Microsoft

Securing Windows Server 2016

Module 1: Security Threat Landscape

Microsoft Services

Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet website references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see **Use of Microsoft Copyrighted Content** at
https://www.microsoft.com/en-us/legal/intellectualproperty/permissions/default.aspx

Microsoft®, Internet Explorer®, Outlook®, SkyDrive®, Windows Vista®, Zune®, Xbox 360®, DirectX®, Windows Server® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Objectives

- After completing this learning unit, you will have an understanding of:
  - The impact security has, the evolution of attacks and the anatomy of an attack
  - How credentials and privileged access can be protected
  - How to protect applications and data in any cloud
  - How to protect the virtualization fabric
  - How to protect with “just enough” OS

Lessons

Lesson 1: Security, attacks and threats

- Introduction

Lesson 2: Securing the environment

- Basics
- Help protect credentials and privileged access
- Help protect applications and data in any cloud
- Help protect the virtualization fabric
- Protect with just enough OS
- Windows Server 2016 security summary

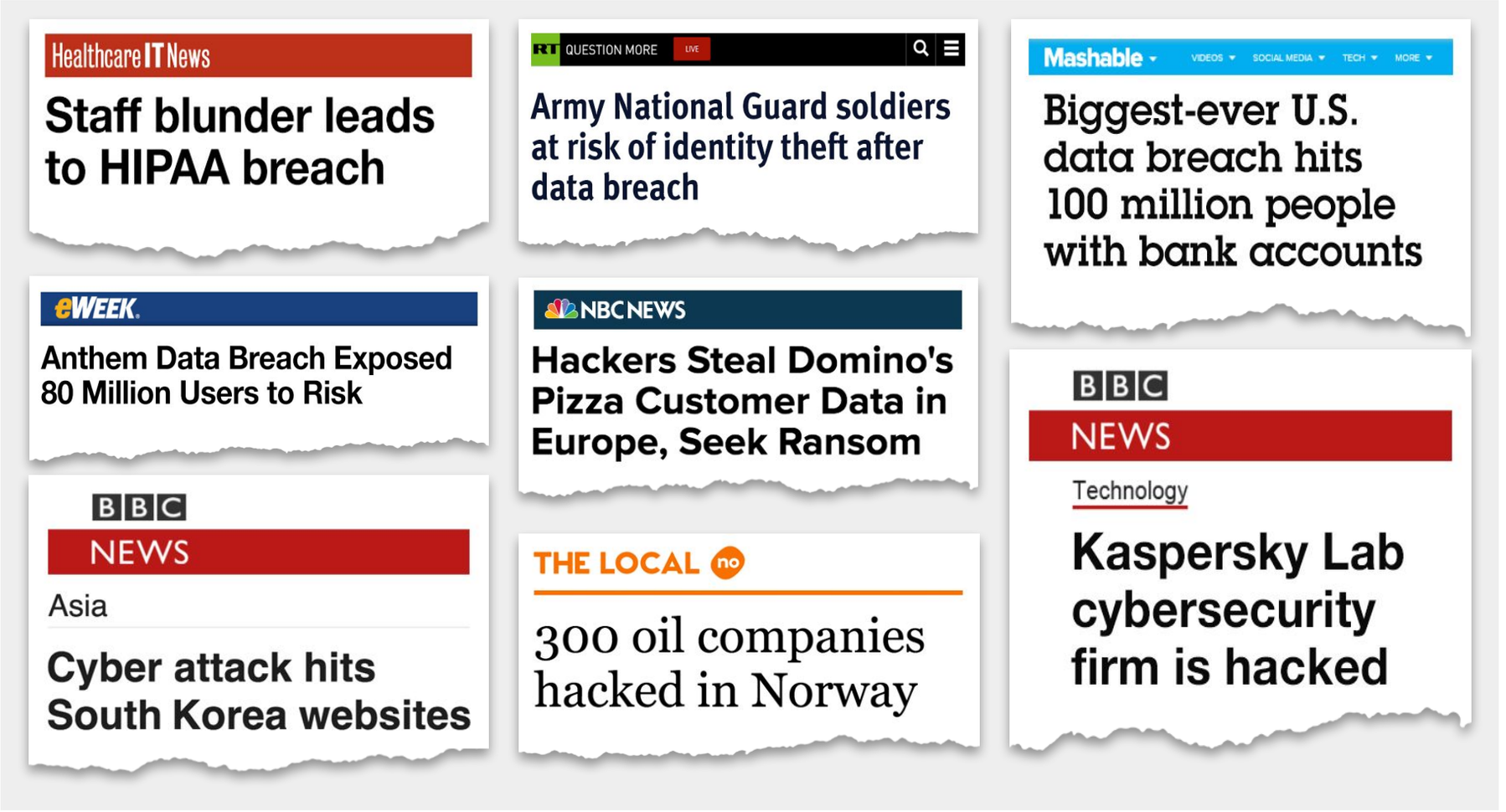
Security Threat Landscape

Lesson 1: Security, attacks and threats

Section: Introduction

Security is a Top Priority for IT

- Increasing incidents
- Multiple motivations
- Bigger risk



Evolution of Attacks

Mischief

Script Kiddies

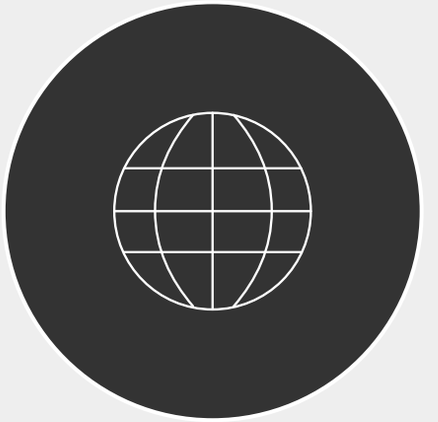
Unsophisticated

Fraud and theft

Organized Crime

More sophisticated

Damage and disruption



Nations, Terror Groups, Activists

Very sophisticated and well resourced

“Cyber security is a **CEO issue**.”

-McKinsey

$3.0 Trillion

Impact of lost **productivity and growth**

$4 Million

Average **cost of a data breach** (15% YoY increase)

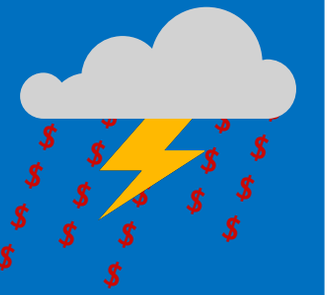
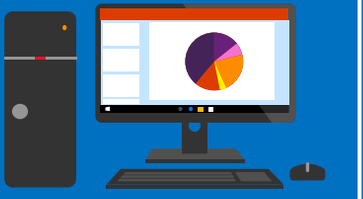
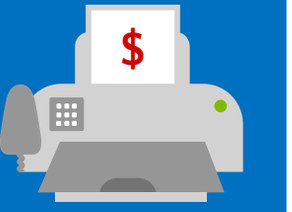
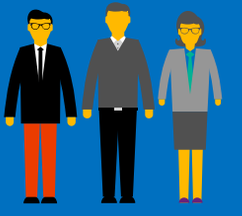
$500 Million

Corporate **liability** coverage.

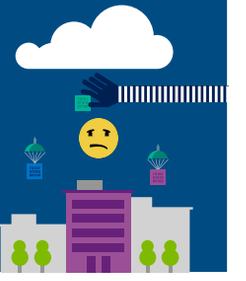
Cyber threats are a **material risk** to your business

Source: McKinsey, Ponemon Institute, Verizon

Microsoft Services

	Before	After
Breaches cost a lot of money (Average $4M based on Ponemon Institute)	• Customers pay for your services 	• You pay customers compensation to keep them using your services 
Productivity	• Employees efficiently perform work activities 	• Employees waste hours a day using manual processes 
Overspending Reflex	• Appropriately sized & dedicated IT Security team 	• IT Security team exponentially increases in size and remediation efforts require new and expensive products 

Microsoft Services

	Before	After
Industry Reputation	• Industry credibility, positive reputation, customer confidence • Corporate secrets are secret	• Loss of credibility, embarrassing information exposed, customer's lose faith • Corporate secrets are public knowledge; potential loss of competitive advantage
Ransomware	• HBI/MBI assets available for day-to-day business operations 	• Assets encrypted and key business IT services rendered useless 
Customer trust	• Customers happy to trust you with their personal information 	• Customers reluctant to share information with you 

Different Attack Vectors

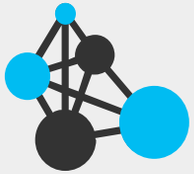
Attack the applications and infrastructure

Compromised privileged accounts

Unpatched vulnerabilities

Phishing attacks

Malware infections



Attack the virtualization fabric

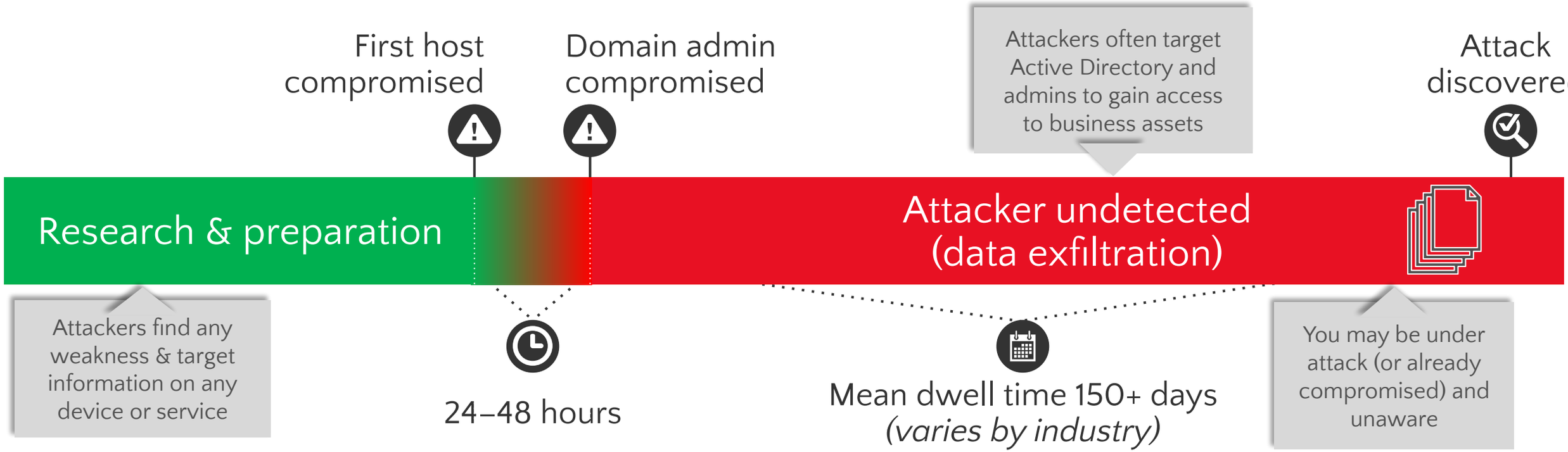
Compromised fabric exposes guest VMs

Easy to modify or copy VM without notice

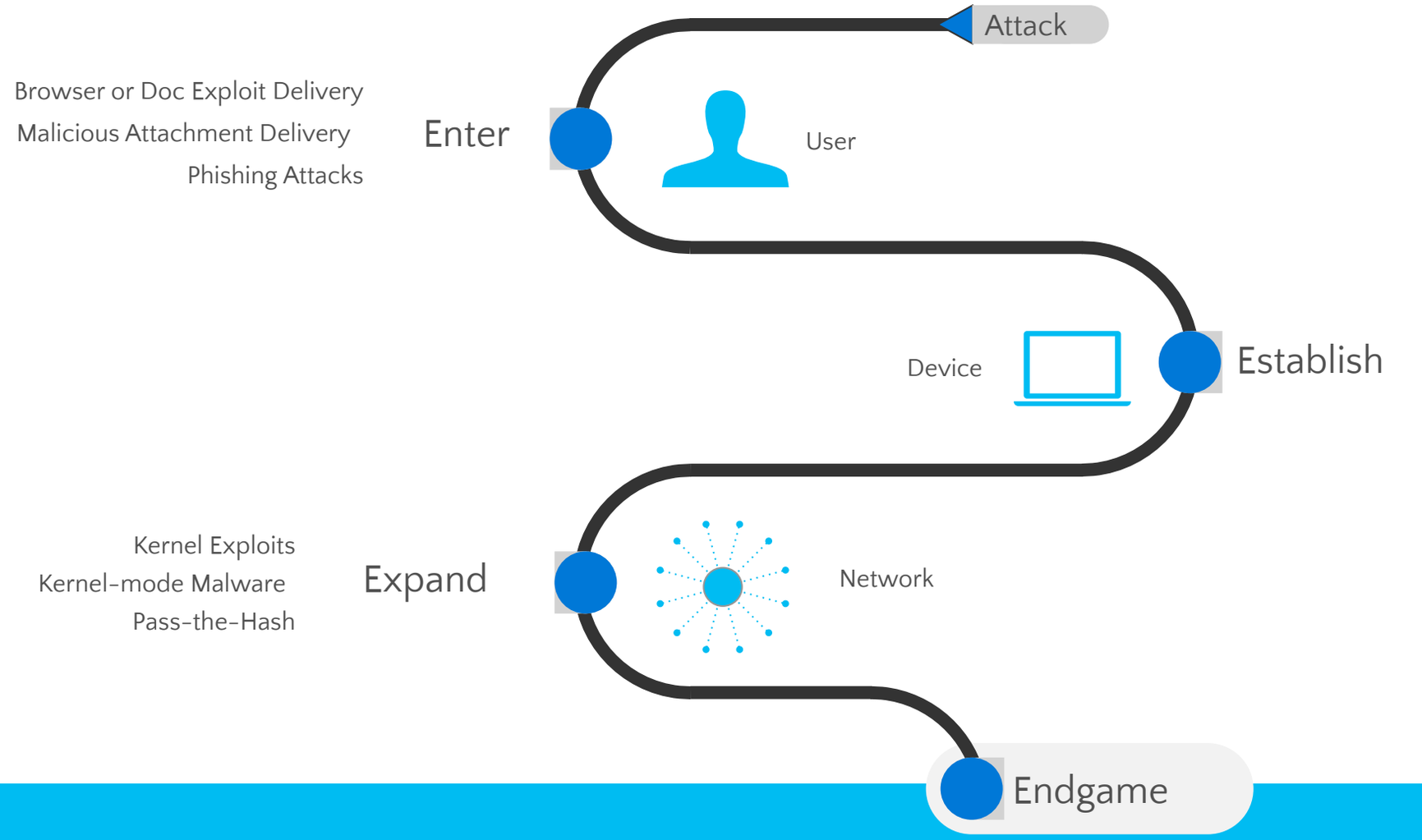
Can’t protect a VM with gates, walls, locks, etc.

VMs can’t leverage hardware security (e.g., TPM)

Attack Timeline



Anatomy of an Attack



BUSINESS DISRUPTION LOST PRODUCTIVITY DATA THEFT ESPIONAGE, LOSS OF IP RANSOM

Example Attack Scenario

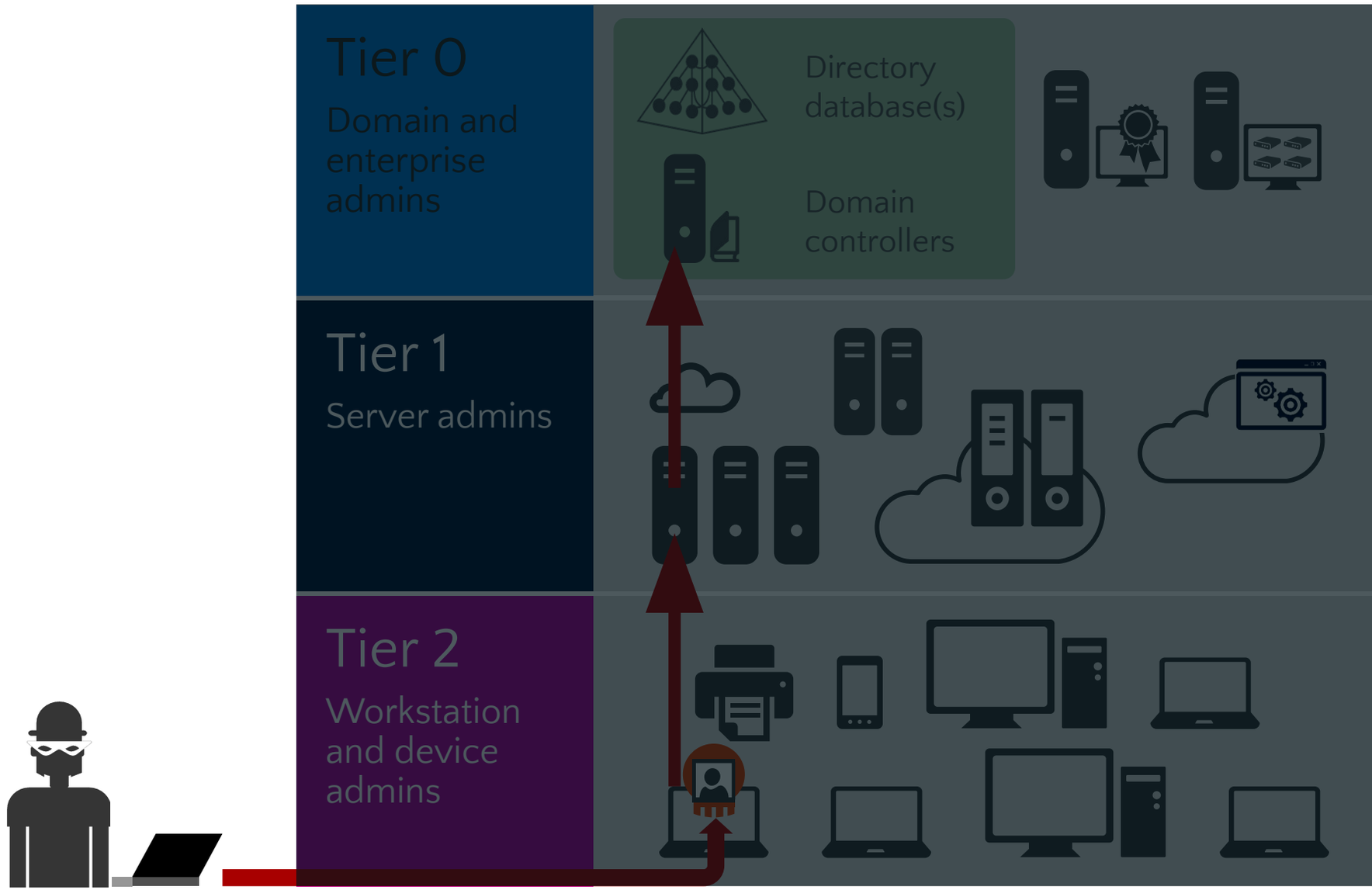
Compromises administrative control

24–48 hours

3. Execute primary mission
   a. Steal data, destroy systems, etc.
   b. Persist presence

2. Privilege escalation
   a. Compromise unpatched servers

1. Beachhead
   (Phishing Attack, etc.)



Schoolboard
50
Employees
300
Students
Public funds

Construction
4,000
Employees
$30 millions YR
Private funds

Energy
95,000
Employees
$5 billions YR
Private funds
Shareholders

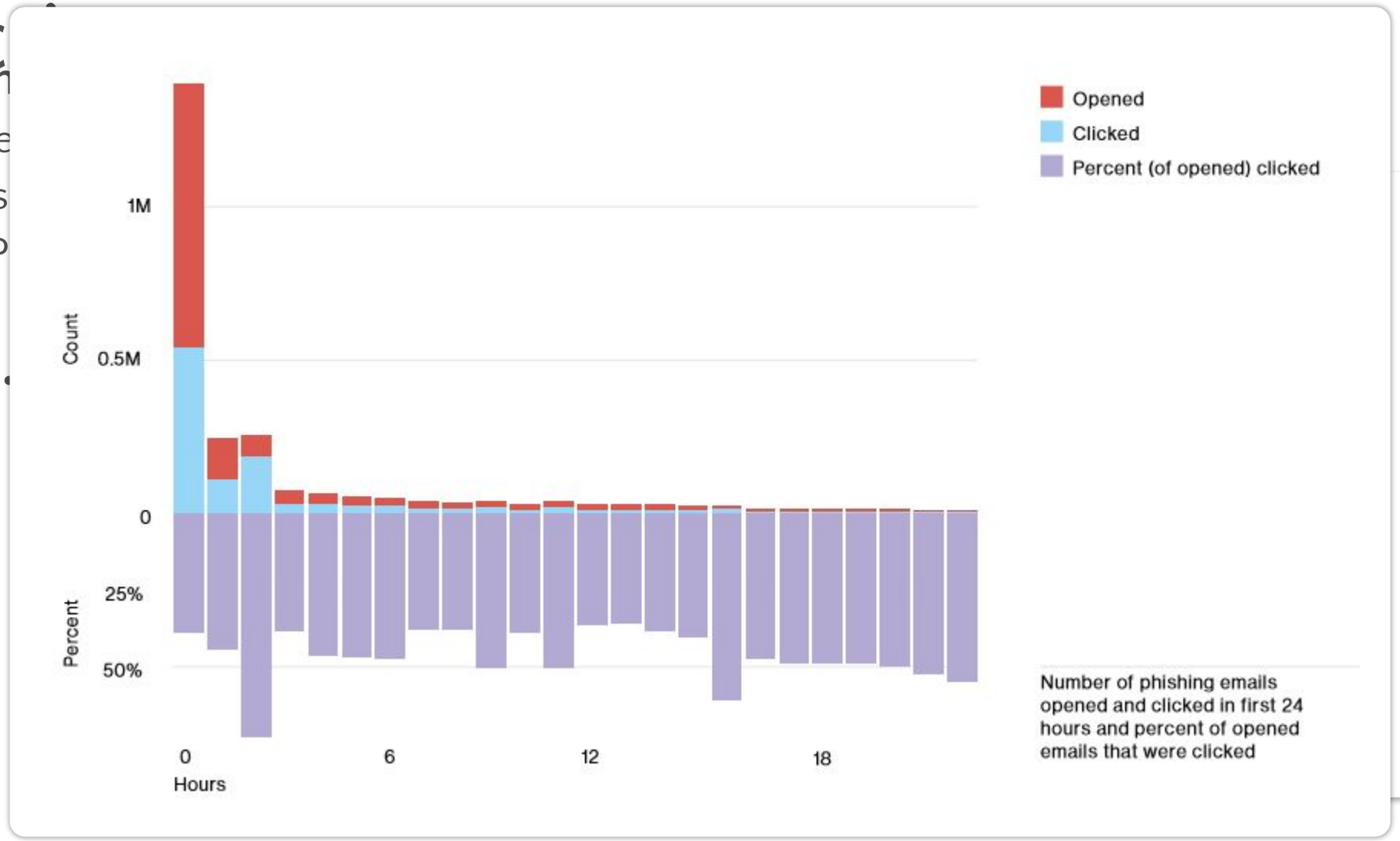
Schoolboard, from the Attacker's Perspec

June th

Email se

helpdes

with a P



attachment

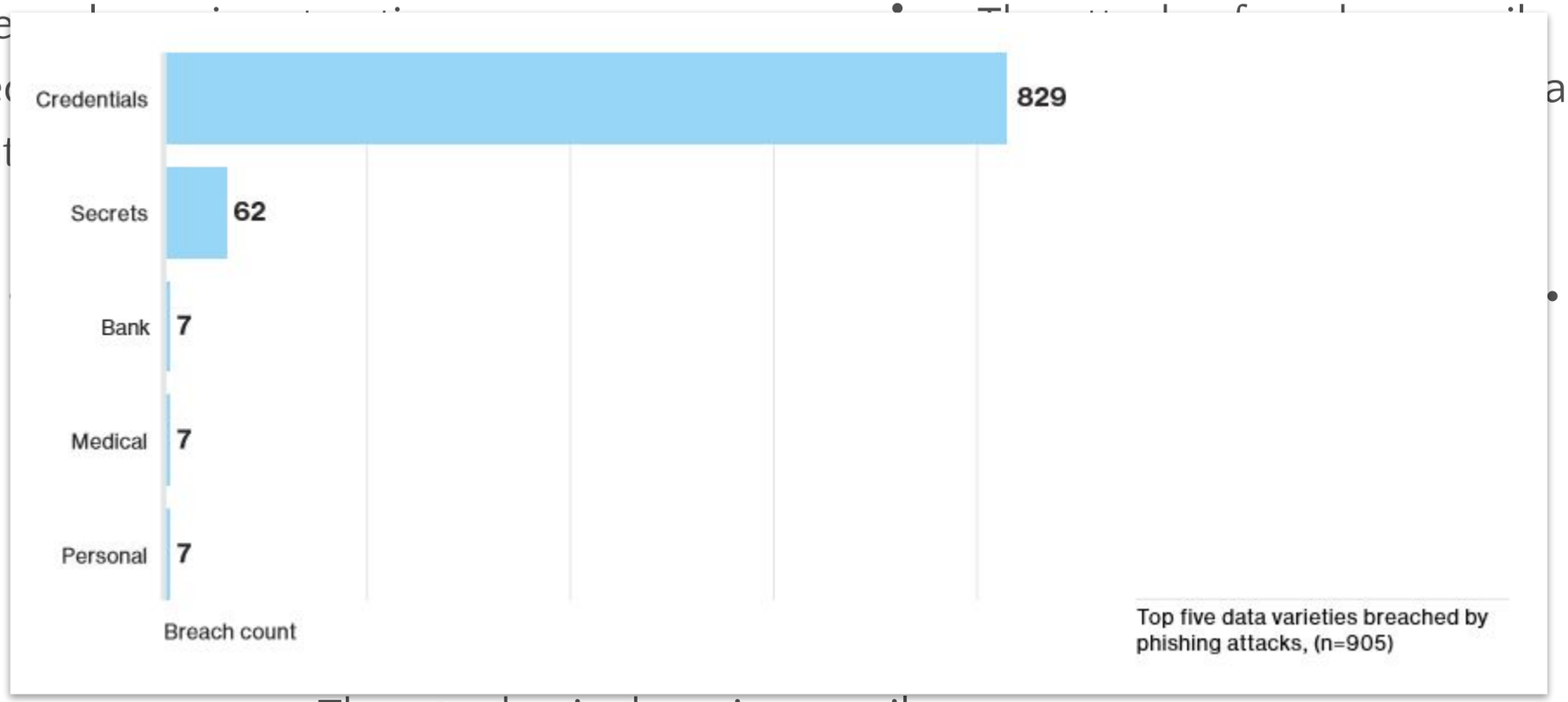
Schoolboard, from the Attacker's Perspective

June the 3rd + 6 minutes

The
cre
to it

June the 4th

ation



The attacker is dumping emails from the helpdesk users.

Schoolboard, from the Attacker's Perspective

June the 4th

The attacker takes remote control of one of the sleeping helpdesk computers and then accesses to PAY01

June the 4th

The attacker downloads the public documentation of the payroll application

June the 4th

The helpdesk user is an Administrator of the payroll application and more (Domain Admins member)

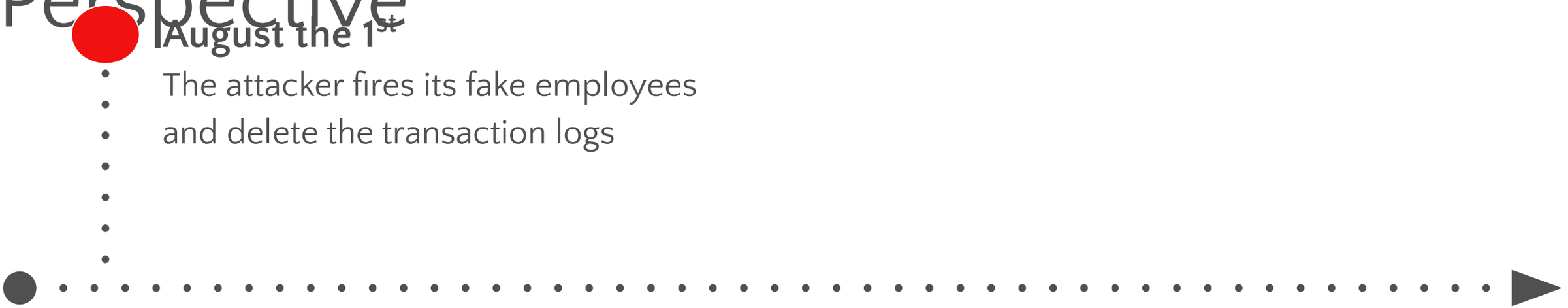
July the 1st

The attacker creates fake employees in the payroll system and assigns them foreign bank accounts

Schoolboard, from the Attacker's Perspective

August the 1st

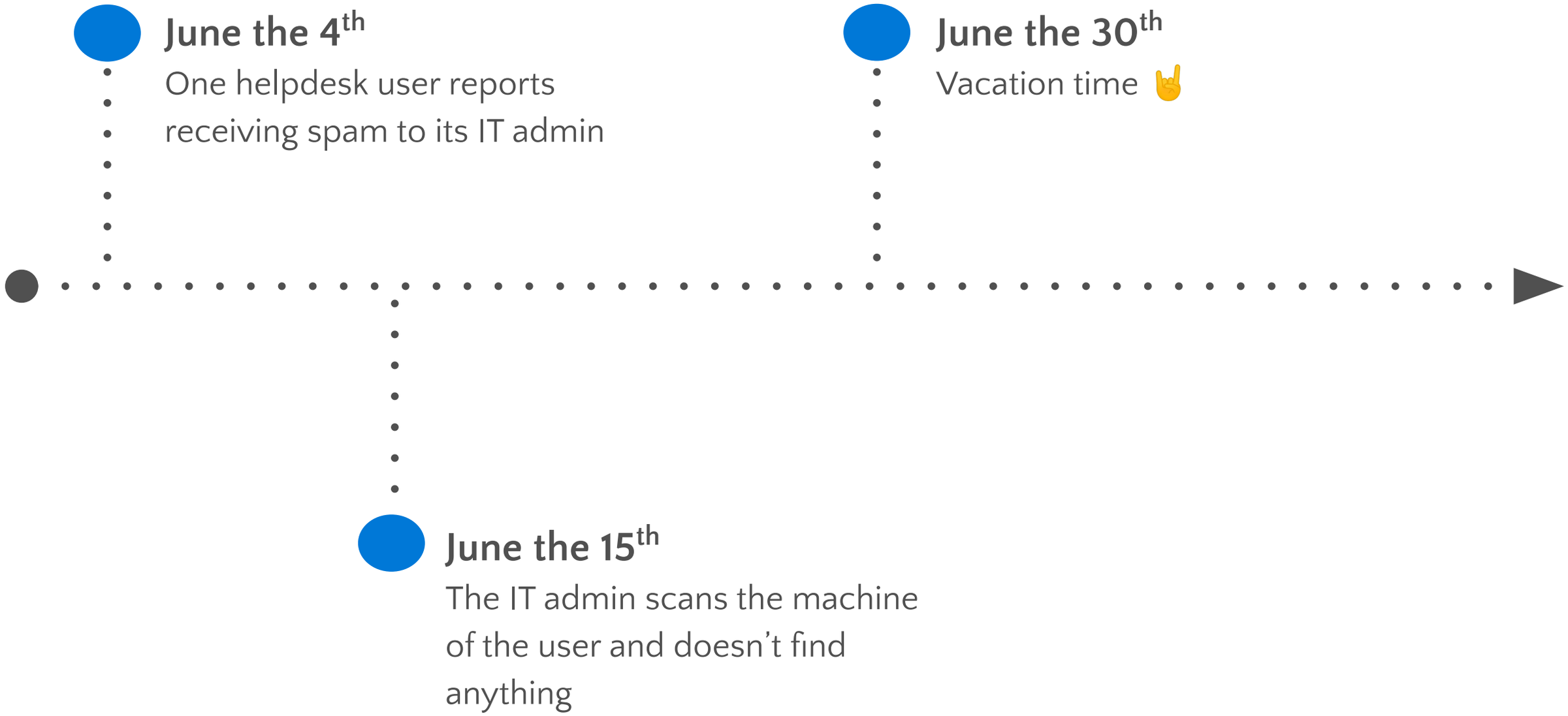
The attacker fires its fake employees
and delete the transaction logs



$140 K

Money embezzlement
½ of the yearly budget of the schoolboard
Tax payers' money

Schoolboard, from the Other Side



Schoolboard, from the Other Side

August the 15th
The bank calls the accountant to inform him of the recent unusual summer activities

August the 31st
Press release

81%

In 81% of breaches, the affected organization did not detect the breach themselves but were notified by others.

What went wrong?

- Spam/phishing detection
- Phishing awareness training
- Suspicious activities reporting process (Security Incident Management)
- No separation of privileged accounts
- Helpdesk accounts have too many privileges

Construction

4,000
Employees

$30 millions YR
Private funds

Construction, from the Attacker's Perspective

January the 3rd

A mobile server room disappears from a construction site

January the 5th

Most of the hardware is sold

A domain controller is identified

January the 6th

The NTDS.DIT database is cracked.

A majority of the passwords are discovered

Planning a targeted attack

This includes the passwords of privileged accounts

January the 7th

Review of the other stolen data, identified webmail and VPN endpoints

Construction, from the Attacker's Perspective

January the 10th

VPN connection made on behalf of CONSTRUCTION\Joe

January the 10th

From Joe's session, runas as Administrator and discovery of all connected assets

January the 10th to February the 15th

Extract all targeted data

Implement a shutdown script via GPO to extract credentials of the connected users and send them to a remote server

February the 16th

All assets are now a member of a botnet. Machines are waiting for instructions

Construction, from the Attacker's Perspective

March the 1st

Some identities are sold
The attacker prepares the field for a ransomware drop

March the 2nd

VSS is stopped on a majority of servers and backup software
Is configured to backup only OS

April the 1st

D-day for Ransomware activation
Use GPO to deploy the payload on every AD joined machine

April the 2nd

All enterprise data is encrypted

Construction, from the Attacker's Perspective

April the 14th

After 12 days of work without IT data, and because the most of the backups are too old, most of the ransoms are paid

$220K ransom

Some old data has been restored
The attacker is still present on the network

$2M business impact

Construction, from the Other Side

January the 6th

A construction site is back to work after the holiday break

Servers and laptops are reported stolen

January the 7th

The IT admins are not too worried as the file server has not a lot of data and laptops were old

January the 12th

New hardware is shipped

Security is reinforced

CCTV is implemented

Security guards patrol more often

Construction, from the Other Side

March the 15th

DBA are complaining about backups failing

April the 2nd

Users cannot access their personal data nor their corporate (server hosted) data

~200 days

Most of attacks go **undetected for around a year** (on average), leaving organizations vulnerable to ongoing loss and damage.

backups of critical servers in the meantime

this got resolved

What went wrong?

Physical protection

Procedures in case of theft

Inefficient monitoring

Energy

95,000 Employees

$5 billion

Private funds

Networks

Corporate

Closed network in production sites

Energy, from the Attacker's Perspective

March the 3rd

The attacker got a valid account from a previous hack

March the 7th

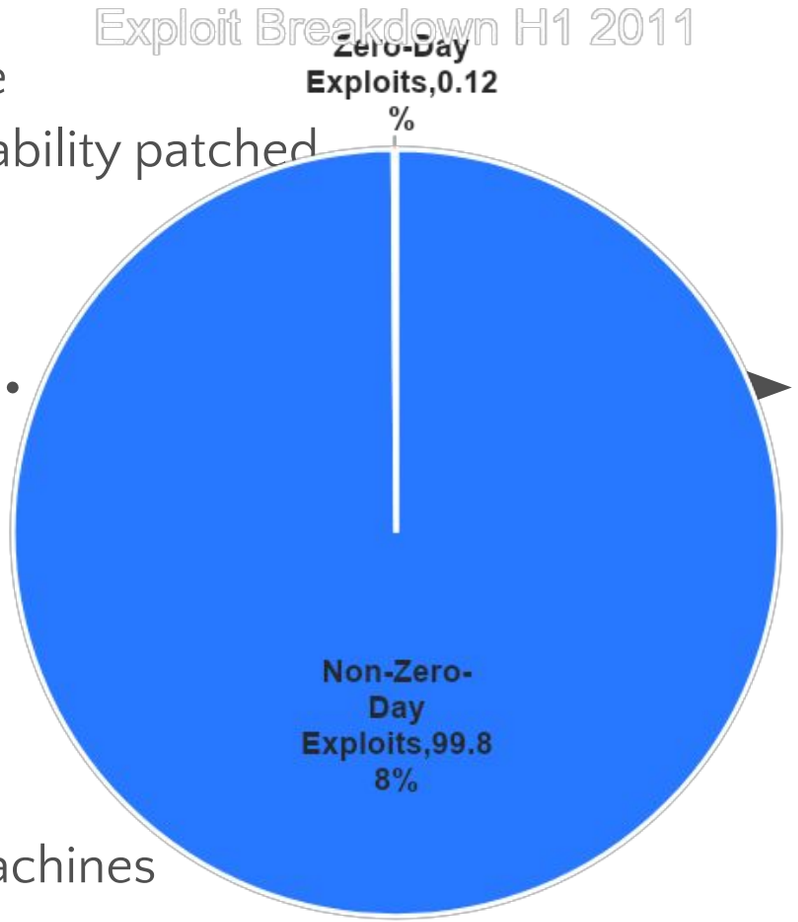
Drop new malware

It exploits a vulnerability patched last month

March the 5th

Lateral movemenent to more than 50 machines

Harvest new set of credentials



Energy, from the Attacker's Perspective

April the 5th

Giga bytes of data
are extracted
The attacker gets intel about
the ID used in the closed network

May the 1st

The attacker is creating service accounts
member of the Backup Operators group

April the 30th

The attacker is installing its own
VMs and deploy a Kali

May the 5th

Drop custom USB flash drives
with embedded cred around
the production staff

Energy, from the Attacker's Perspective

May the 7th

The production is down
in one critical site

May the 8th

Ransomware are
Corp and produc

$12k ransom

Some old data has been restored
The attacker is still present on the network

$35M fines

Failed to comply to security regulations

$90M loss market share

Energy, from the Other Side

April the 4th

AV team clean up malwares found
on several workstations
(systems are formatted)

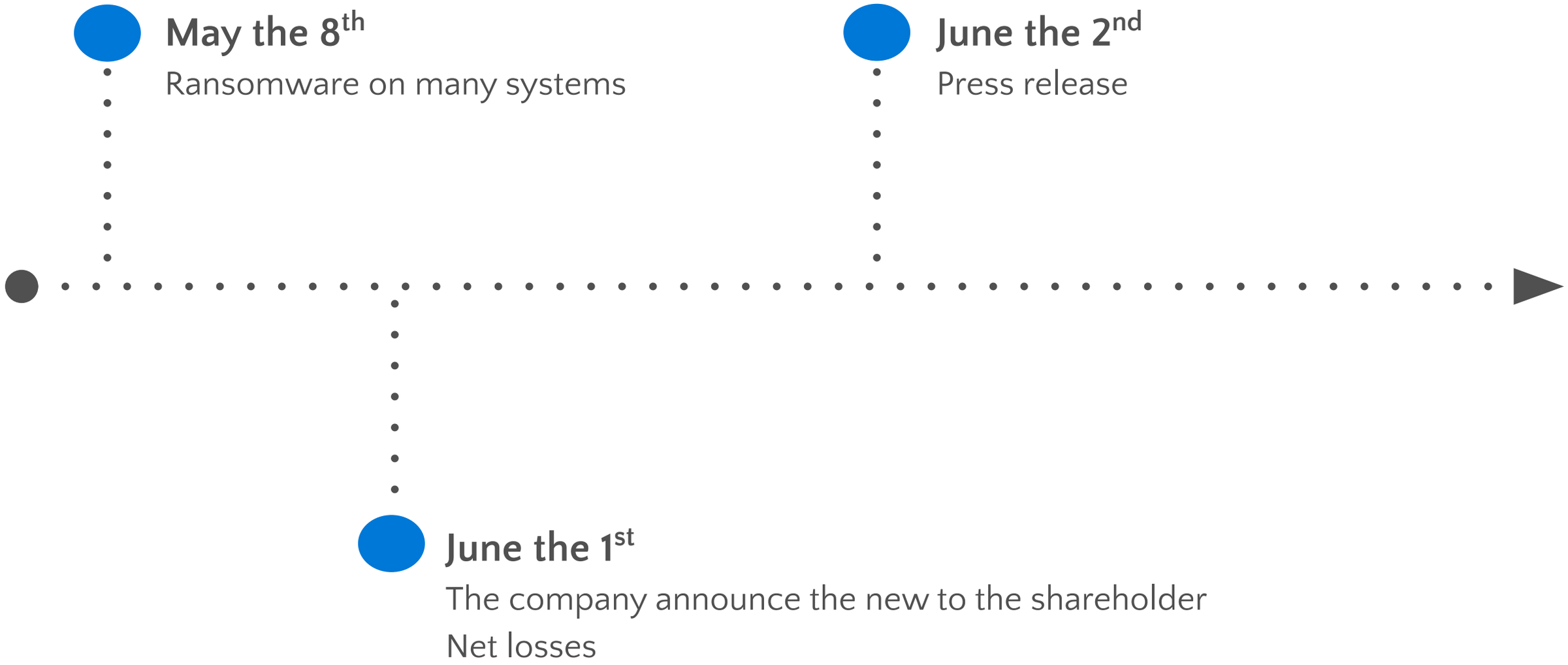
May the 6th

Network team detect abnormal
network activities. Delete suspicious VM
and change passwords of VM admins

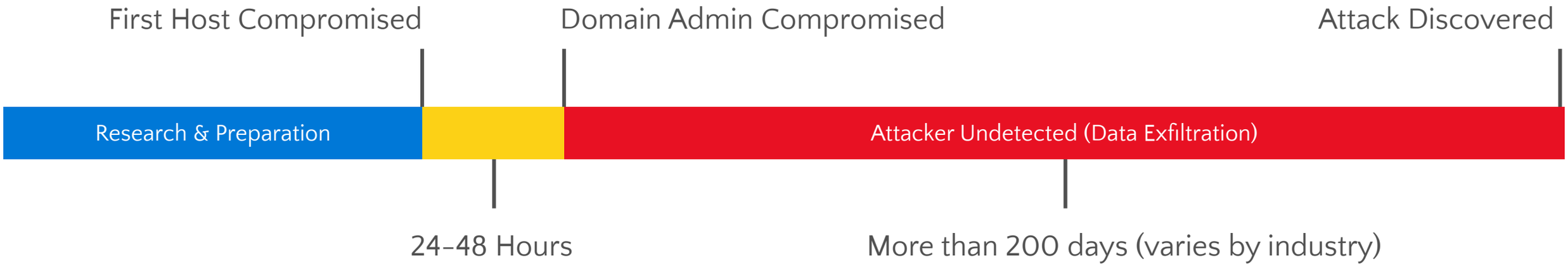
May the 7th

Major production outage
Production site down, no ETA

Energy, from the Other Side



Typical Attack Timeline & Observations



Attack Sophistication

Attack operators exploit any weakness

Target information on any device or service

Target AD & Identities

Active Directory controls access to business assets

Attackers commonly target AD and IT Admins

Attacks not detected

Current detection tools miss most attacks

You may be under attack (or compromised)

Response and Recovery

Response requires advanced expertise and tools

Expensive and challenging to successfully recover

Cost of an attack

The cost of these attacks to the global economy, and to an individual company, is significant. It is estimated that the total potential cost of cybercrime to the global economy is $500 billion. The average cost of a data breach to a company is estimated at $3.5 million. However, the cumulative impact as a result from damage to brand reputation, loss of confidential data, and intellectual property is just as, if not more, damaging.

(Source: CSIS-McAfee Report)

(Source: Ponemon Institute releases 2014 Cost of Data Breach)

Security Threat Landscape

Lesson 2: Securing the environment

Section: Basics

Hard Lessons…

The network is no longer the security perimeter (it hasn't been for some time)	Identity is the (new) security perimeter
Entry—we can't stop this from happening	People will be fooled, bribed, blackmailed, etc.
Eliminating human error isn't possible	Phishing works and will continue to do so
Insider-attacks are a big problem	Anomalous activity monitoring helps in detection; limit access through identity management & isolation
Compliance is very important	But compliance and security are not the same thing: **compliant != secure**
Prevention methods aren't always technical or architectural	Many will be operational and that will impose some level of additional operational friction—security has a price $$$

Windows Server **Security Posture**

1. Protect

Ongoing focus & innovation on preventative measures; block known attacks & known malware

2. Detect

Comprehensive monitoring tools to help you spot abnormalities and respond to attacks faster

3. Respond

Leading response and recovery technologies plus deep consulting expertise

4. Isolate

Isolate OS components & secrets; limit admin. privileges; rigorously measure host health

What do we need to secure and how?

Managed privileged identities

Secure the OS

Secure virtualization

Fundamentals of Information Security

The CIA Triad

Information Security Concepts and Fundamental Principles

- Confidentiality
- Integrity
- Availability

Fundamentals of Information Security

- The three pillars

Confidentiality

Data is not disclosed unless authorized

Cryptography

...

Integrity

Data has not been changed, destroyed, or lost

Digital Signatures

...

Availability

Data being accessible and usable upon demand

Redundant network

...

HIDDEN – More Information

References for Canada

- Annex 1 – Departmental IT Security Risk Management Activities: IT Security Risk Management: A Lifecycle Approach (mentioned all over the place in that order here)
https://www.cse-cst.gc.ca/en/node/265/html/24453
- Overview: IT Security Risk Management: A Lifecycle Approach
https://www.cse-cst.gc.ca/en/node/265/html/22814
- IT Security Risk Management: A Lifecycle Approach
https://www.cse-cst.gc.ca/en/publication/itsg-33

Fundamentals of Information Security

- Constraints

Non-repudiation

Assurance that the sender of the data is provided with the proof of delivery, and the recipient is provided with the proof of the sender's identity

Need to know

Need for access to information to complete a certain task

Principle of least privilege

Granting the minimum that the entity needs to do its work

Defense-in-Depth Modeling

- You want to make it…
  - Harder
  - Longer
  - More noisy

… for the attacker

- You want to be an unattractive target

Defense-in-Depth Modeling

Operating systems, hardening, patch management, HIDS

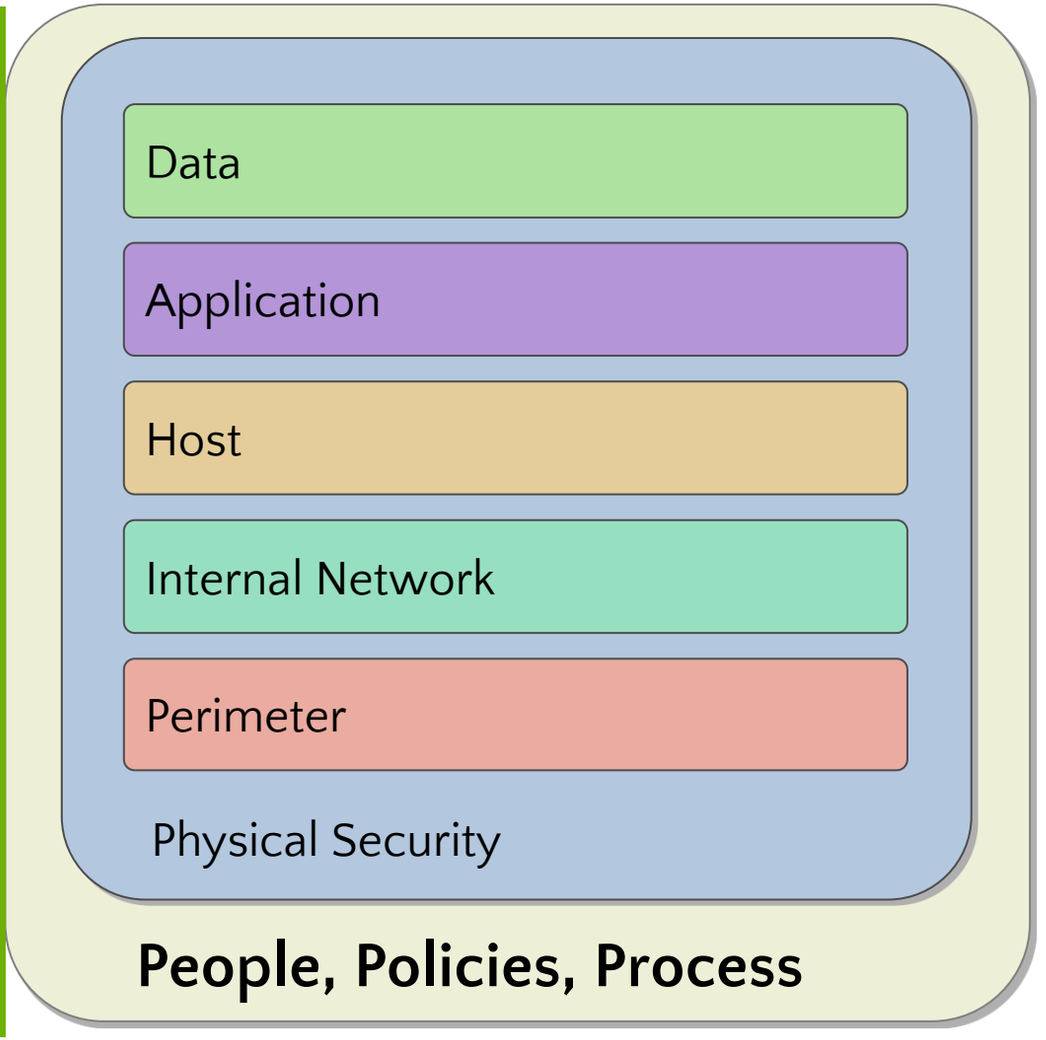
Firewalls, Network Access, Quarantine Control, NAP

ACL

Layers of Defense:

When talking about the various layers to protect, we want to consider a variety of attack vectors. Take a moment to review each layer as presented in the picture on the right. Consider where your organization might be vulnerable.

During this class, we will be discussing various ways you can harden your Microsoft infrastructure. However, you should always think about how the concepts we present here can be applied elsewhere within your environment.



Windows Desktop feature	Physical layer	Perimeter layer	Network layer
Trusted Platform Module	√		
BitLocker	√		
Encrypted File System	√		
VPN		√	
Network Access Protection		√	
Direct Access		√	
IPSec, Windows Firewall			√
Network Segmentation			√
Securing Wireless LANs			√

Windows Desktop feature	Host layer	Application layer	Data layer
Patch Management	√		
Antivirus, Windows Defender	√		
UAC, MIC, Session 0, EMET	√		
Host hardening, GPO, DCM		√	
IIS Hardening		√	
Secure Applications Development		√	
BitLocker, EFS			√
RMS			√
ACLs			√

Defense-in-Depth Modeling

- Strategic shift

From **perimeter security** …

Protect information
Establish security practices
Manage threats
Respond strongly

… to **assumed breach**

Risk Management

Key Concepts

- What is a **vulnerability**?
  - A flaw or weakness in a system's design, implementation, or operation and management.
- What is a **risk**?
  - The probability of a vulnerability being exploited in the current environment, leading to a degree of loss of confidentiality, integrity, or availability, of an asset

Basic Security Principles

- Security decisions are risk management decisions
  - Risk can never be reduced to zero
  - Prioritization and focus becomes important
- Assess Risk
  - Identify and prioritize risks to the business
- Conduct Decision Support
  - Identify and evaluate control solutions based on a defined cost-benefit analysis process
- Implement Controls
  - Deploy and operate control solutions to reduce risk to the business.
- Measure Effectiveness
  - Analyze the risk management process for effectiveness
  - Verify that controls are providing the expected degree of protection

Basic Security Principles:

How We Protect It

- Principle of Least Privilege (POLP)
  - Access varies based on minimum amount of privilege for the requirement
  - Access allowed only for required duration
- Reduce the Attack Surface
  - Lower attack surface directly reduces the probability of a successful attack
- Security Zones
  - Objects with similar security requirements are grouped
  - Similar security is then applied to the whole group
- Role-Based Security
  - Security applied based on job or task requirements
  - Based on the Principle of Least Privilege

The 10 Immutable Laws of Security Administration:

- Nobody believes that anything bad can happen to them, until it does
- Security only works if the secure way also happens to be the easy way
- If you do not keep up with security fixes, your network will not be yours for long
- It does not do much good to install security fixes on a computer that was never secured to begin with.
- Eternal vigilance is the price of security
- There is really someone out there trying to guess your passwords
- The most secure network is a well-administered one
- The difficulty of defending a network is directly proportional to its complexity
- Security is not about risk avoidance; it is about risk management
- Technology is not a panacea
- 10 Immutable Laws of Security Administration: http://technet.microsoft.com/en-us/library/cc722488.aspx

The 10 Immutable Laws of Security Administration:

- If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.
- If a bad guy can alter the operating system on your computer, it's not your computer anymore.
- If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
- If you allow a bad guy to run active content in your website, it's not your website any more.
- Weak passwords trump strong security.
- A computer is only as secure as the administrator is trustworthy.
- Encrypted data is only as secure as its decryption key.
- An out-of-date antimalware scanner is only marginally better than no scanner at all.
- Absolute anonymity isn't practically achievable, online or offline.
- Technology is not a panacea.

Sample AD assets

- Domain Controllers
- Active Directory Backups
- Administrative Accounts and Groups
- Identities and attributes
- Group Policies
- Administrative Workstations
- Administrative Delegations
- Administration Team

Vulnerabilities

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

- Examples:
  - Physical
    - Unlocked doors
    - Unguarded access to computing facilities
    - Insufficient fire suppression systems
  - Natural
    - Facility located on a fault line
    - Facility located in a flood zone
    - Facility located in an avalanche area

Vulnerabilities (continued)

- Hardware
  - Outdated firmware
  - Systems not physically secured
  - Misconfigured systems
- Software
  - Out-of-date antivirus software
  - Missing patches
  - Poorly written applications

Vulnerabilities (continued)

- Communications
  - Unencrypted network protocols
  - Connections to multiple networks
  - No filtering between network segments
- Human
  - Poorly defined procedures
  - Stolen credentials
- Media
  - Electrical interference

Vulnerabilities (continued)

- Poorly written or secured scripts
- Weak admin accounts security
- Poorly secured AD objects
- Unnecessary software and services installed on domain controllers
- Lack of Security Audit and Monitoring

Security Threat Landscape

Lesson 2: Securing the environment

Section: Help protect credentials and privileged access

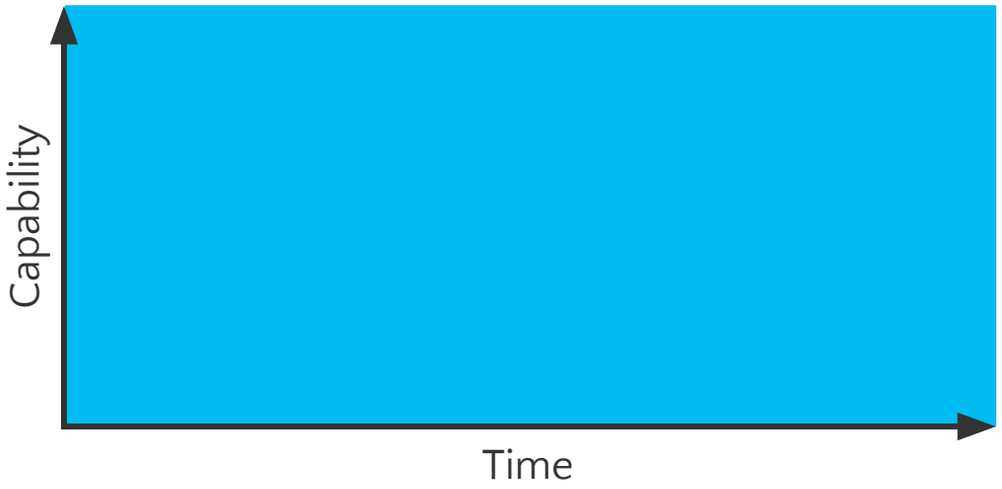
Challenges in Protecting Credentials

Social engineering leads to credential theft

Most attacks involve gathering credentials (Pass-the-Hash attacks)

Administrative credentials typically provide unnecessary extra rights for unlimited time

Typical administrator



Helping Protect Privileged Credentials

Just Enough Administration (JEA)

limits administrative privileges to the bare-minimum required set of actions (limited in space)

Just in Time Administration (JIT)

provides privileged access upon request through a workflow that is audited and limited in time

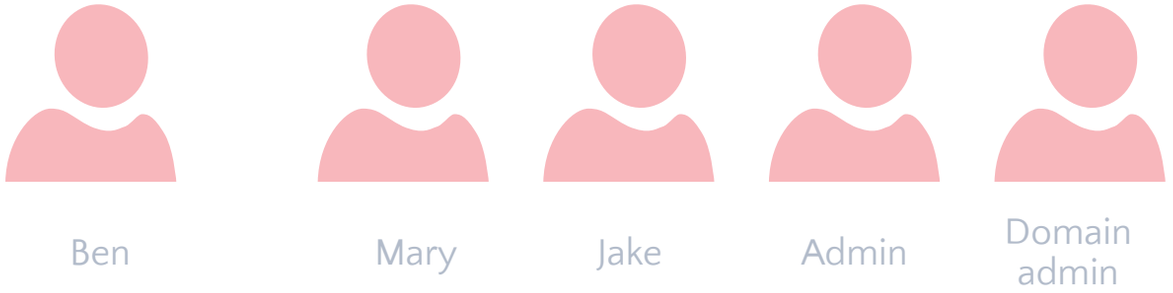
JEA and **JIT** administration

Helping Protect Privileged Credentials

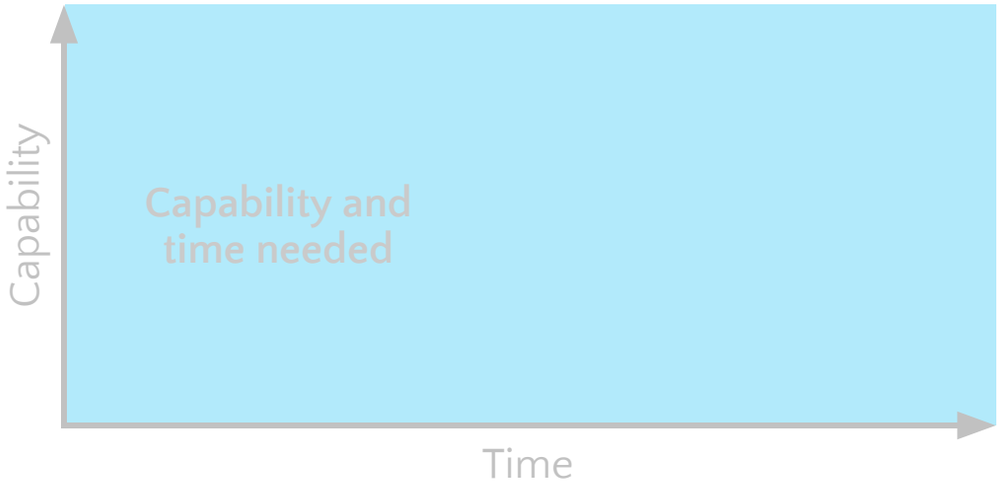
Just Enough Administration (JEA) limits administrative privileges to the bare-minimum required set of actions (limited in space)

Just in Time Administration (JIT) provides privileged access upon request through a workflow that is audited and limited in time

Credential Guard prevents **Pass the Hash** and **Pass the Ticket** attacks by protecting stored credentials and credential artifacts using Virtualization based Security (VBS)



JEA and **JIT** administration



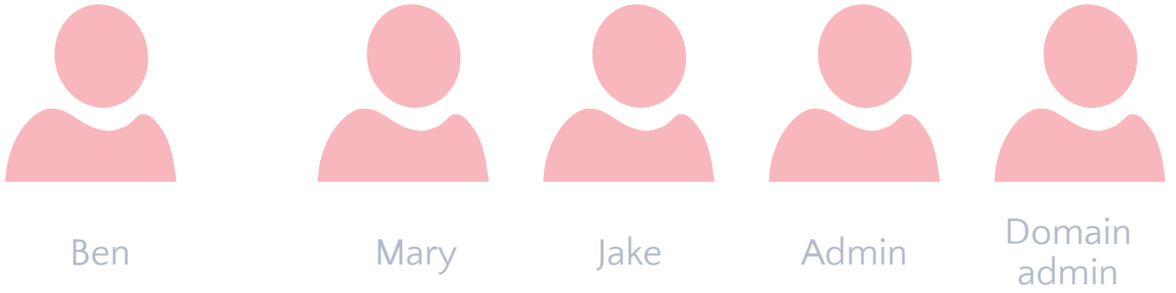
Helping Protect Privileged Credentials

Just Enough Administration (JEA) limits administrative privileges to the bare-minimum required set of actions (limited in space)

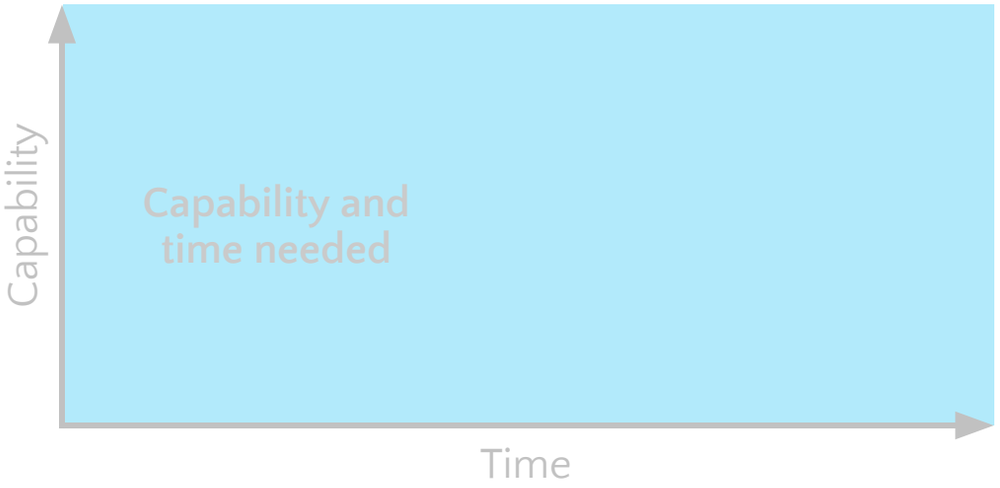
Just in Time Administration (JIT) provides privileged access upon request through a workflow that is audited and limited in time

Credential Guard prevents **Pass the Hash** and **Pass the Ticket** attacks by protecting stored credentials and credential artifacts using Virtualization based Security (VBS)

Remote Credential Guard works in conjunction with Credential Guard for RDP sessions providing SSO over RDP while eliminating the need for credentials to be passed to the host



JEA and **JIT** administration



Security Threat Landscape

Lesson 2: Securing the environment

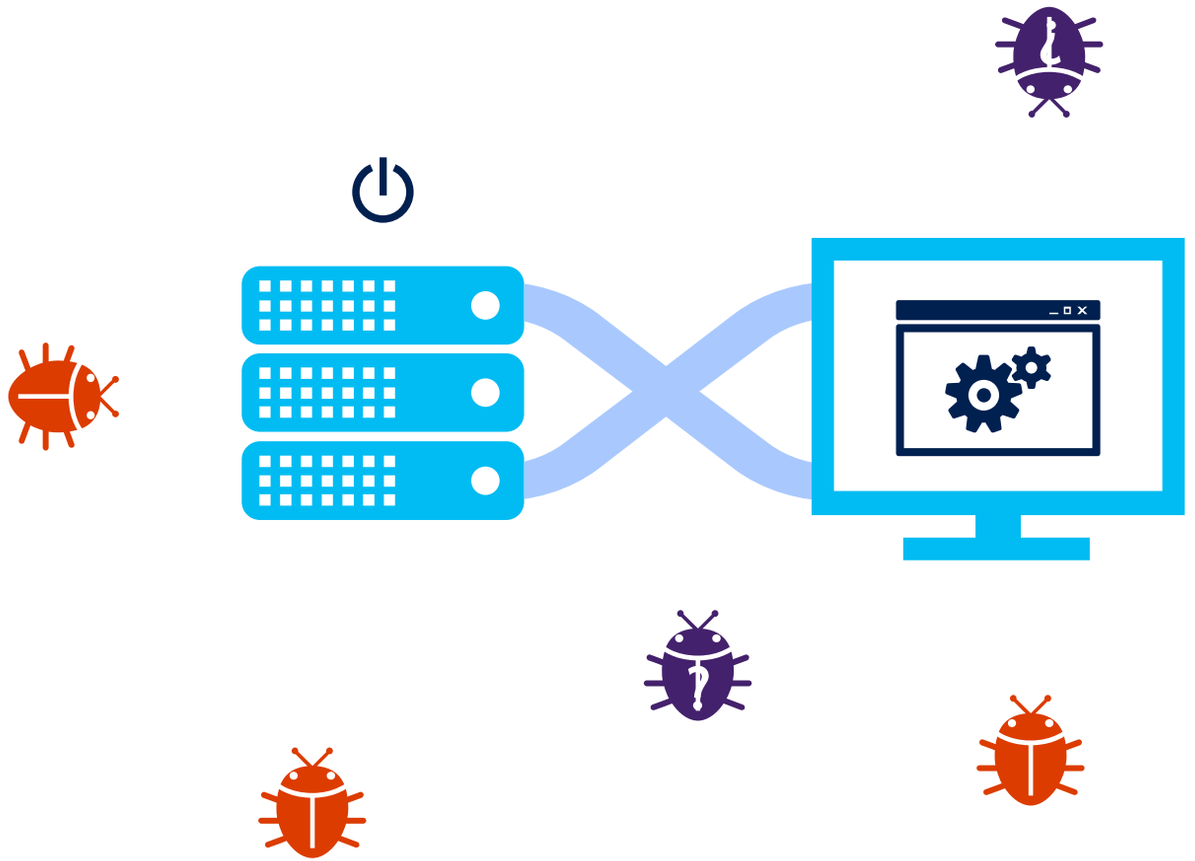
Section: Help protect applications and data in any cloud

Challenges Protecting the OS and Applications

New exploits can attack the OS boot-path all the way up through applications operations

Known and unknown threats need to be blocked without impacting legitimate workloads

Security Information and Event Management (SIEM) systems are only as intelligent as the information provided from the OS



Helping Protect OS and Applications

Device Guard

Ensure that only permitted binaries can be executed from the moment the OS is booted.

Windows Defender

Actively protects from known malware without impacting workloads.

Control Flow Guard

Protects against unknown vulnerabilities by helping prevent memory corruption attacks.

Enhanced Logs

Log new audit events to better detect malicious behavior by providing more detailed information to security operation centers

Security Threat Landscape

Lesson 2: Securing the environment

Section: Help protect the virtualization fabric

Help Protect the Virtualization Fabric

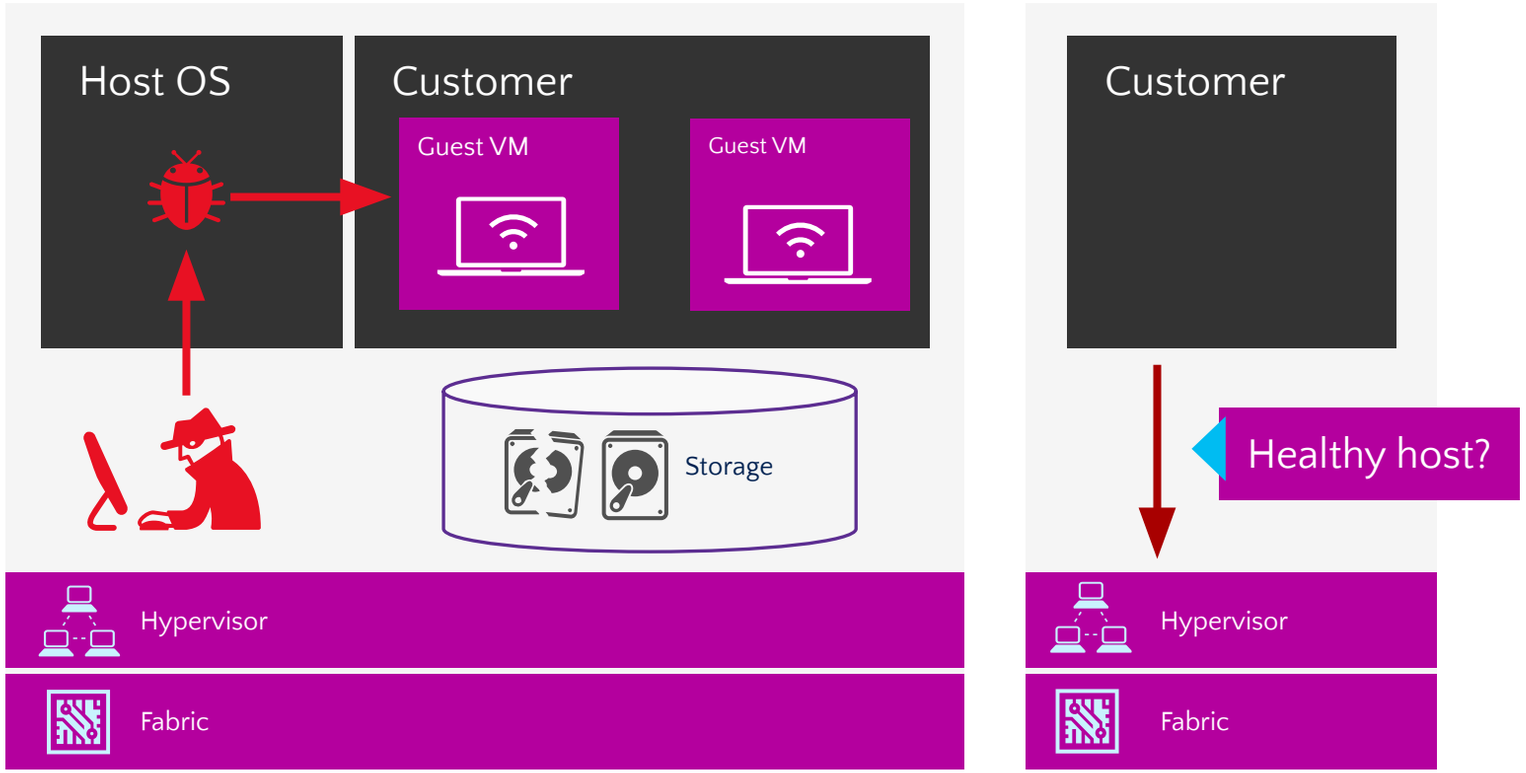
Challenges Protecting Virtual Machines

Any compromised or malicious fabric administrators can access guest virtual machines.

Health of hosts not taken into account before running VMs.

Tenant's VMs are exposed to storage and network attacks.

Virtual machines can't take advantage of hardware-rooted security capabilities such as TPMs.



Helping Protect Virtual Machines

Shielded Virtual Machines

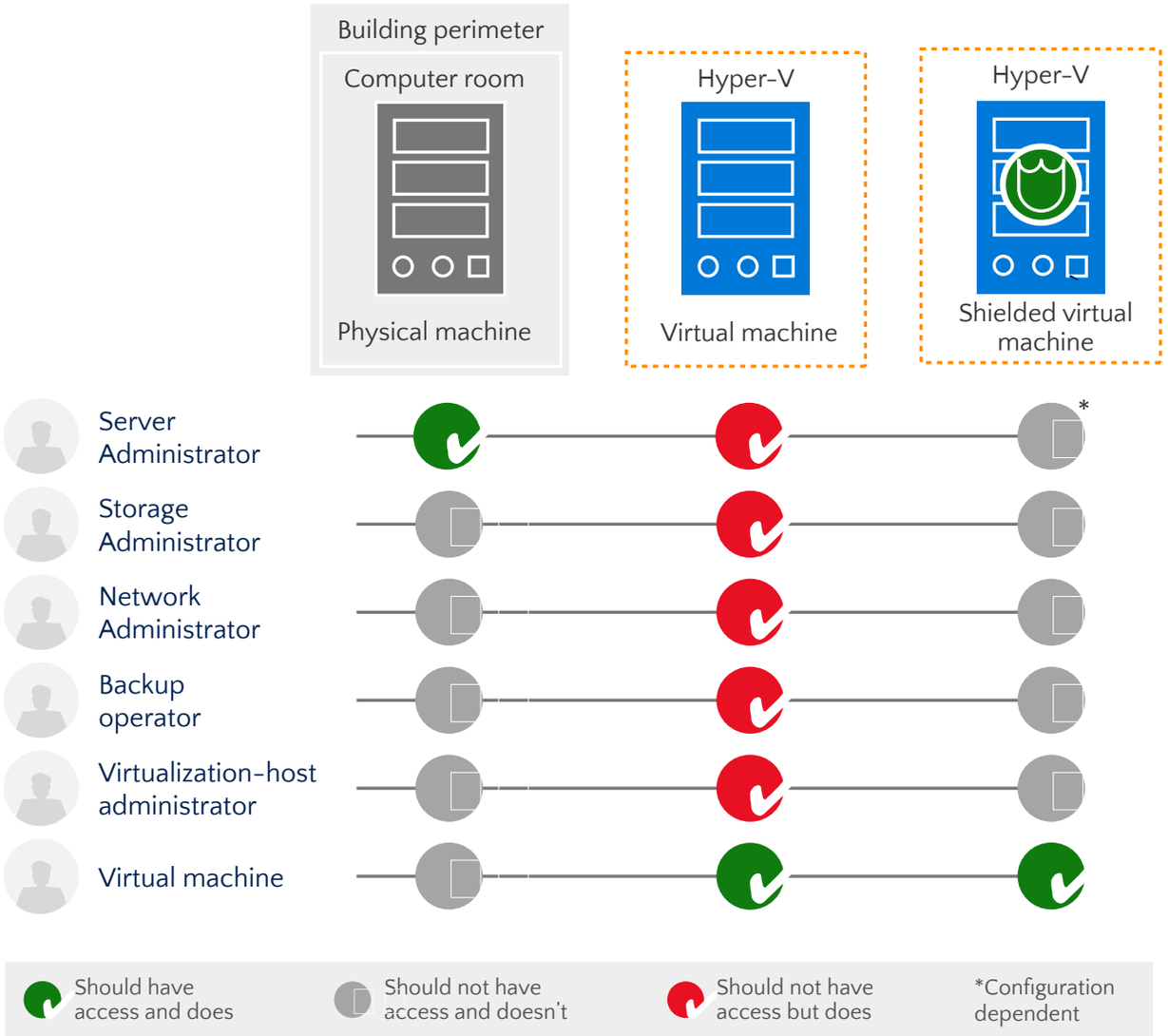
Use BitLocker to encrypt the disk and state of virtual machines protecting secrets from compromised admins and malware.

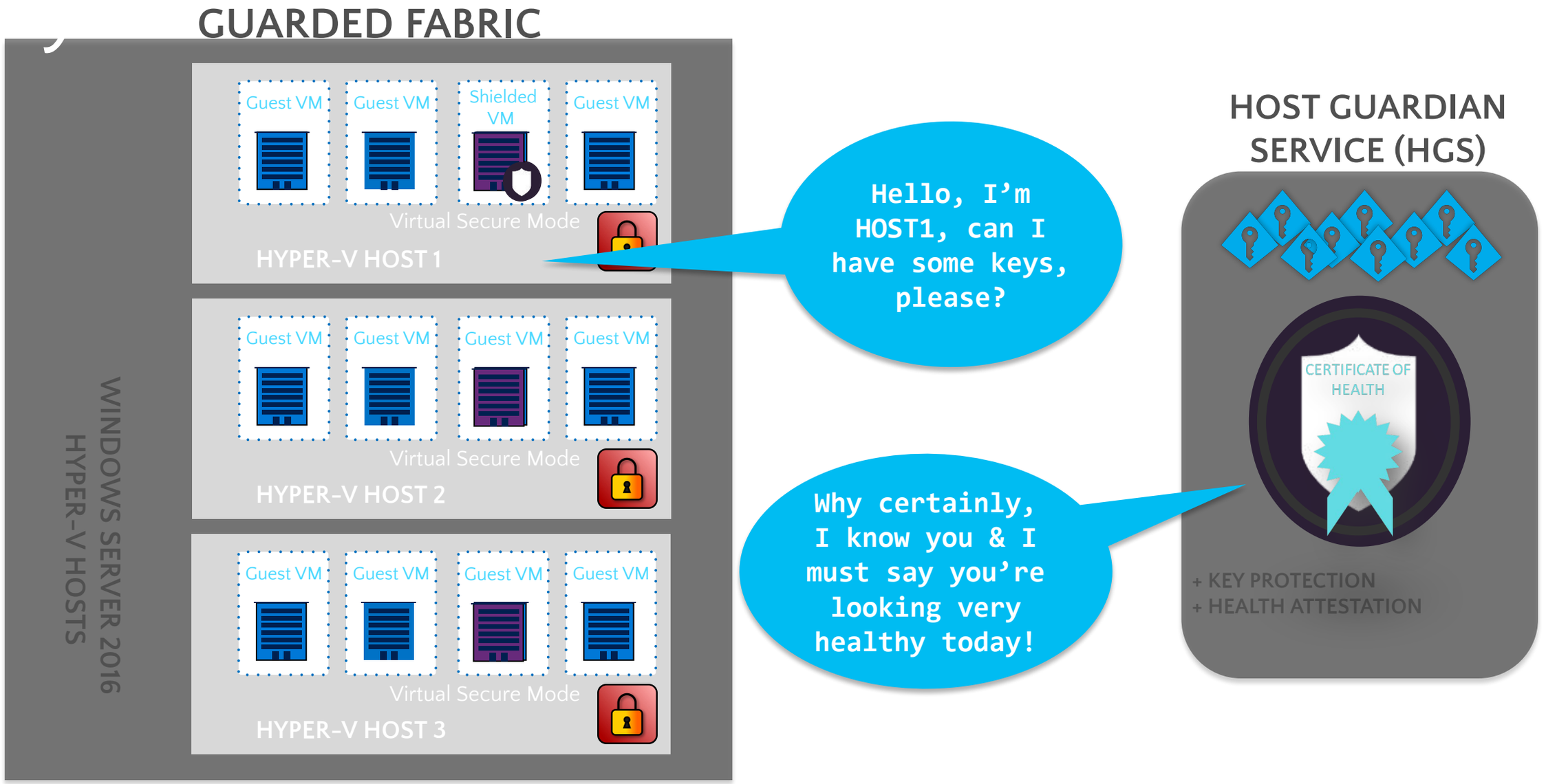
Host Guardian Service

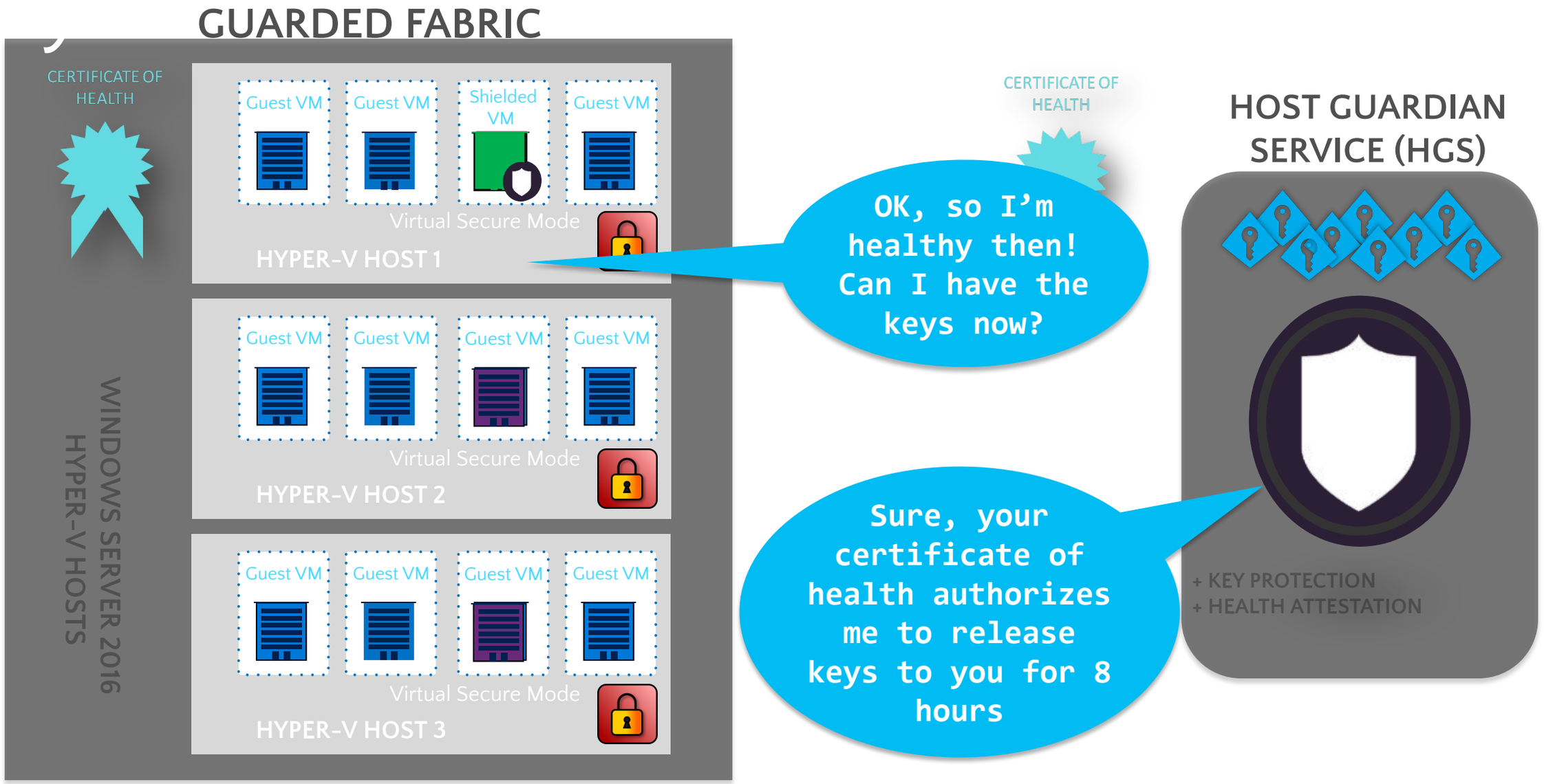
Attests to host health releasing the keys required to boot or migrate a Shielded VM only to healthy hosts.

Generation 2 VMs

Supports virtualized equivalents of hardware security technologies (e.g., TPMs) enabling BitLocker encryption for Shielded Virtual Machines.




GUARDED FABRIC
Guest VM
Guest VM
Shielded VM
Guest VM
Virtual Secure Mode
HYPER-V HOST 1
Guest VM
Guest VM
Guest VM
Guest VM
Virtual Secure Mode
HYPER-V HOST 2
Guest VM
Guest VM
Guest VM
Guest VM
Virtual Secure Mode
HYPER-V HOST 3
WINDOWS SERVER 2016
HYPER-V HOSTS
Hello, I'm HOST1, can I have some keys, please?
Why certainly, I know you & I must say you're looking very healthy today!
HOST GUARDIAN SERVICE (HGS)
CERTIFICATE OF HEALTH
+ KEY PROTECTION
+ HEALTH ATTESTATION


GUARDED FABRIC
CERTIFICATE OF HEALTH
Guest VM
Guest VM
Shielded VM
Guest VM
Virtual Secure Mode
HYPER-V HOST 1
Guest VM
Guest VM
Guest VM
Guest VM
Virtual Secure Mode
HYPER-V HOST 2
Guest VM
Guest VM
Guest VM
Guest VM
Virtual Secure Mode
HYPER-V HOST 3
WINDOWS SERVER 2016
HYPER-V HOSTS
CERTIFICATE OF HEALTH
OK, so I'm healthy then! Can I have the keys now?
Sure, your certificate of health authorizes me to release keys to you for 8 hours
HOST GUARDIAN SERVICE (HGS)
+ KEY PROTECTION
+ HEALTH ATTESTATION

> Shielded Virtual Machines remove a hosting obstacle and are a huge competitive differentiator. No one but Microsoft has this technology now.

Philip Moss
Chief Product Officer
Acuutech

Security Threat Landscape

Lesson 2: Securing the environment

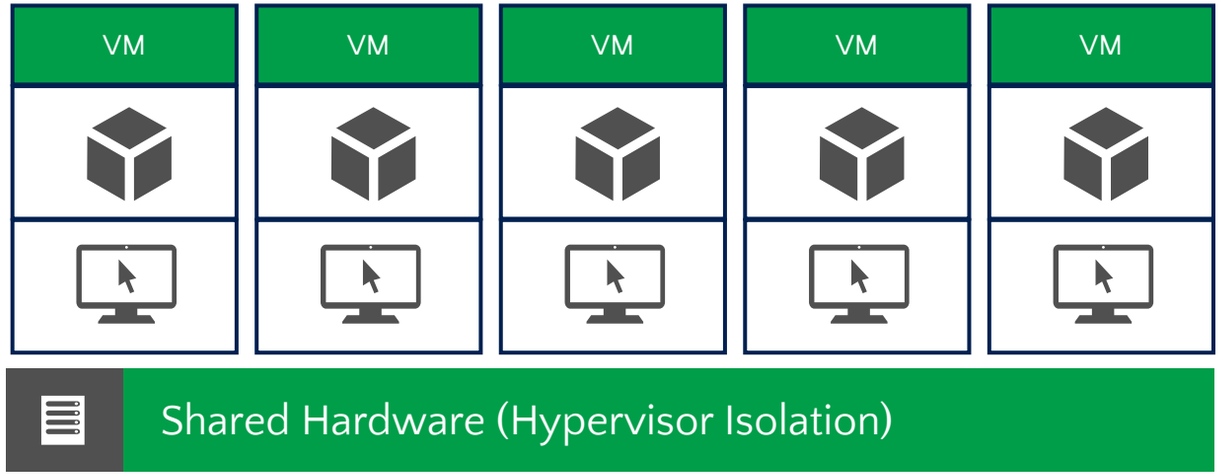
Section: Protect with just enough OS

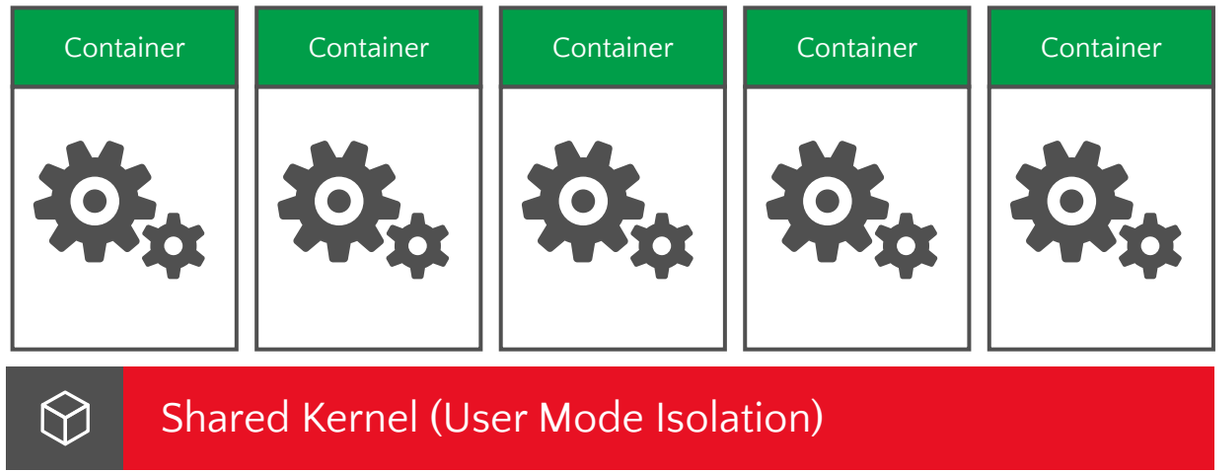
Challenges in Protecting New Apps

Developers are protecting by making use of packaging and deployment tools such as containers.

Containers share the same kernel which limits isolation and exposes compliance and regulatory risks.

Reduce the risk by providing only the components required by application to run.





Windows Server 2016 Approach

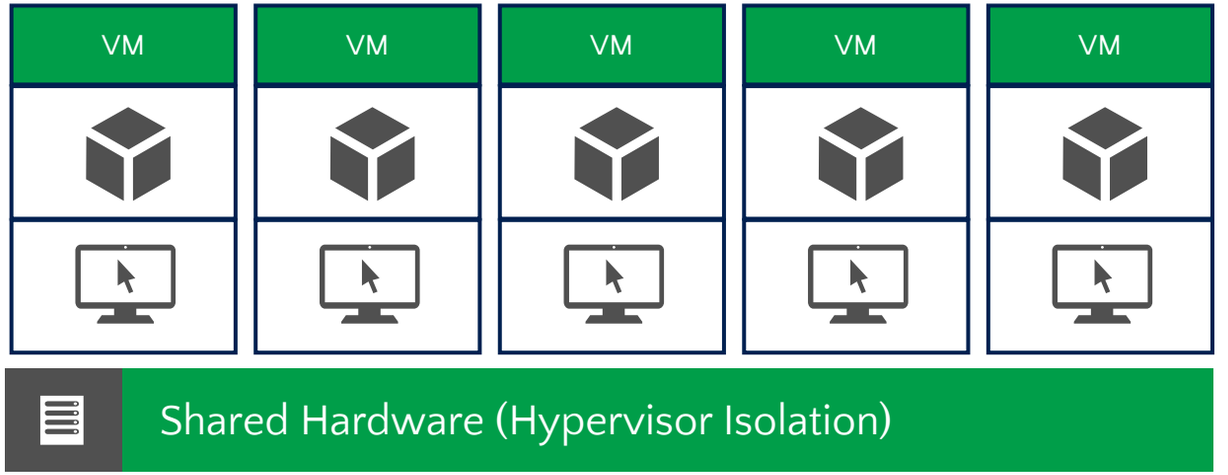
Hyper-V containers

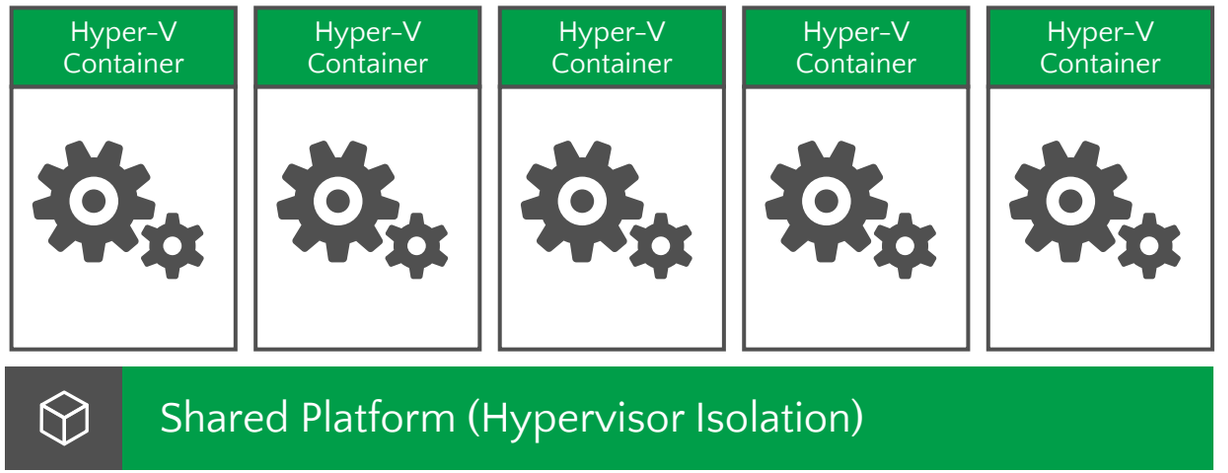
Provide hypervisor isolation for each container with no additional coding requirements.

Helps align with regulatory requirements for PCI and PII data.

Nano Server

Reduce the attack surface by deploying a minimal “just enough” server footprint.





Security Threat Landscape

Lesson 2: Securing the environment

Section: Windows Server 2016 security summary

Windows Server 2016 Security Summary

Virtualization Fabric

Protecting virtual machines

Shielded VMs (Server 2012, 2016 guests)

Virtual TPM for Generation 2 VMs

Guarded fabric attesting to host health

Secure boot for Windows and Linux

Hyper-V platform

Nano based Hyper-V host

Virtualization-based security

Distributed networking firewall

Secure containers

Hyper-V containers

Containers hosted in a Shielded VM

Infrastructure and applications

Privileged identity

Credential Guard

Remote Credential Guard

Just In Time administration

Just Enough administration

Threat resistance

Control Flow Guard

Device Guard

Built in anti-malware

Threat detection

Enhanced threat detection

DO NOT REMOVE: this is a hidden slide for notes purposes

Knowledge Check

- Question #1: What is the new security perimeter?
- Question #2: What are the four option we discussed that are used to protect against credential theft?
- Question #3: Why is a shielded-VM more secure then a regular VM?