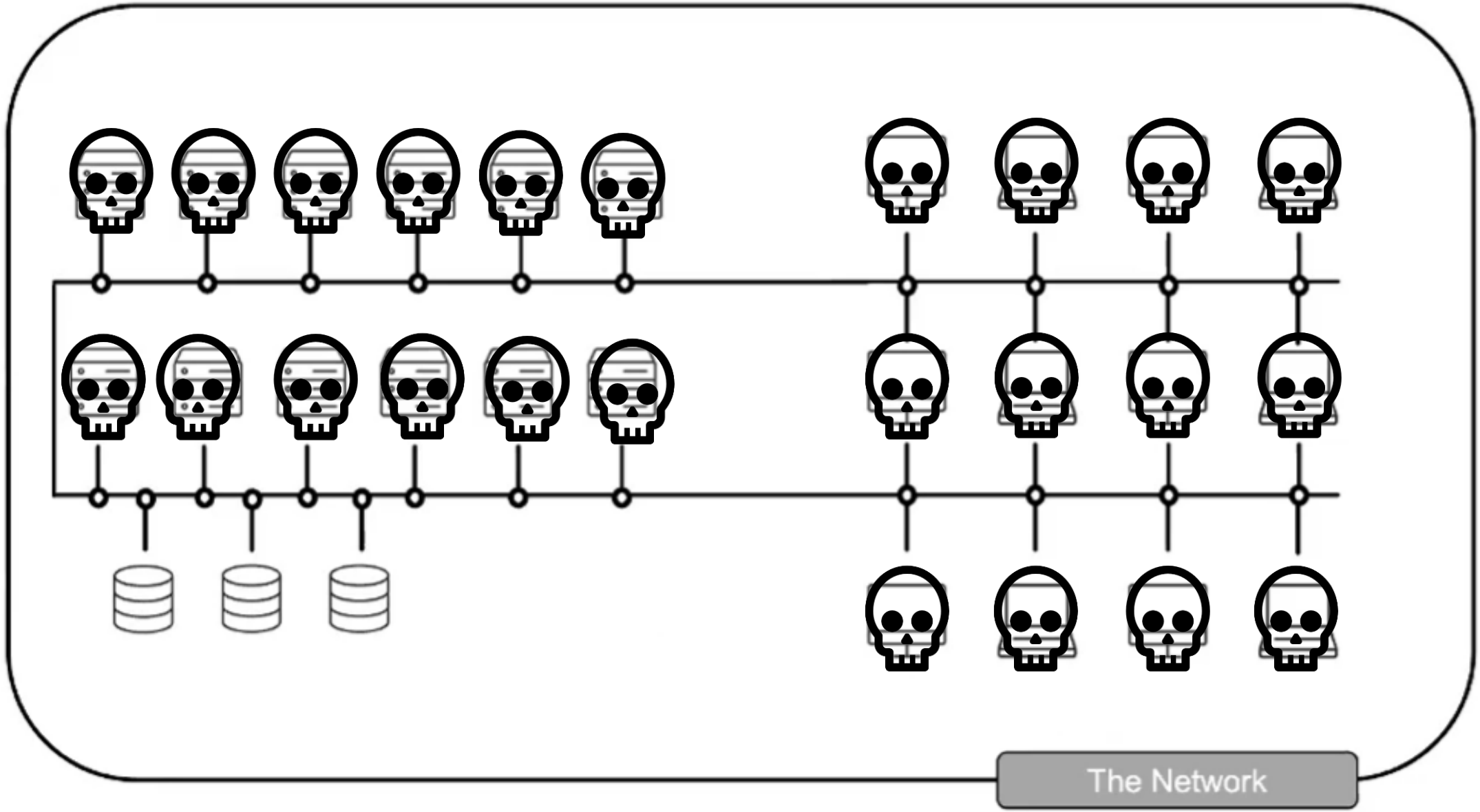
- Move laterally towards the system with privileged account
- Harvest credentials

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

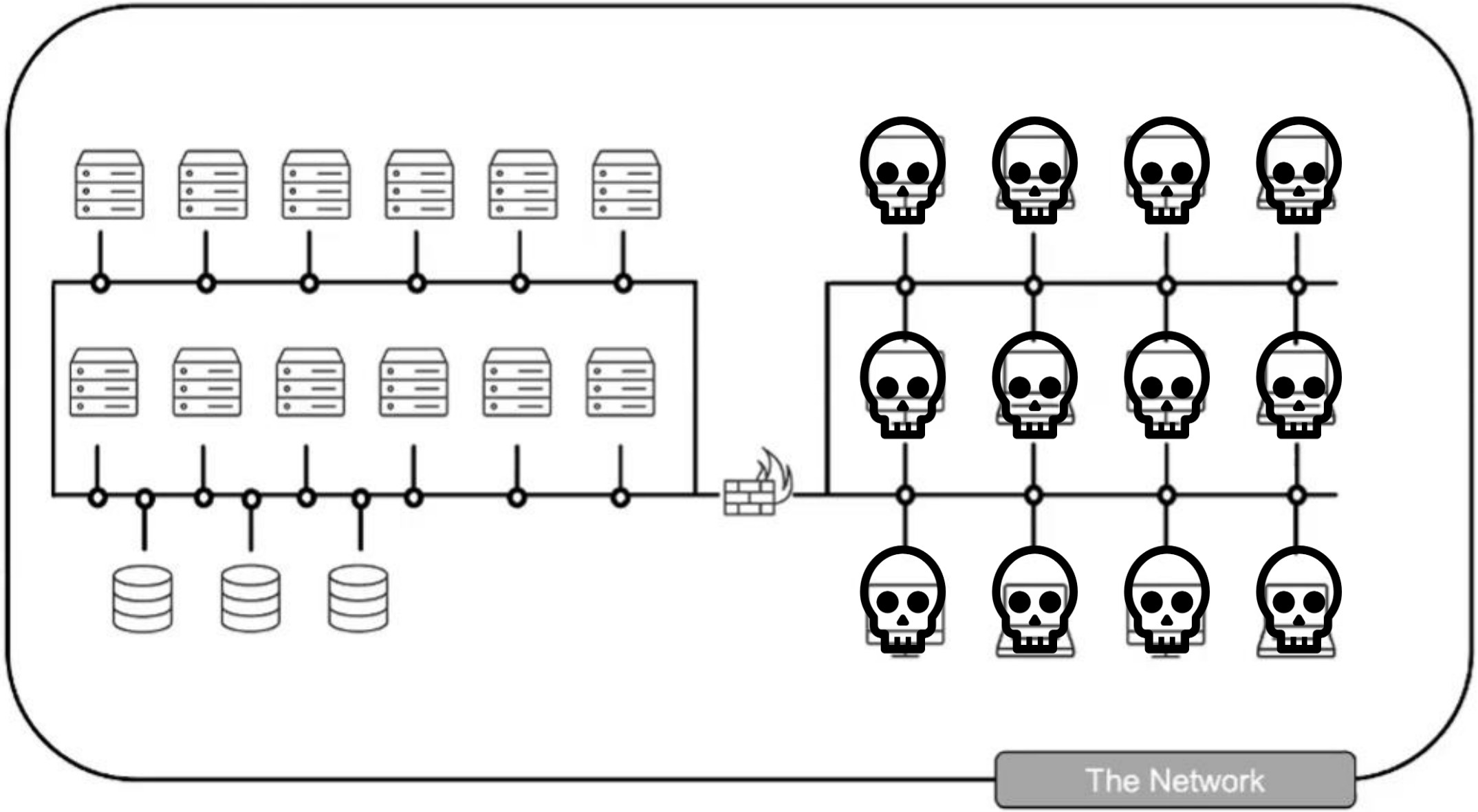
- A little as one day (e.g., EternalBlue, BlueKeep, Zerologon)
- Common target protocols: RDP, SMB, RPC, SSH, WMI

Step 5 – Exfil/Encrypt Everything/Extort x2!

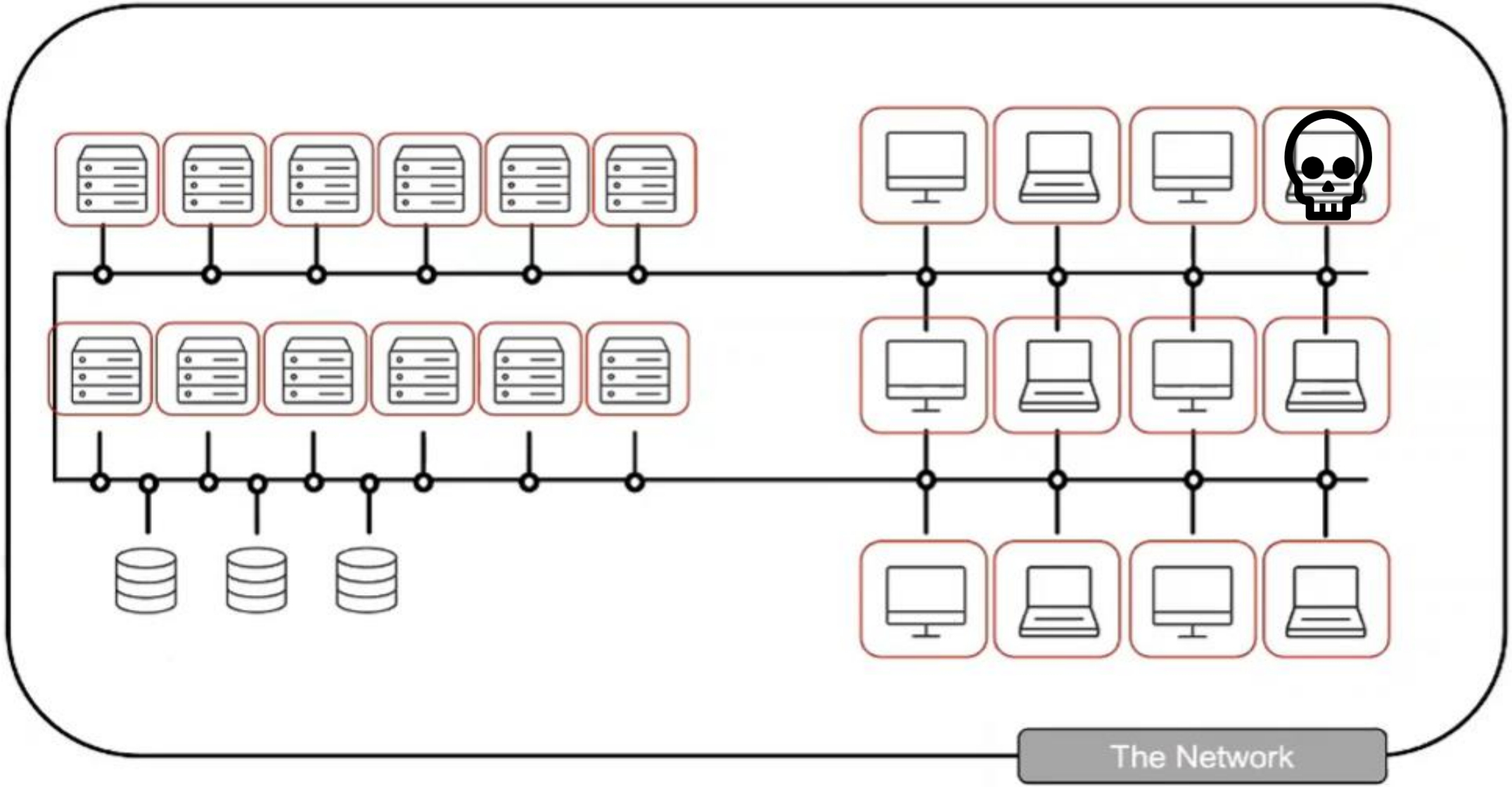
Network Segmentation: Flat Network



Network Segmentation: Segmentation Added



Network Segmentation: Microsegmentation



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

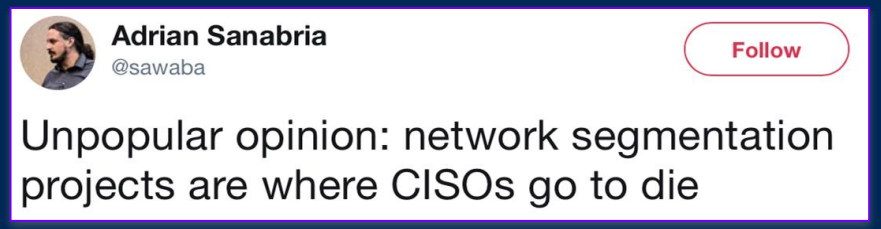
Frequent change windows and downtime are untenable

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

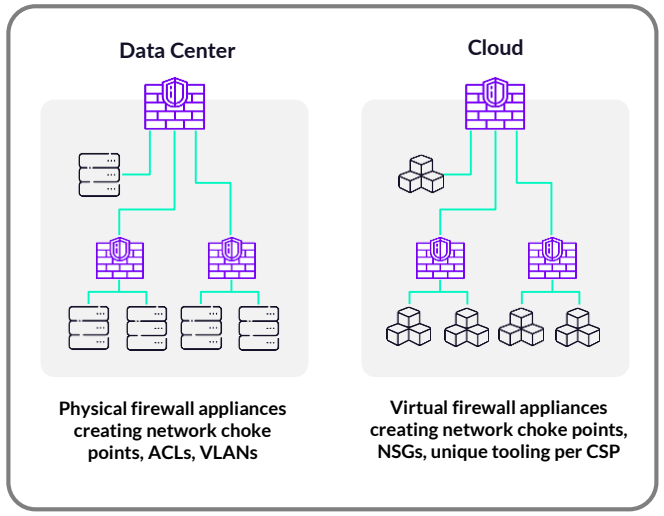
Conquer

Detect threats and respond with speed and precision

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

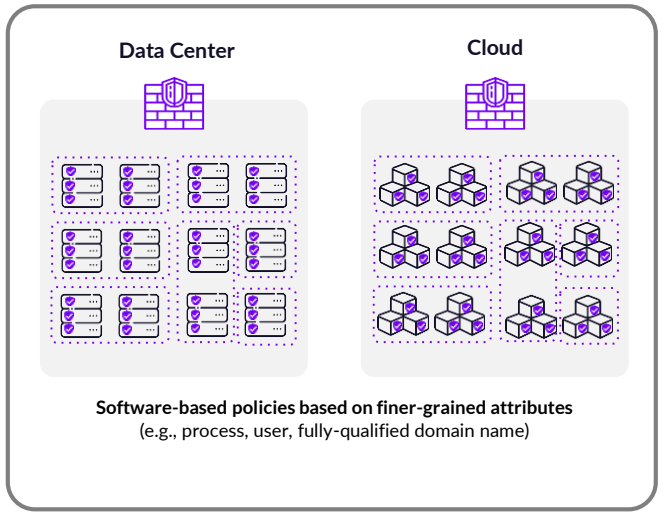
It’s Time to Rethink Segmentation

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

Broad Environment and Platform Coverage

The Rest of the Market	Guardicore
• Can only support modern Windows and Linux OS versions • Cannot support legacy use cases • Cannot support agentless • No 3rd party integrations	• Maintain widest agent coverage in the industry! • Legacy OS support • Agentless solutions available when agents can't be installed – leave no risk on the table • No friction with existing configurations • Integration with 3rd party flow providers and enforcement points

Customer Impact

- Many organizations still keep their crown jewels on legacy systems due to various IT constraints
- Inability to support those systems takes the bane out of the whole idea of segmenting them

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

Demo

Akamai

Agent OS Support Matrix

Akamai Guardicore supports the following operating systems for agent installations:

- Modern Windows / Linux: Fully supported.
- Legacy Windows / Linux: Supported with L4 enforcement.
- AIX, Solaris of specific versions: Supported with L4 enforcement.
- HP-UX of specific versions: Supported for Visibility only.
- FreeBSD of specific versions: supported with L4 Visibility and L4 Enforcement.

OS support matrix is continuously extended by Guardicore.

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?

Douglas Holland
Senior Solutions Engineer
Akamai Technologies

Brian S. Dennis
Principal Technologist-Public Sector
Akamai Technologies

