





Ransomware Prevention Methods:

Keeping the Threats Out of Texas
Higher Education



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 Technologies

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?**



1,740

**Attacks
against
schools and
universities**



\$6.62 Billion

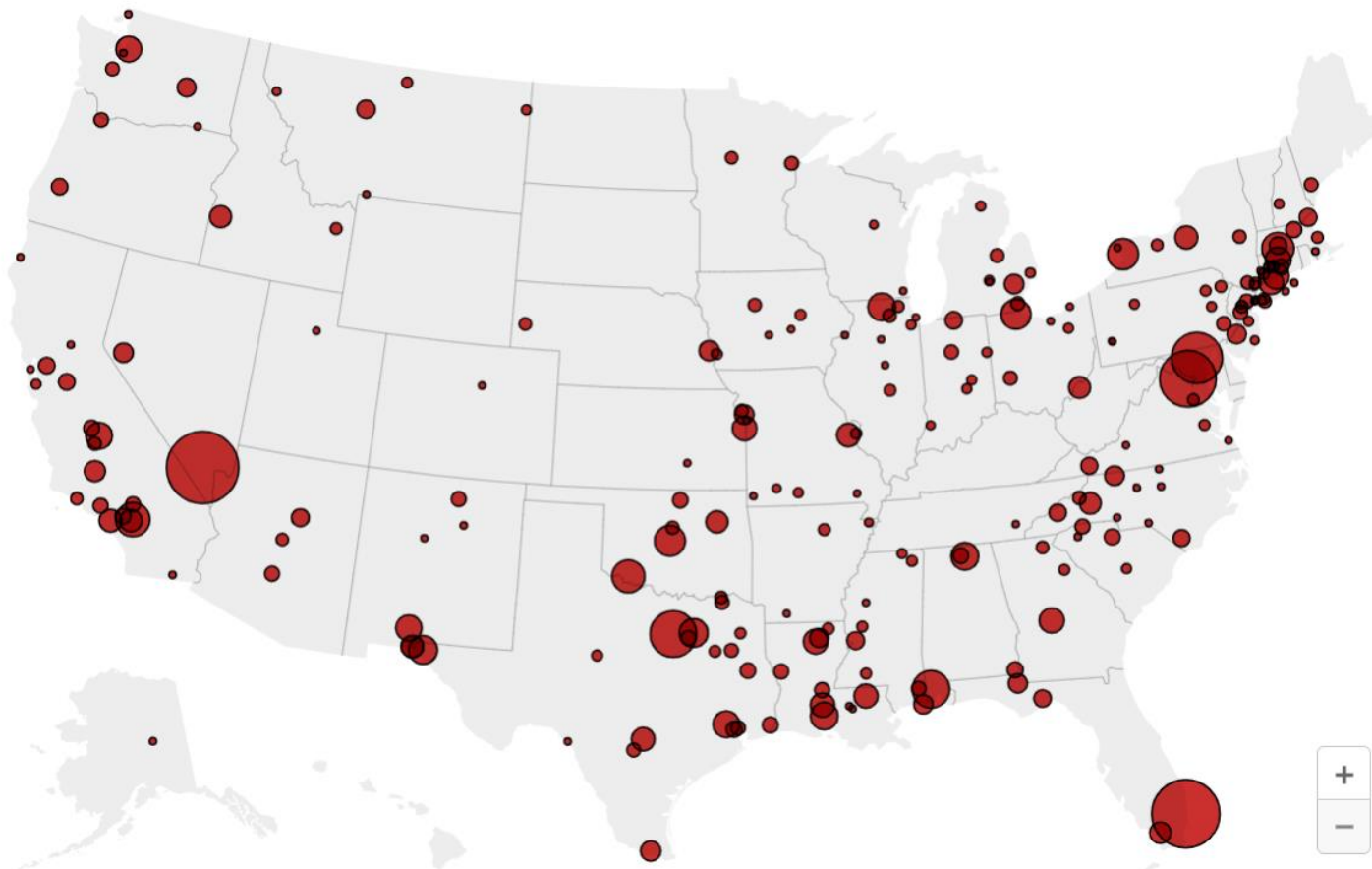
**Downtime
Costs**



1.36 Million

**Students
disrupted by
ransomware**

2021 Attack Map



A Closer Look:

Ransomware Mitigation with Software-Based Segmentation

Let's Talk More About Legacy Systems



Challenges

- Security
- Data Quality
- Costs
- Productivity

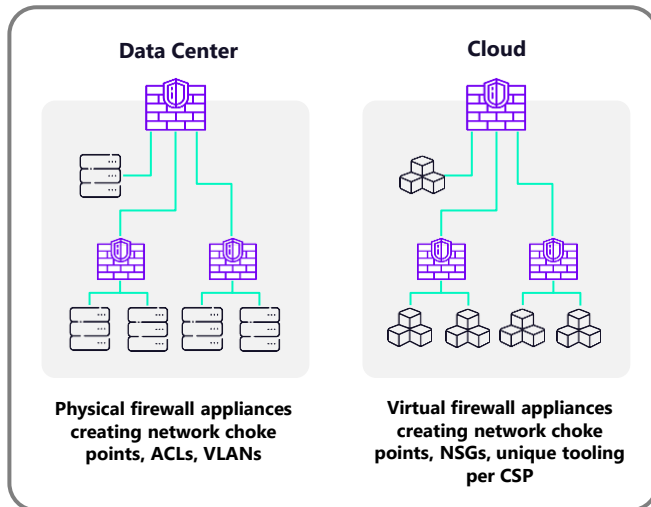


Strategies

- Isolate the Legacy System
- Identify Vulnerabilities
- Harden Security
- Inventory Access and Data
- Deploy Software Based Segmentation

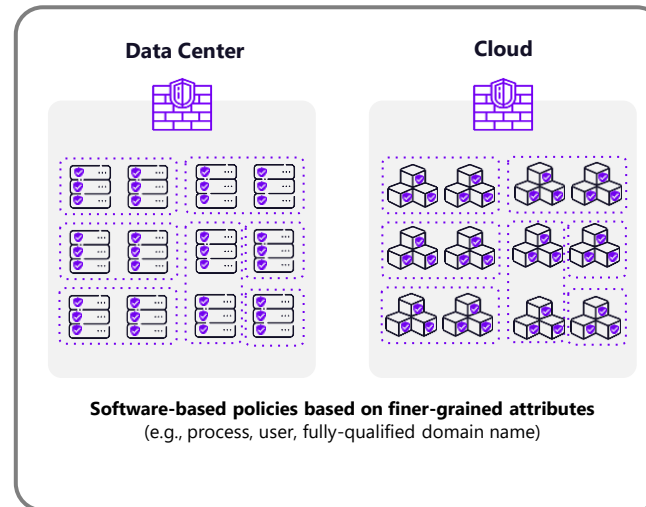
It's Time to Rethink Segmentation

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



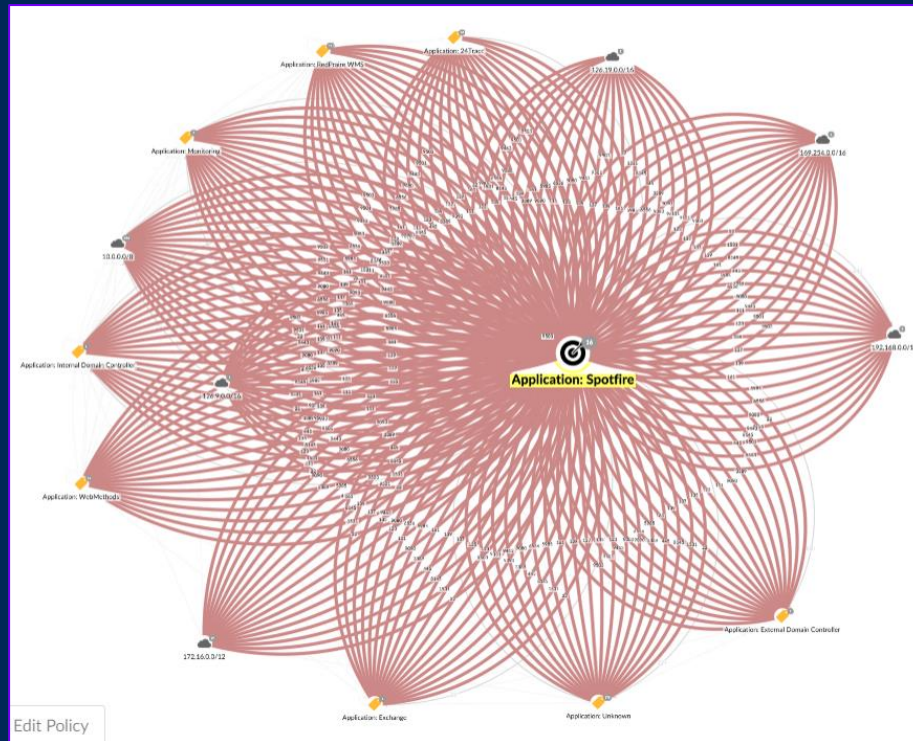
- Software-only approach
- One set of security policies that work everywhere
- Easy to visualize and change
- Workload-centric policies

Faster
Reduce Risk
Lower Costs

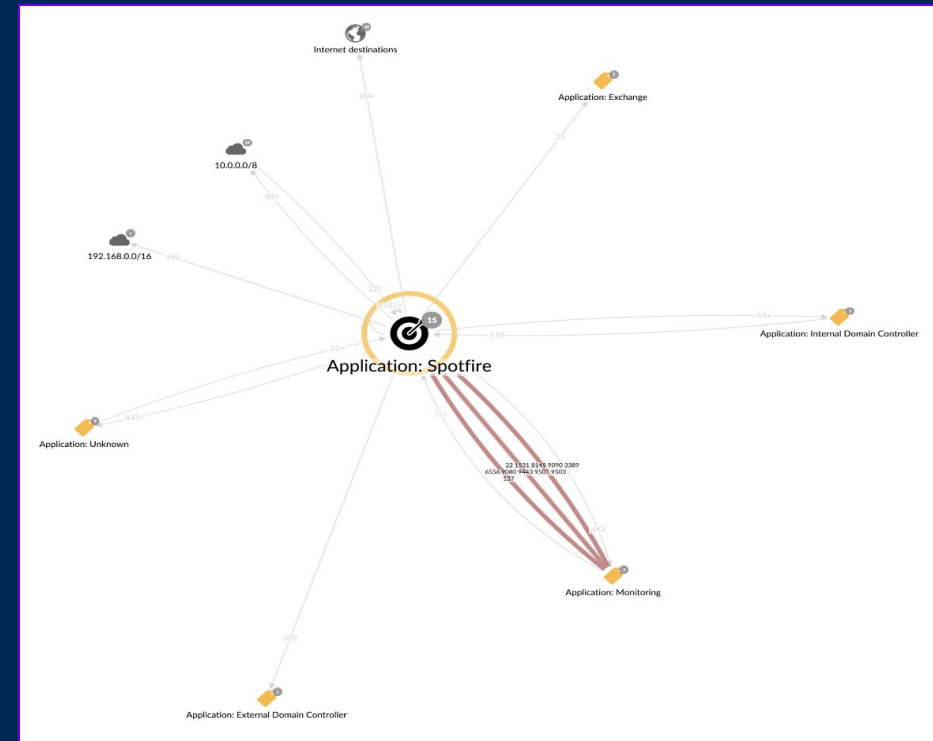
*Minimize hardware
refresh cycles and
overhead*

Segmentation - a critical control for Ransomware

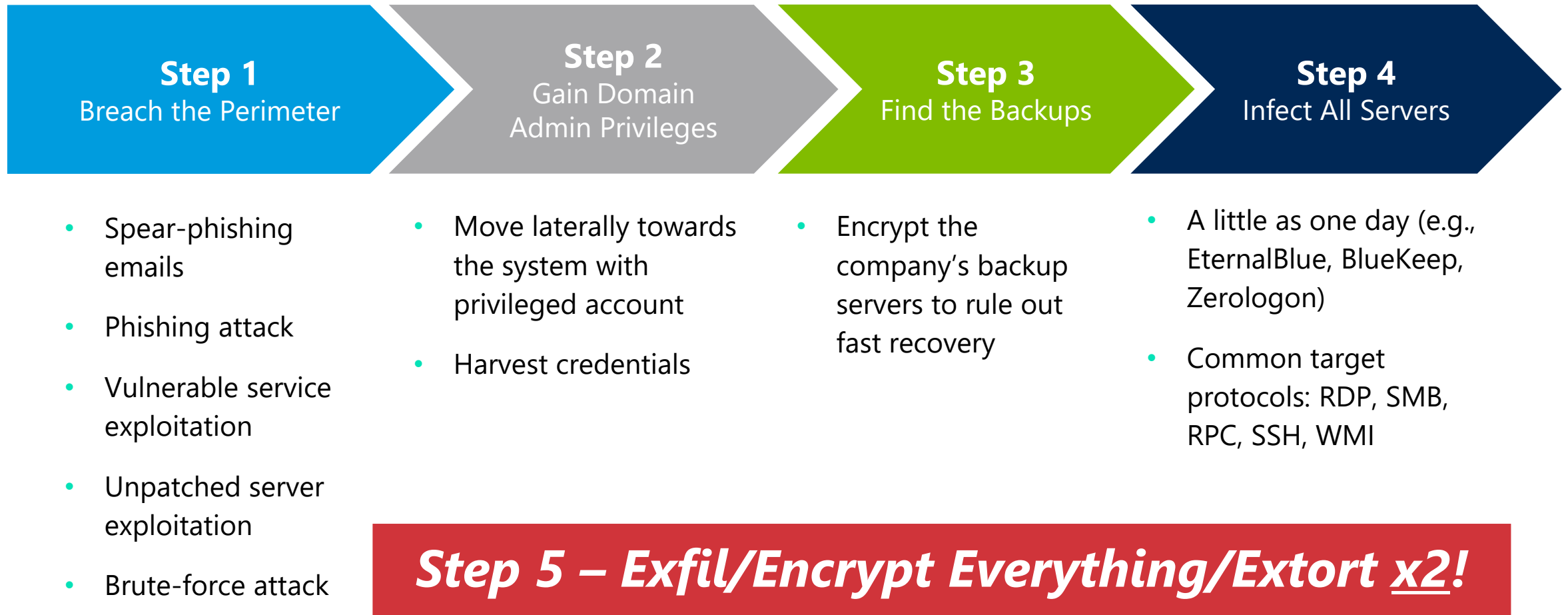
Without segmentation



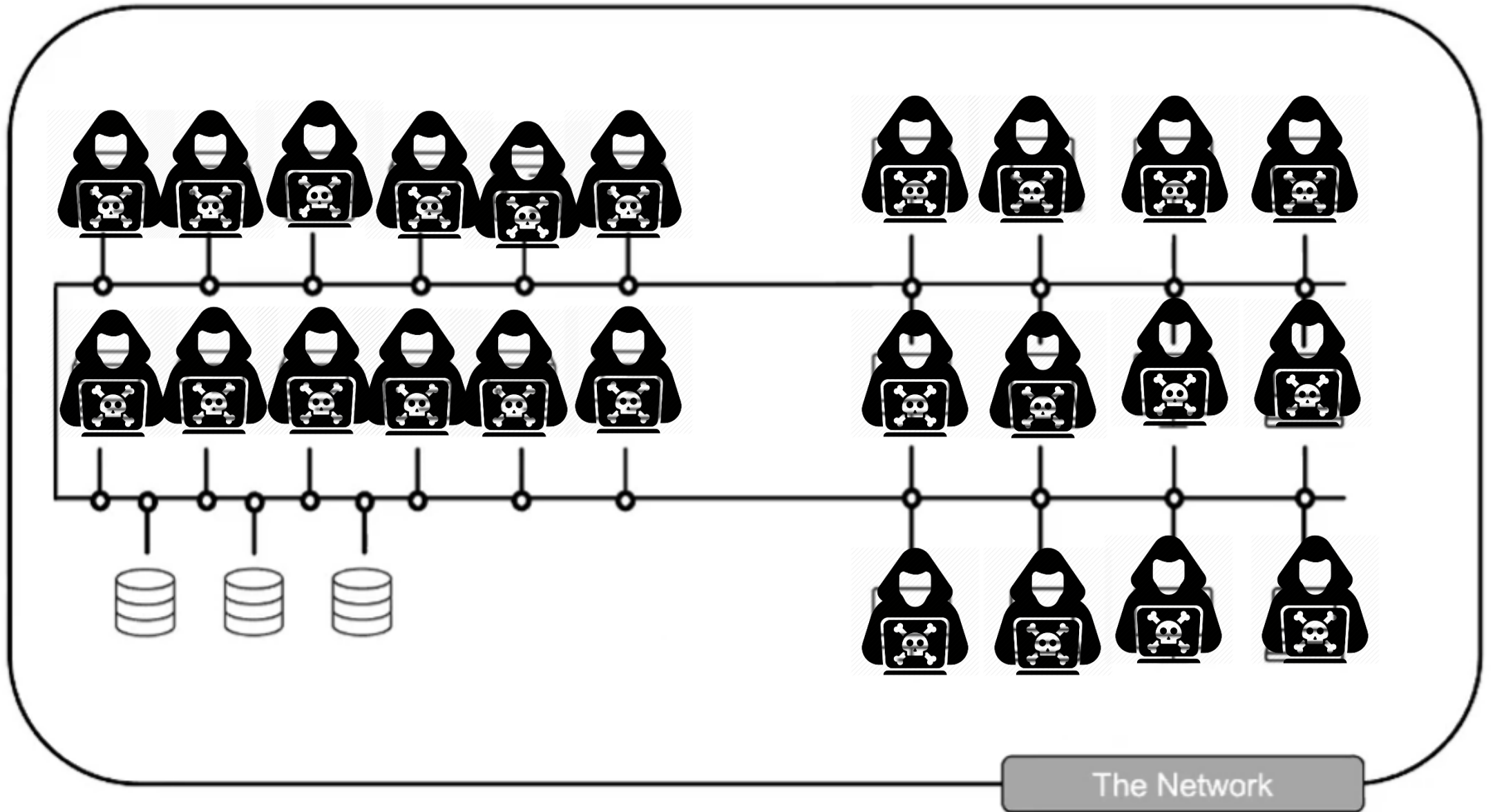
With segmentation



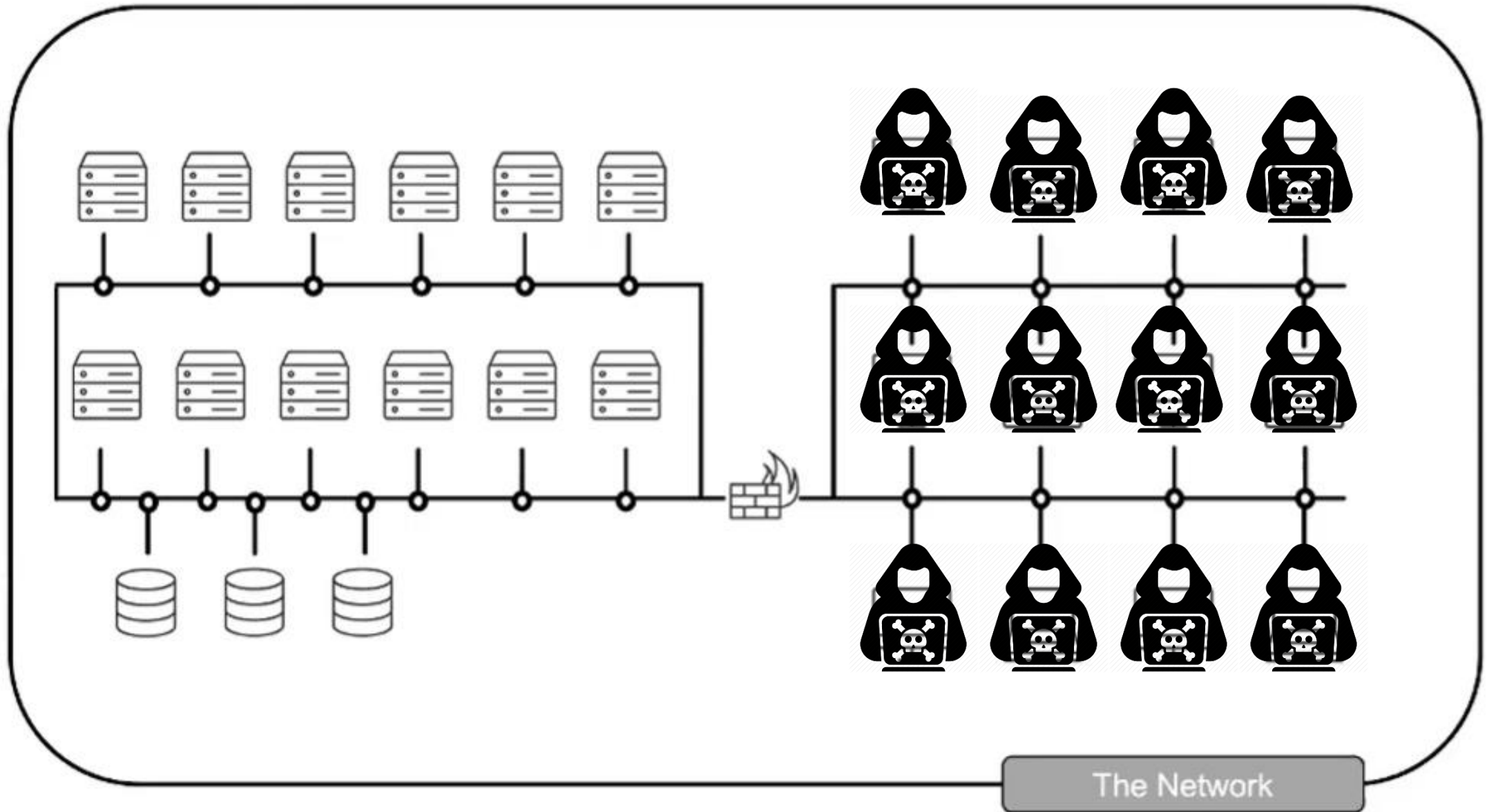
How a Typical Ransomware Attack Unfolds



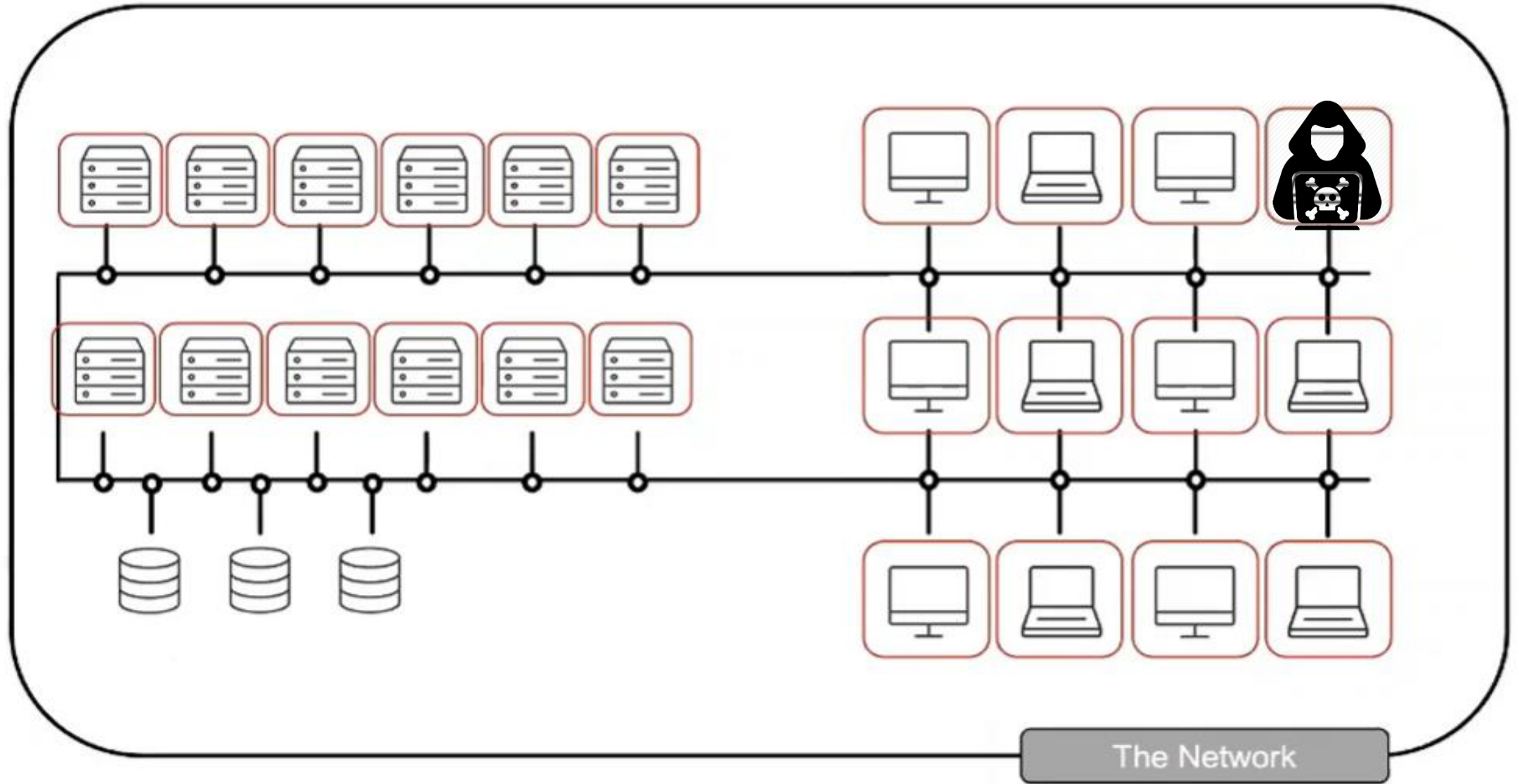
Network Segmentation: Flat Network



Network Segmentation: Segmentation Added



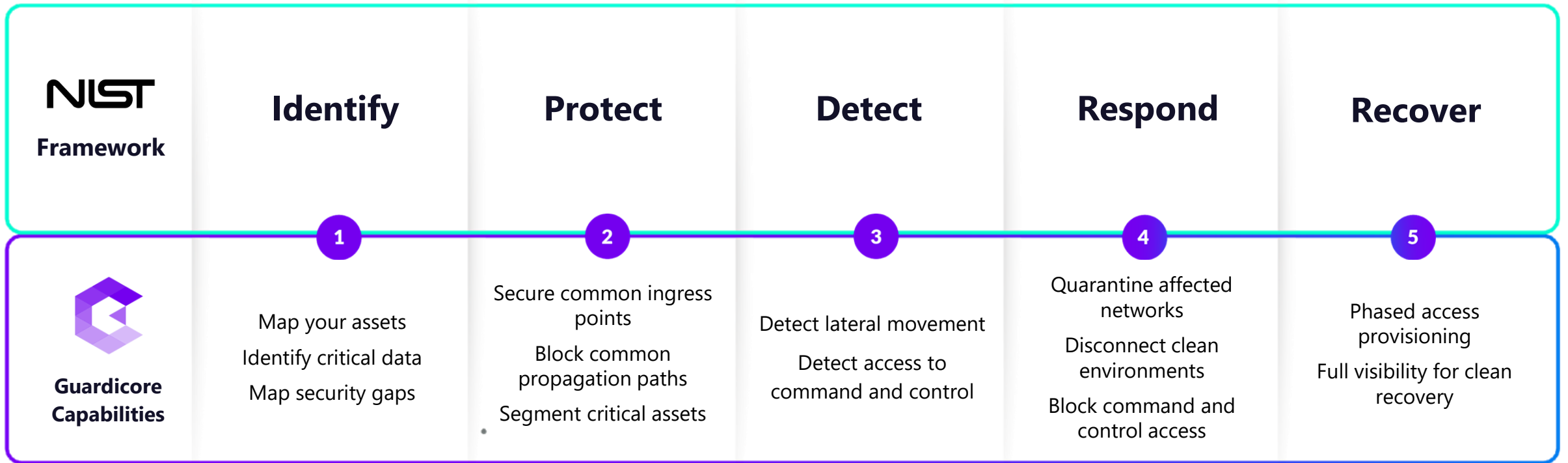
Network Segmentation: Microsegmentation



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



Reducing Ransomware Risk with Guardicore



Demo



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

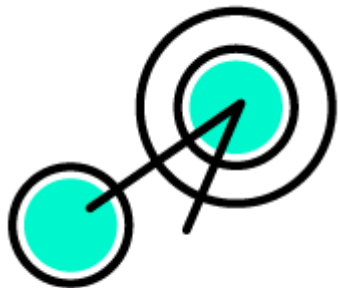
Competing priorities
lead to friction and delays

The definition of a “network” is
A MOVING TARGET

Most organizations
are now **hybrid cloud**

Microservices and containers
communicate differently

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

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



Lower Cost

85% TCO
savings over
infrastructure
based
segmentation

Broad Environment and Platform Coverage

The Rest of the Market	Guardicore
<ul style="list-style-type: none">• Can only support modern Windows and Linux OS versions• Cannot support legacy use cases• Cannot support agentless• No 3rd party integrations	<ul style="list-style-type: none">• 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 retain their crown jewels on legacy systems due to various IT constraints
- Inability to support legacy systems takes the bane out of the whole idea of segmenting them



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
- Empowers immediate Threat Hunting as agents are being deployed

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