RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO2-T08

Using the Cloud to Secure Versus Securing the Cloud

Tom Corn

SVP/GM Security Products
VMware
@therealtomcorn

an Ounce of Prevention
is worth a Pound of Cure

THE

Pennſylvania GAZETTE.

Protection of Towns from Fire

February 4, 1735

Being old and lame of my Hands, and thereby uncapable of assisting my Fellow Citizens, when their Houses are on Fire; I must beg them to take in good Part the following Hints on the Subject of Fires.

In the first Place, as an Ounce of Prevention is worth a Pound of Cure, I would advise 'em to take Care how they suffer living Brands-ends, or Coals in a full Shovel, to be carried out of one Room into anot
pan shut; for Sc
Appearance till
you may be forc
and hazard you

And now we tal
to the Act for p
Coopers Shops,
Houses in the p
testable Practic
Fire Place, whic
Turpentine, sta
Brand shall rou

Once more; if Chimneys were more frequently and more carefully clean'd, some Fires might thereby be prevented. I have known foul Chimneys burn most furiously a few Days after they were swept: People in Confidence that they are clean, making large Fires. Every Body among us is allow'd to sweep Chimneys, that please to undertake that Business; and if a Chimney fires thro' fault of the Sweeper, the Owner pays the Fine, and the Sweeper goes free. This Thing is not right. Those who undertake Sweeping of Chimneys, and employ Servants for that Purpose, ought to be licensed by the Mayor; and if any Chimney fires and flames out 15 Days after Sweeping, the Fine should be paid by the Sweeper; for it is his Fault.

We have at present got Engines enough in the Town, but I question, whether in many Parts of the Town, Water enough can be had to keep them going for half an Hour together. It seems to me some Publick Pumps are wanting; but that I submit to better Judgments.

As to our Conduct in the Affair of Extinguishing Fires, tho' we

obedience, to these Officers in any, at such Times, is punished by a Fine of 40s. or Ten Days Imprisonment. These Officers, with the Men belonging to the Engine, at their Quarterly Meetings, discourse of Fires, of the Faults committed at some, the good Management in some Cases at others, and thus communicating their Thoughts and Experience they grow wise in the Thing, and know how to command and to execute in the best manner upon

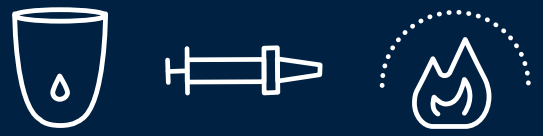
Manner of the new Buildings in London, and as Mr. Turner's House in Front-Street, or Mr. Nichols's in Chesnut-Street,3 are built; which I conceive would tend considerably to their Preservation.

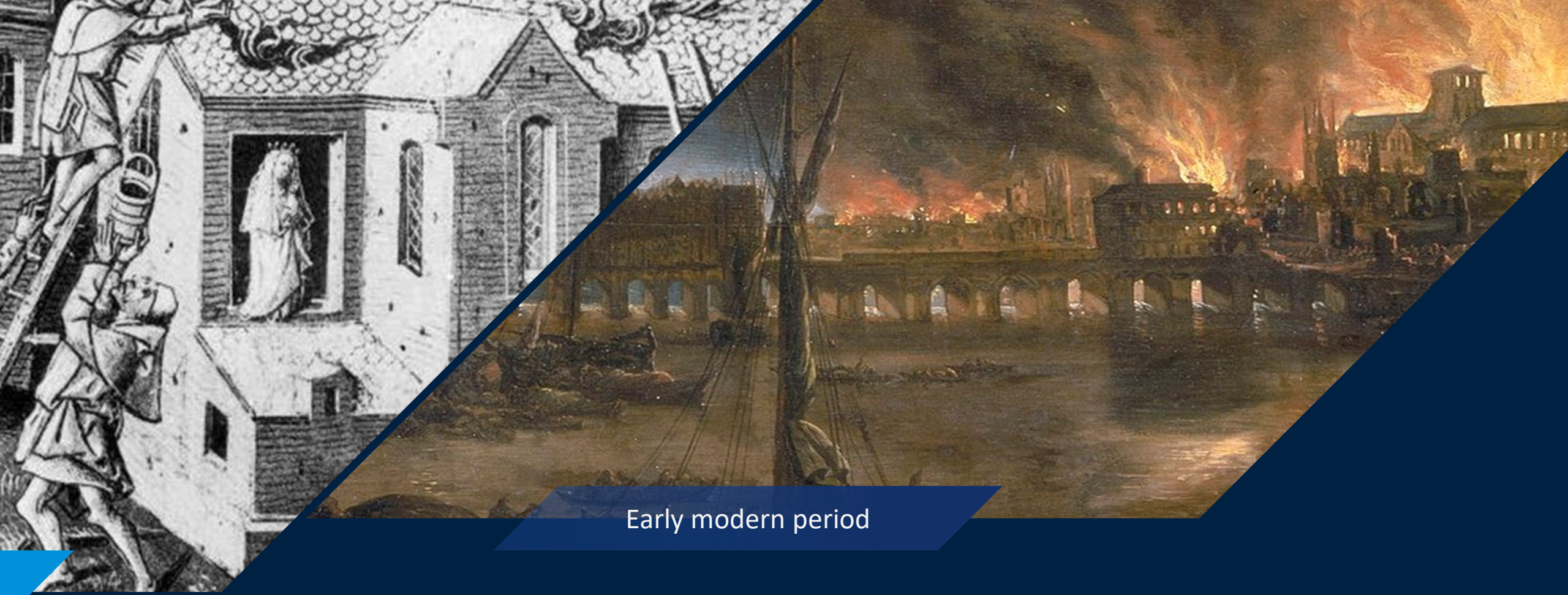
Let others communicate their Thoughts as freely as I have done mine, and perhaps something useful may be drawn from the Whole.

In the first Place, as an Ounce of Prevention is worth a Pound of Cure, I would advise 'em to take care how they suffer living Coals in …

Roman period

Medieval period





Early modern period

Innovation focused on reacting to fires

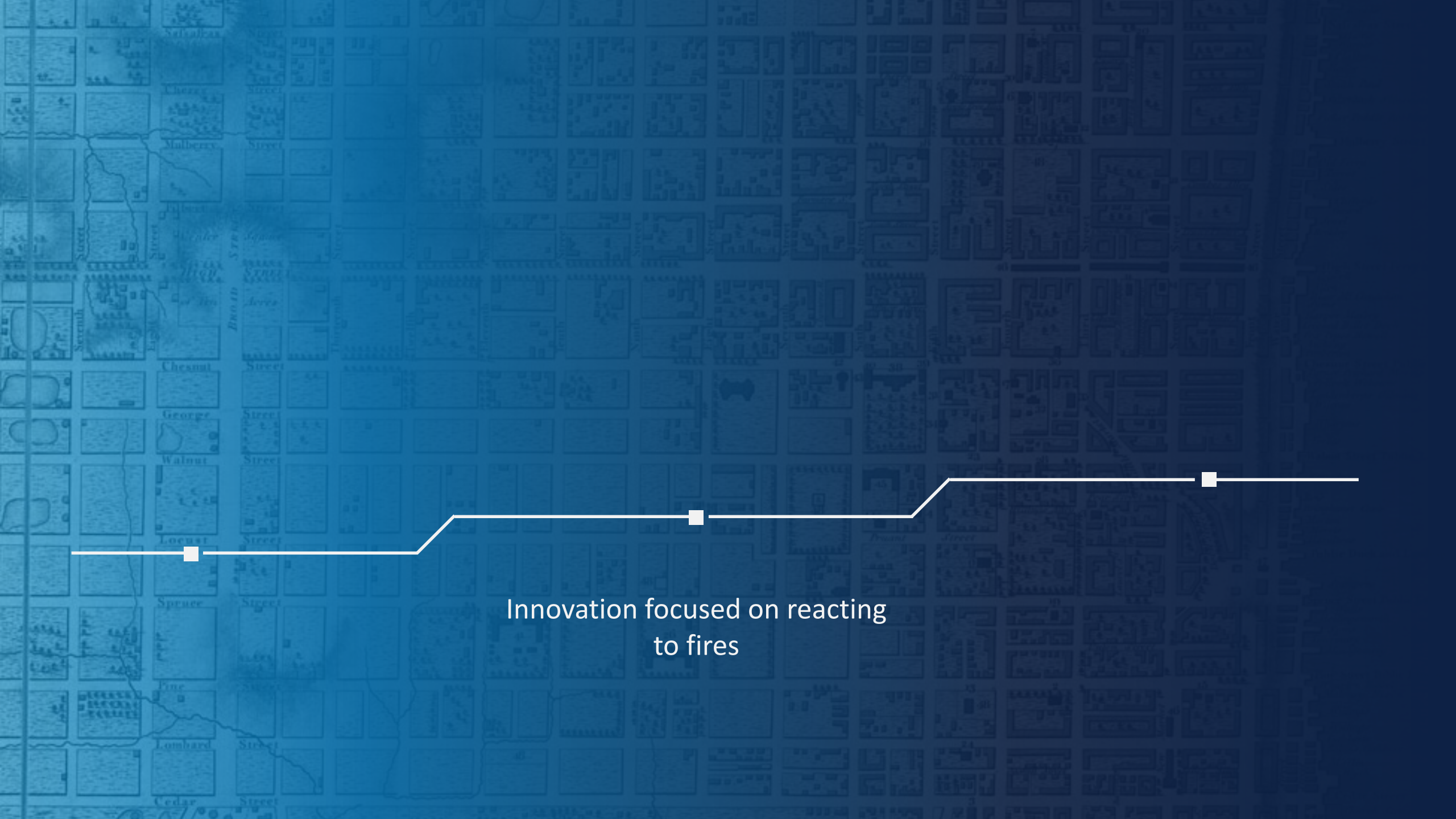

Escalating cost of fires
Innovation focused on reacting to fires

Philadelphia

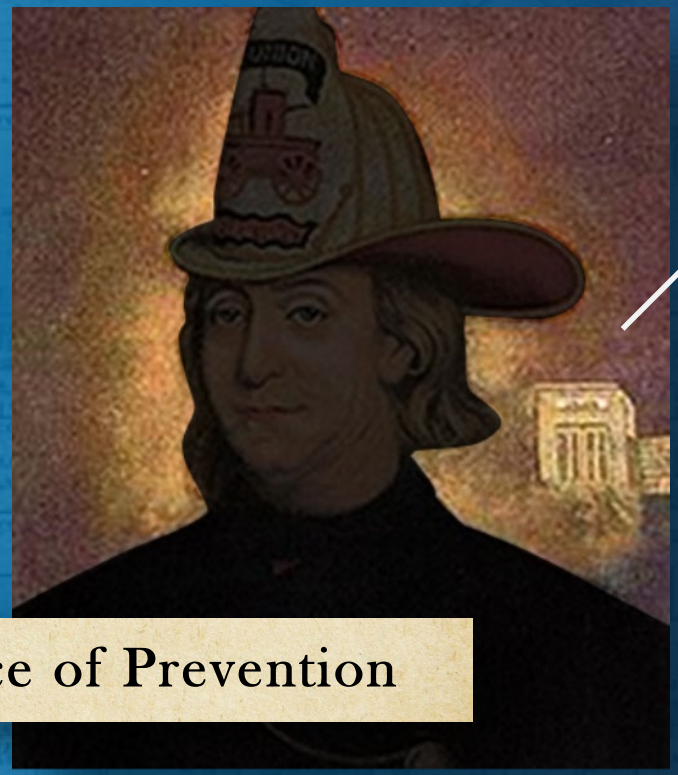
18TH CENTURY

vmware

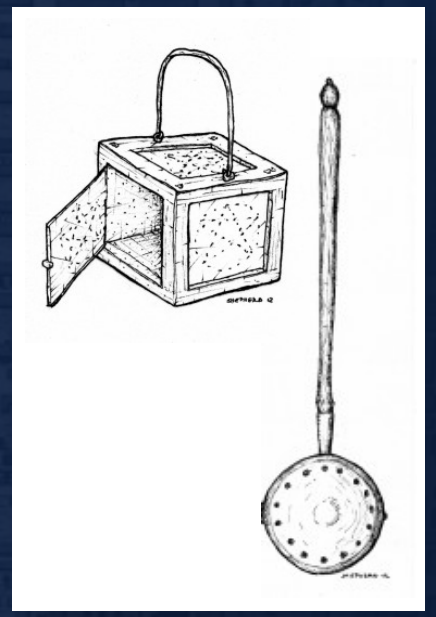

Philadelphia
18TH CENTURY


Innovation focused on reacting
to fires

18th Century fire prevention approaches



Chimney sweeps



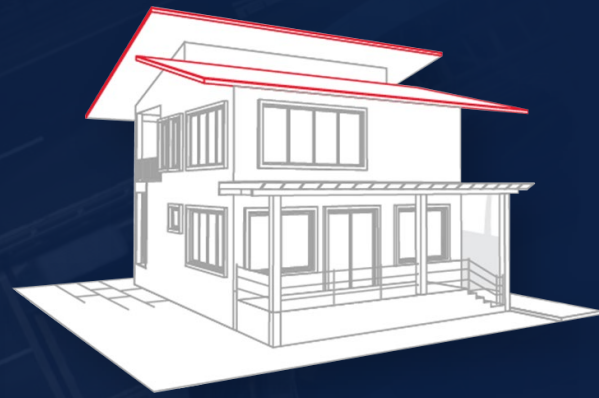
Transferring coals properly

Modern fire prevention approaches

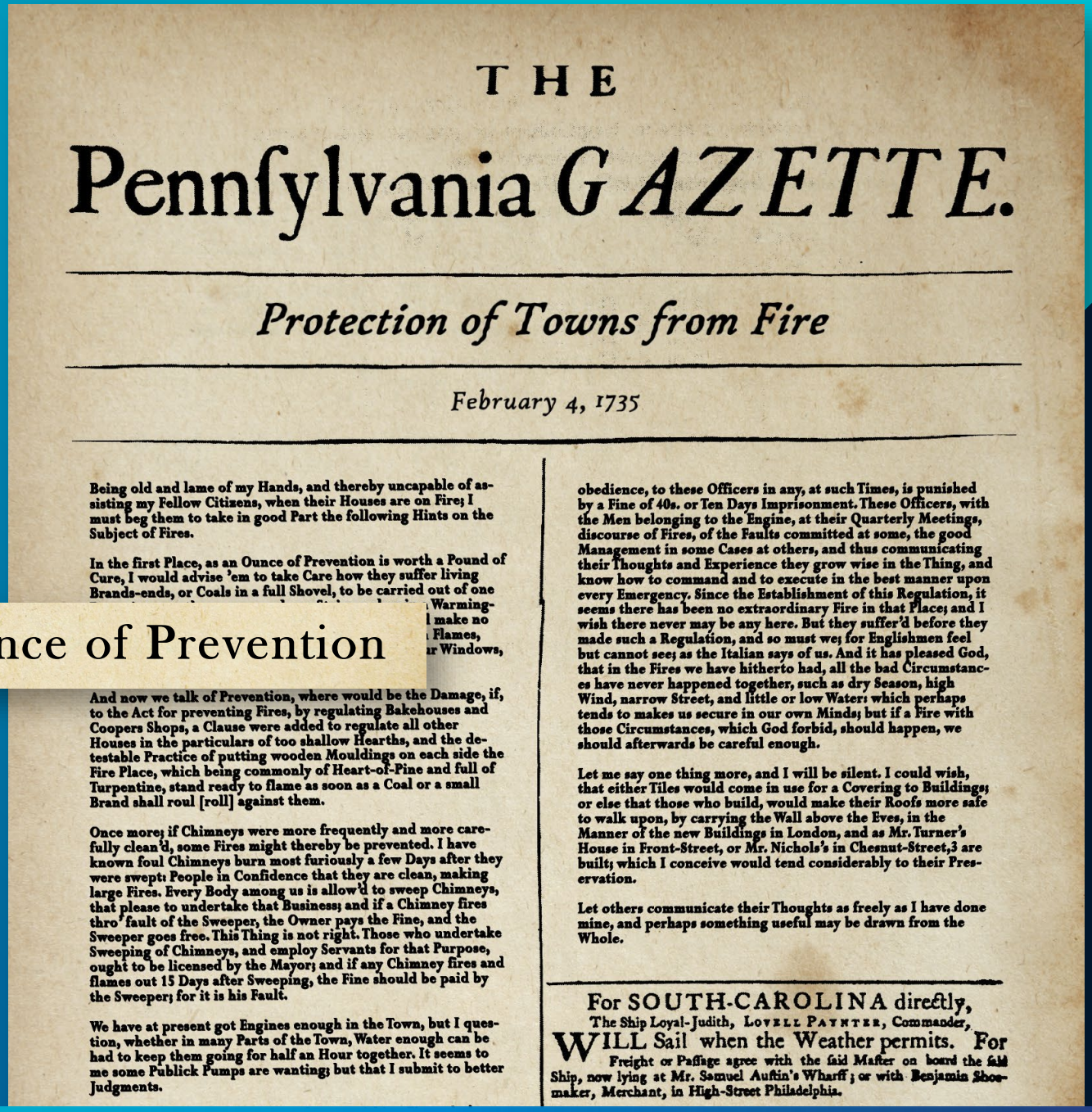
Building regulations and codes

Flame retardant paints and materials

Safe liquid storage



Fire proof homes



THE

Pennſylvania GAZETTE.

Protection of Towns from Fire

February 4, 1735

Being old and lame of my Hands, and thereby uncapable of assisting my Fellow Citizens, when their Houses are on Fire; I must beg them to take in good Part the following Hints on the Subject of Fires.

In the first Place, as an Ounce of Prevention is worth a Pound of Cure, I would advise 'em to take Care how they suffer living Brands-ends, or Coals in a full Shovel, to be carried out of one Warming-
make no
Flames,
Windows,

And now we talk of Prevention, where would be the Damage, if, to the Act for preventing Fires, by regulating Bakehouses and Coopers Shops, a Clause were added to regulate all other Houses in the particulars of too shallow Hearths, and the detestable Practice of putting wooden Mouldings on each side the Fire Place, which being commonly of Heart-of-Pine and full of Turpentine, stand ready to flame as soon as a Coal or a small Brand shall roul [roll] against them.

Once more; if Chimneys were more frequently and more carefully clean'd, some Fires might thereby be prevented. I have known foul Chimneys burn most furiously a few Days after they were swept: People in Confidence that they are clean, making large Fires. Every Body among us is allow'd to sweep Chimneys, that please to undertake that Business; and if a Chimney fires thro' fault of the Sweeper, the Owner pays the Fine, and the Sweeper goes free. This Thing is not right. Those who undertake Sweeping of Chimneys, and employ Servants for that Purpose, ought to be licensed by the Mayor; and if any Chimney fires and flames out 15 Days after Sweeping, the Fine should be paid by the Sweeper; for it is his Fault.

We have at present got Engines enough in the Town, but I question, whether in many Parts of the Town, Water enough can be had to keep them going for half an Hour together. It seems to me some Publick Pumps are wanting; but that I submit to better Judgments.

obedience, to these Officers in any, at such Times, is punished by a Fine of 40s. or Ten Days Imprisonment. These Officers, with the Men belonging to the Engine, at their Quarterly Meetings, discourse of Fires, of the Faults committed at some, the good Management in some Cases at others, and thus communicating their Thoughts and Experience they grow wise in the Thing, and know how to command and to execute in the best manner upon every Emergency. Since the Establishment of this Regulation, it seems there has been no extraordinary Fire in that Place; and I wish there never may be any here. But they suffer'd before they made such a Regulation, and so must we; for Englishmen feel but cannot see; as the Italian says of us. And it has pleased God, that in the Fires we have hitherto had, all the bad Circumstances have never happened together, such as dry Season, high Wind, narrow Street, and little or low Water: which perhaps tends to makes us secure in our own Minds; but if a Fire with those Circumstances, which God forbid, should happen, we should afterwards be careful enough.

Let me say one thing more, and I will be silent. I could wish, that either Tiles would come in use for a Covering to Buildings; or else that those who build, would make their Roofs more safe to walk upon, by carrying the Wall above the Eves, in the Manner of the new Buildings in London, and as Mr. Turner's House in Front-Street, or Mr. Nichols's in Chesnut-Street,3 are built; which I conceive would tend considerably to their Preservation.

Let others communicate their Thoughts as freely as I have done mine, and perhaps something useful may be drawn from the Whole.

For SOUTH-CAROLINA directly,
The Ship Loyal-Judith, LOVELL PAYNTER, Commander,
WILL Sail when the Weather permits. For Freight or Paſſage agree with the ſaid Maſter on board the ſaid Ship, now lying at Mr. Samuel Auſtin's Wharff; or with Benjamin Shoemaker, Merchant, in High-Street Philadelphia.

an Ounce of Prevention

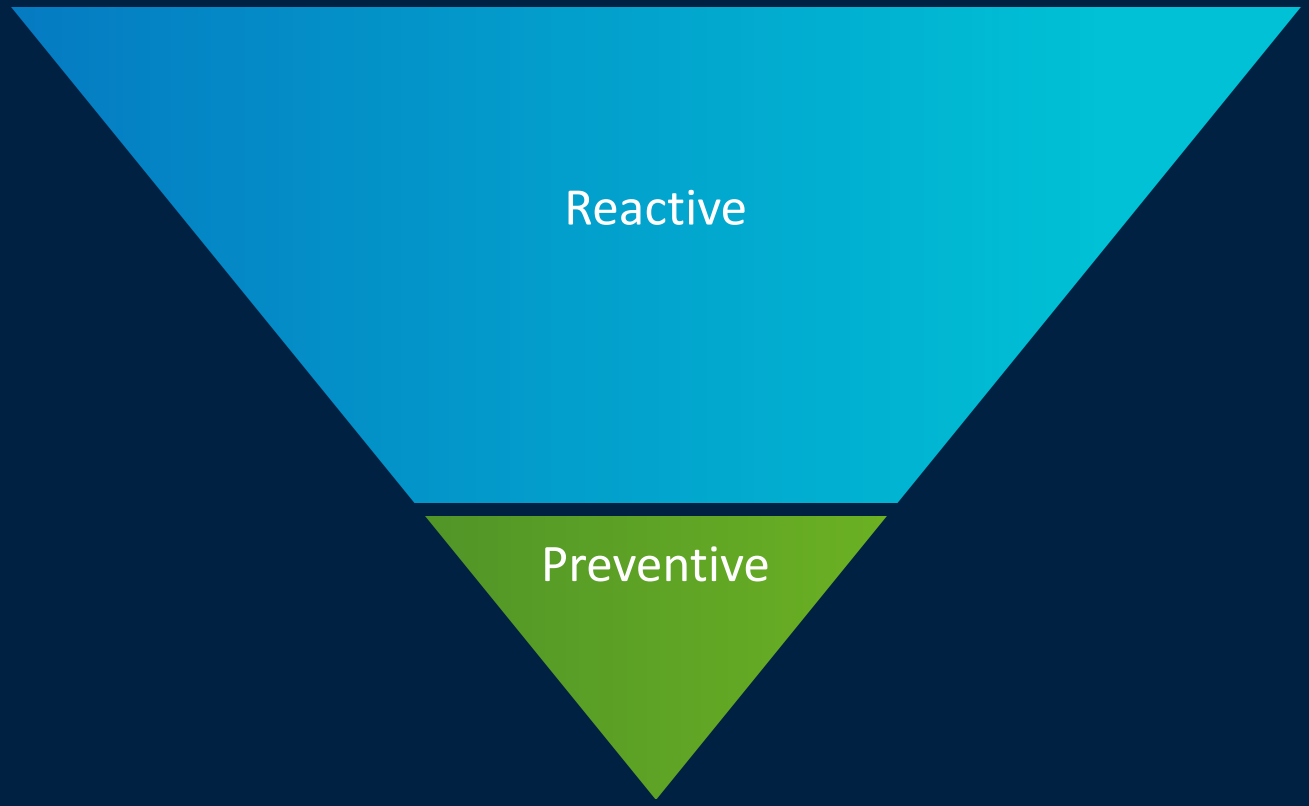
An Ounce of Prevention

Reactive Versus Preventive Cyber Controls

Firefighting versus fire prevention

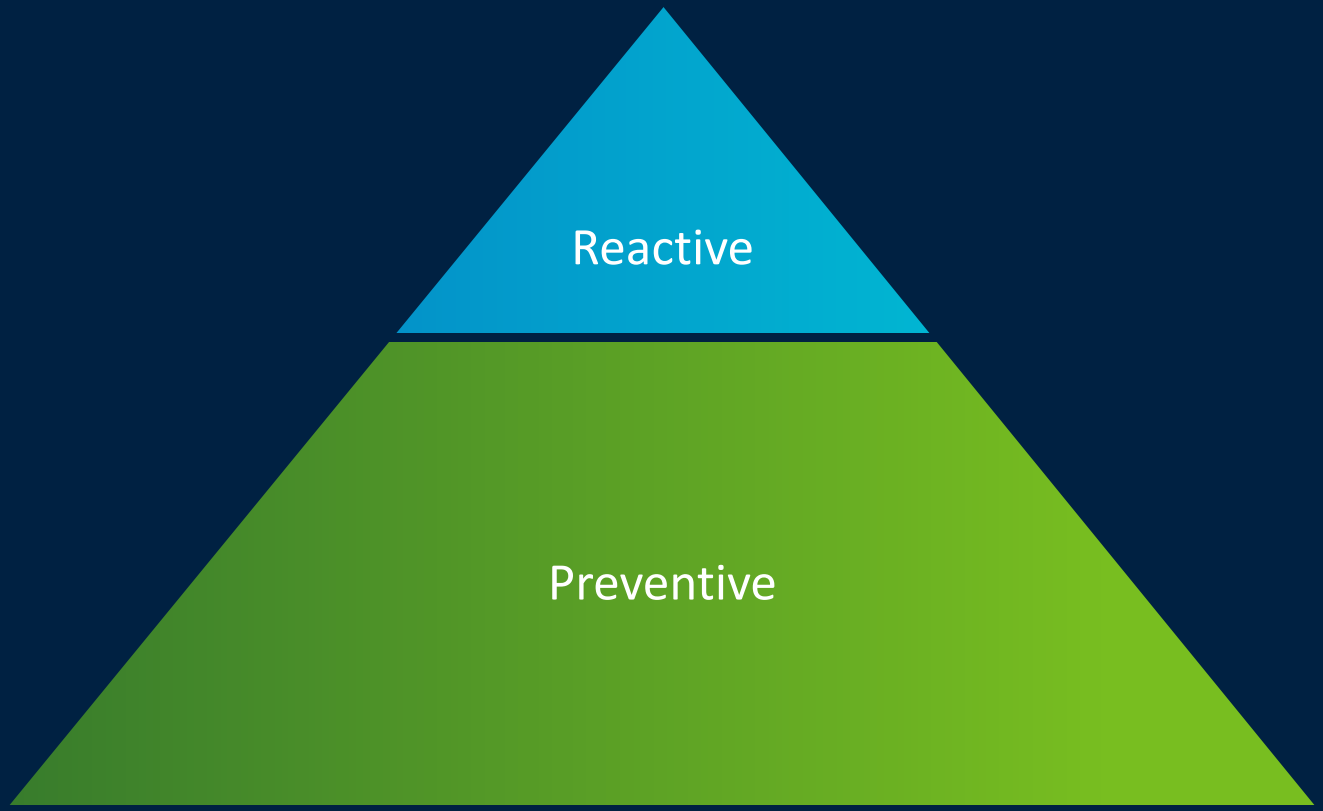
Where do we Invest and Innovate?

Reactive versus preventive cyber controls



What has the Bigger Impact on Risk?

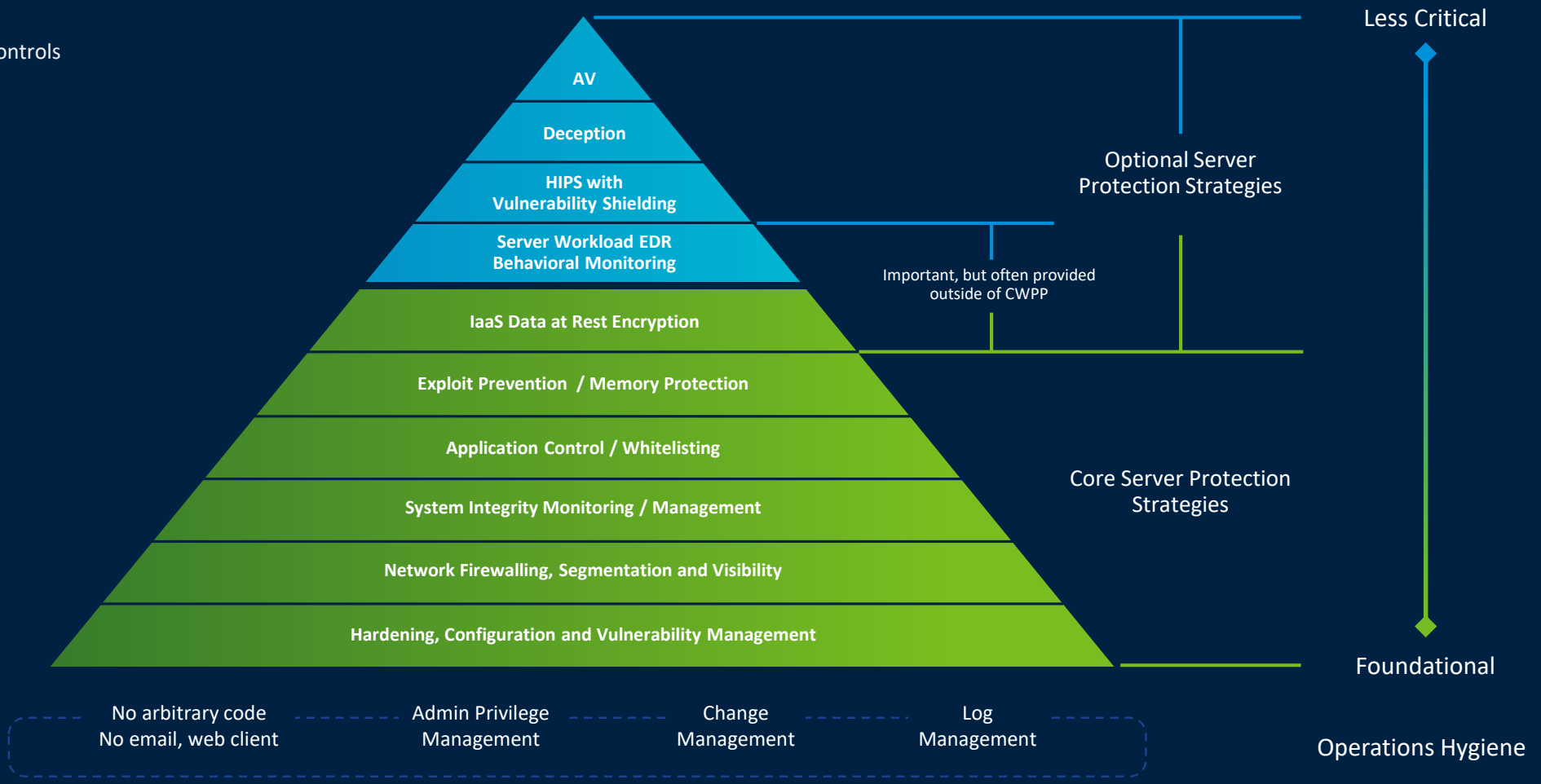
Reactive versus preventive cyber controls



Cloud Workload Protect Controls Hierarchy

Gartner Market Guide for Cloud Workload Protection Framework

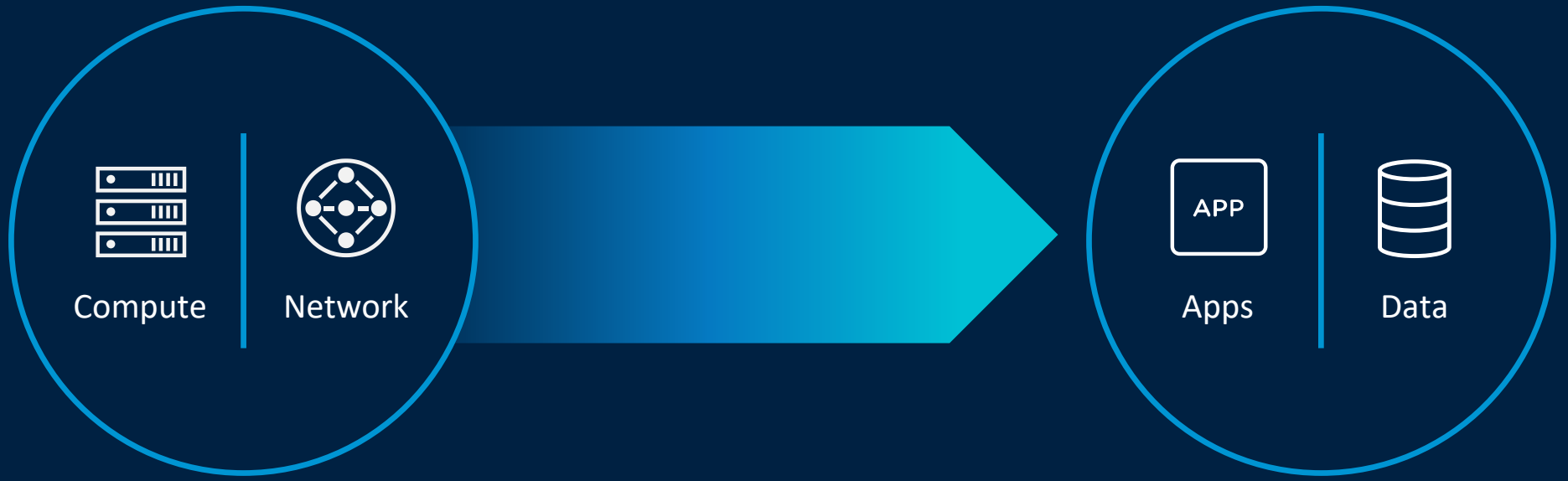
Figure 1. Cloud Workload Protection Controls Hierarchy, © 2018 Gartner, Inc.



Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, March 26th 2018. *Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. Charts/graphics created by VMware based on Gartner research.*

What Would it Take to Rethink Prevention?

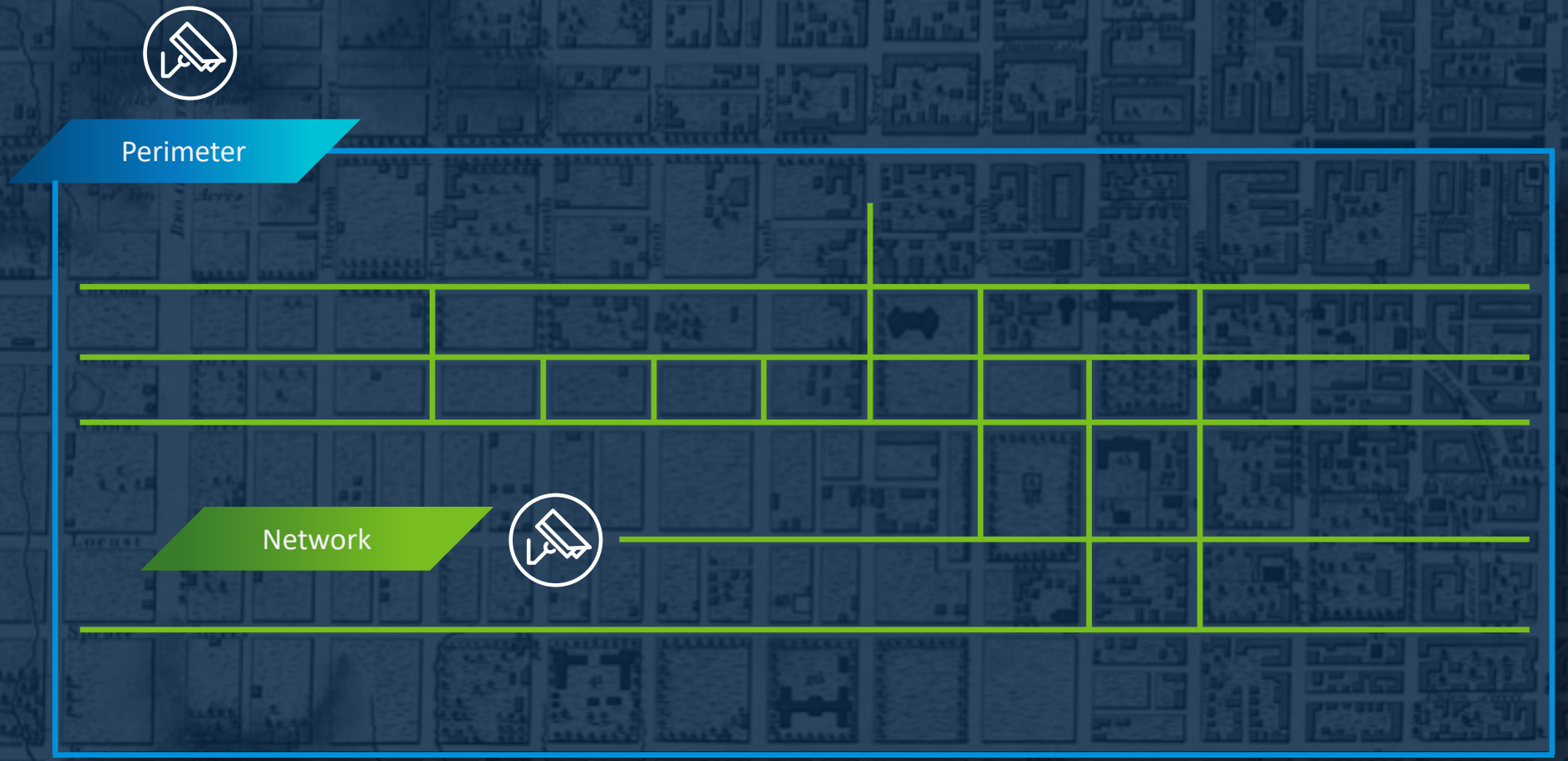
Shift the focus from infrastructure to applications



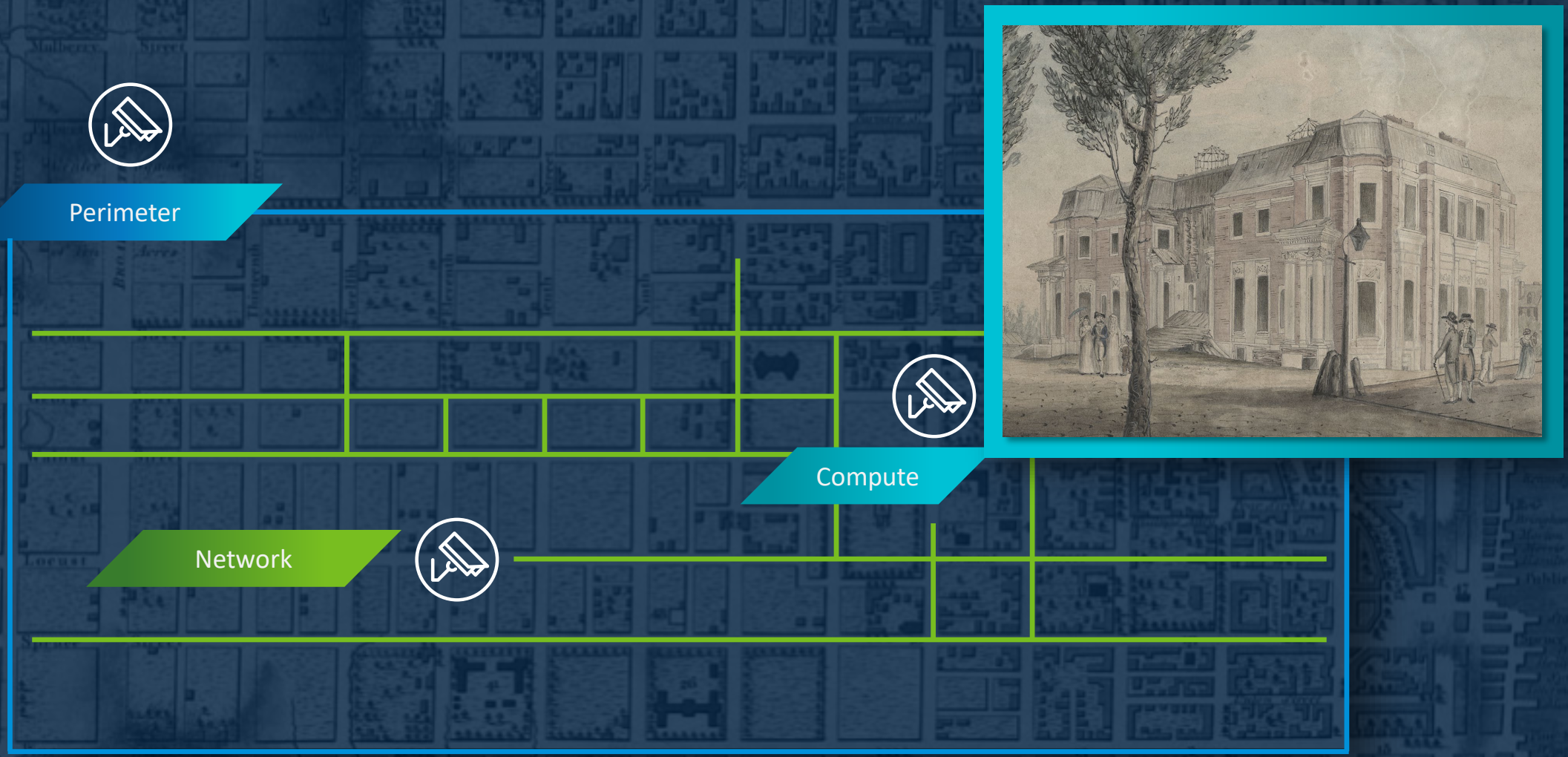
An Infrastructure-Centric Approach

Perimeter

An Infrastructure-Centric Approach

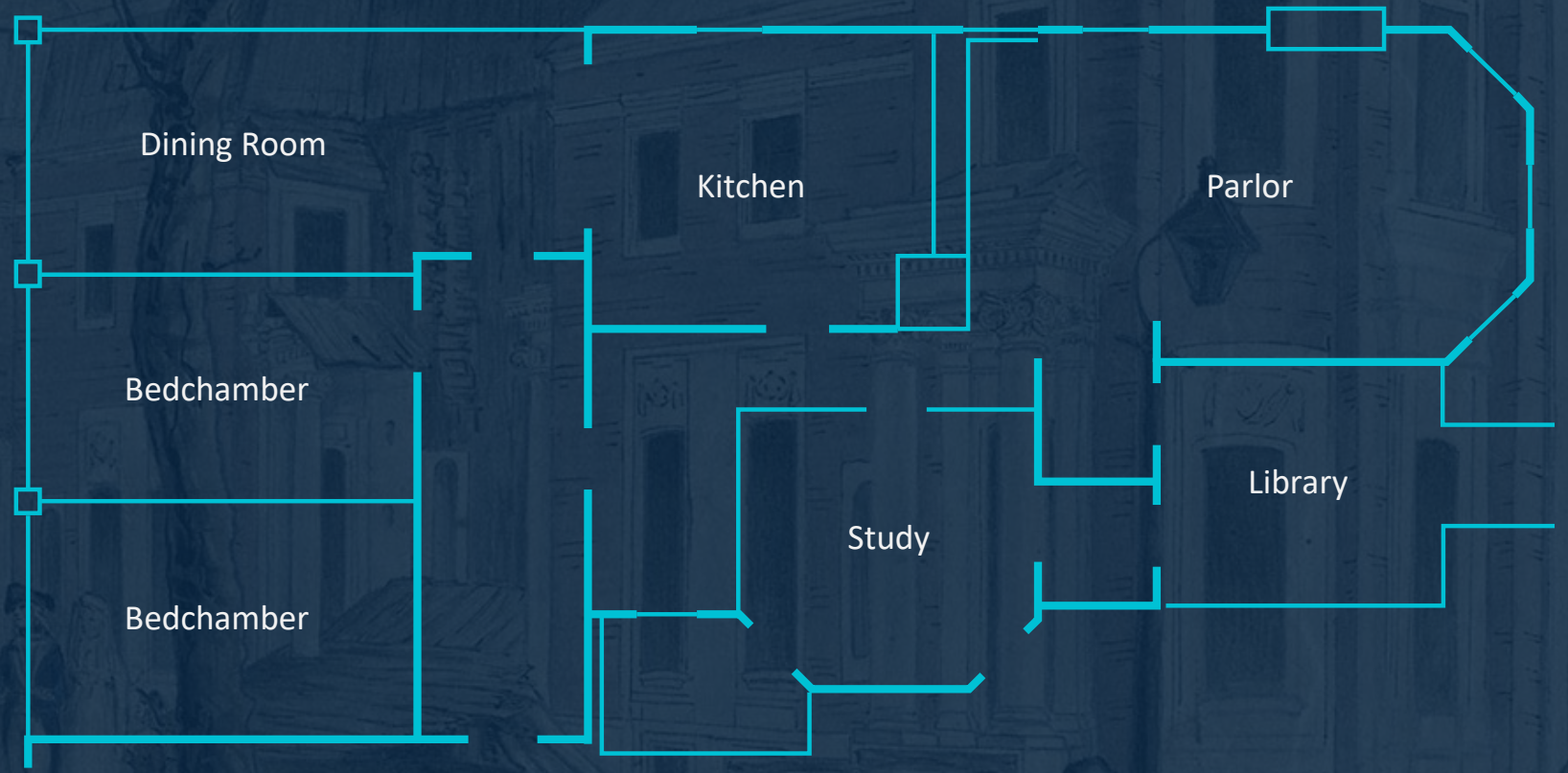


An Infrastructure-Centric Approach



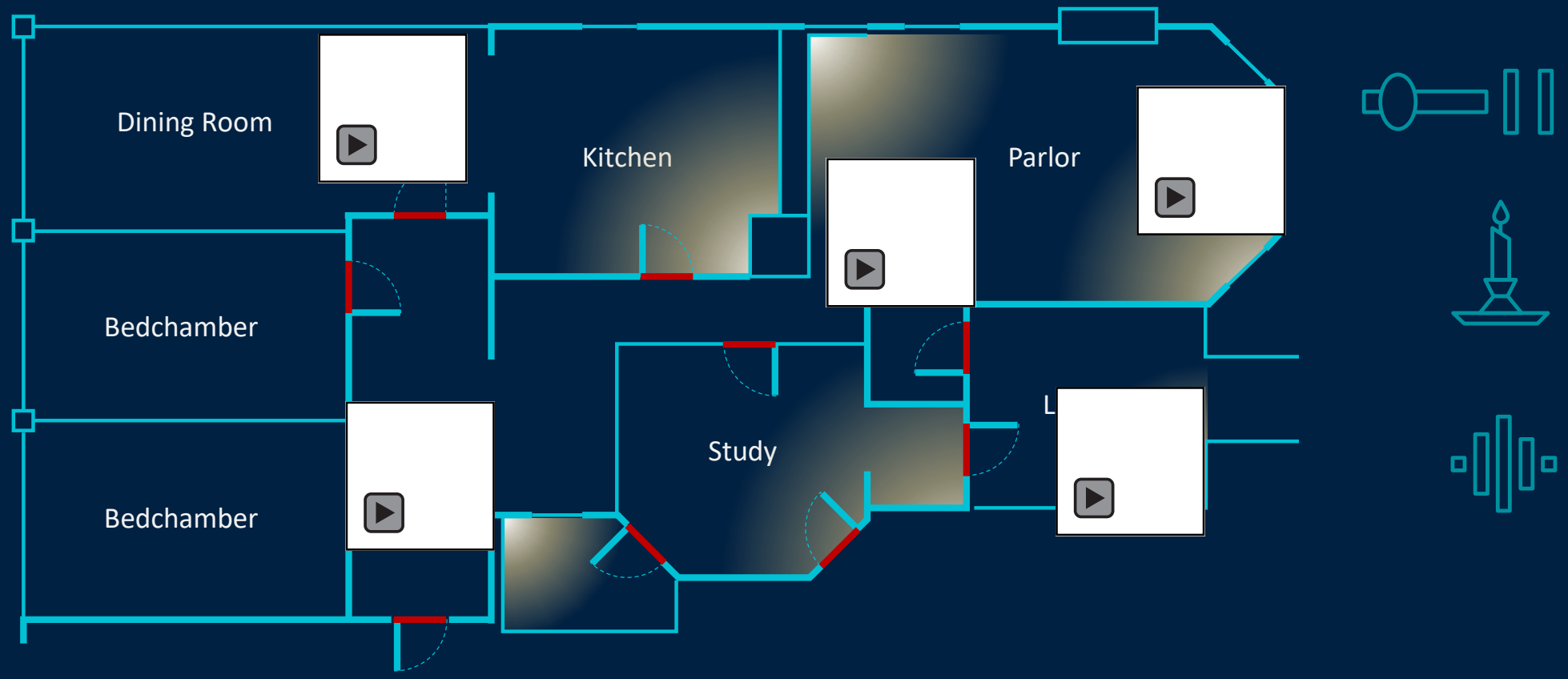
An Application-Centric Approach

Understand the composition, topology and behavior of your application



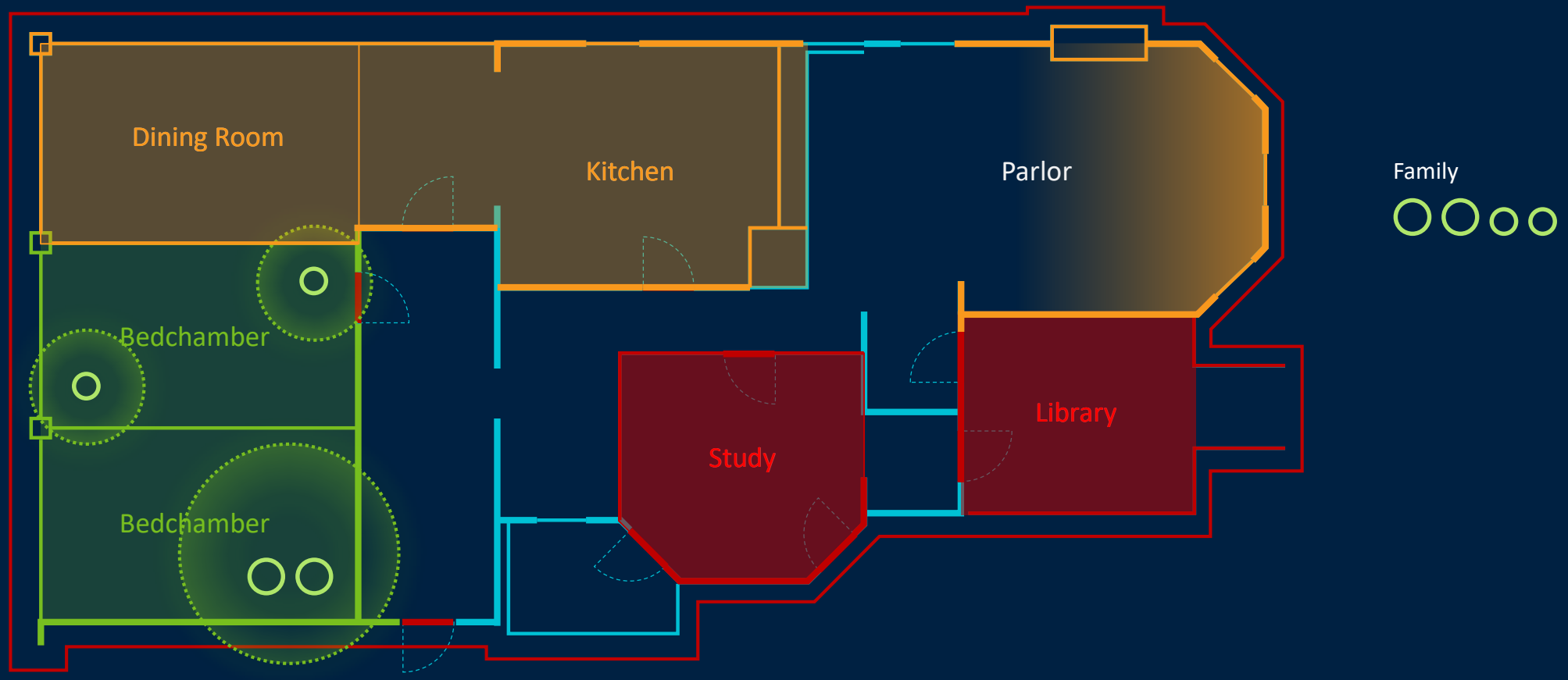
An Application-Centric Approach

Understand the composition, topology and behavior of your application



An Application-Centric Approach

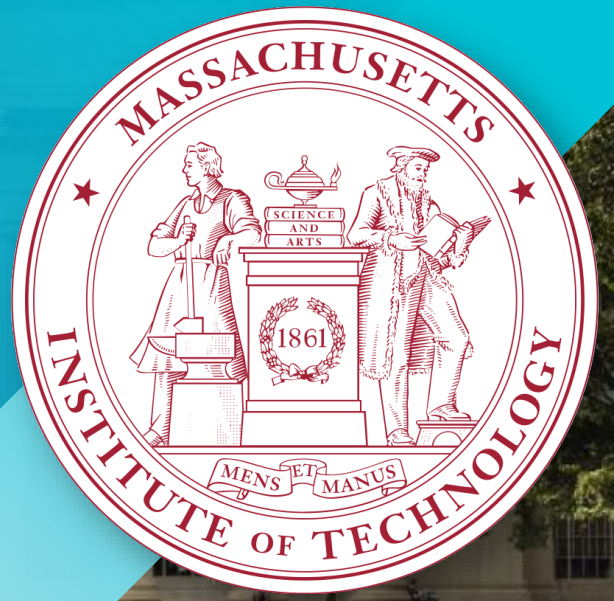
Use that understanding to drive how you lock and monitor



Principle of Least Privilege

"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."

Professor Jerome Saltzer,
MIT Communications of the ACM

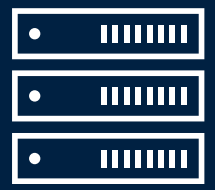



Attacker advantage
Defender advantage

Focus on Infrastructure

Attacker advantage

Defender advantage



Compute

Storage

Network

Focus on Threats

Attacker advantage

Defender advantage

Compute

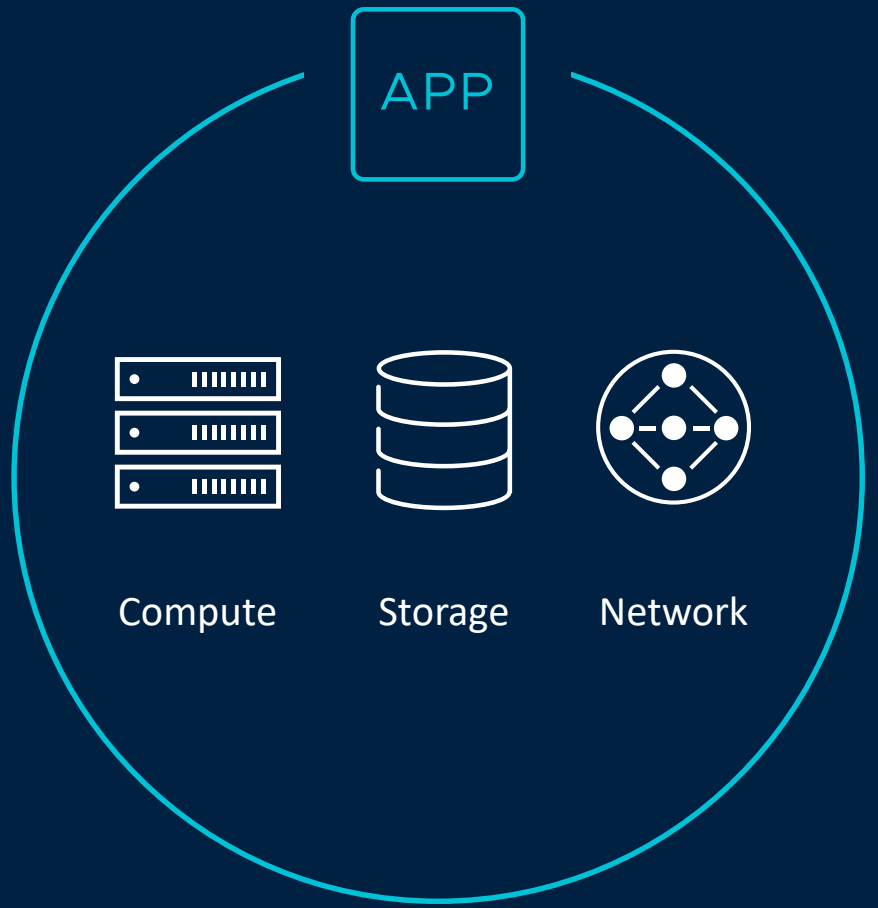
Storage

Network

Focus on the Application

Attacker advantage

Defender advantage




APP

Application

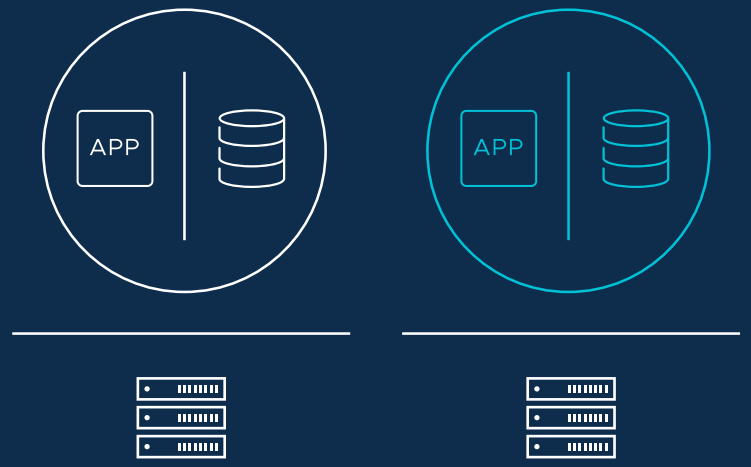
Automation

Intrinsic

The Unique Properties of Clouds

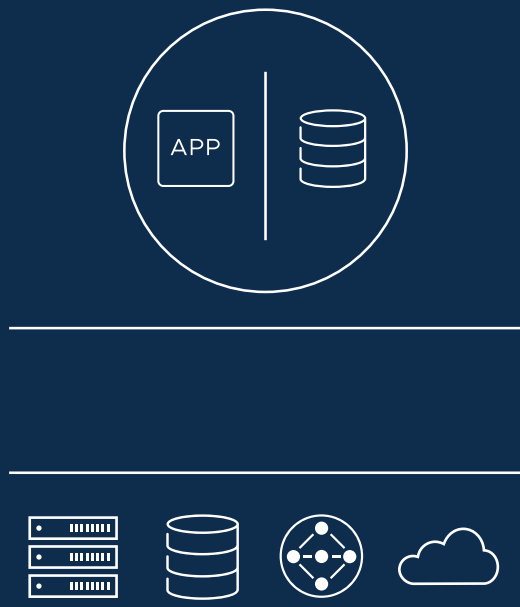
Leveraging the Unique Properties of Virtualization

Application

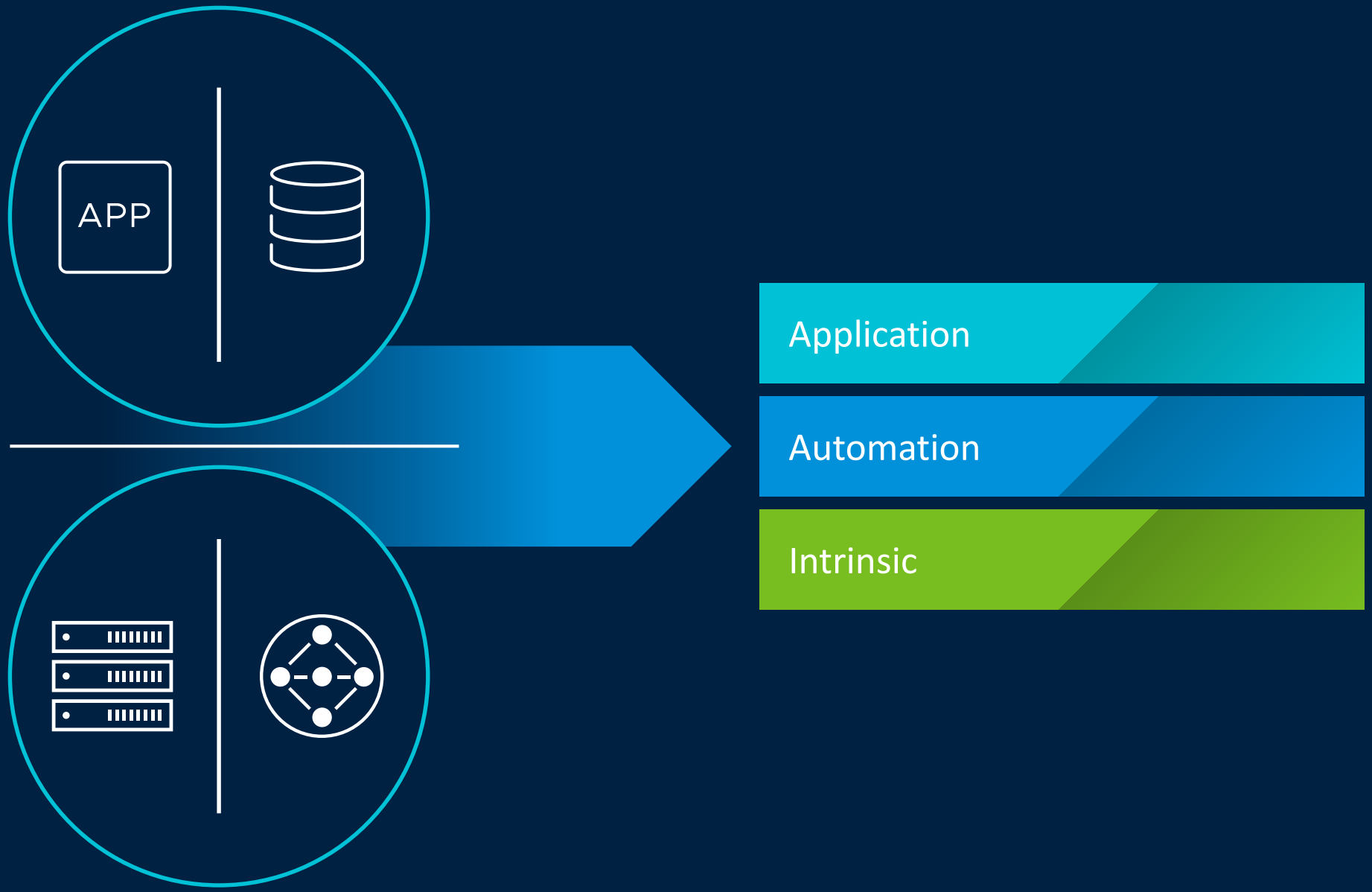


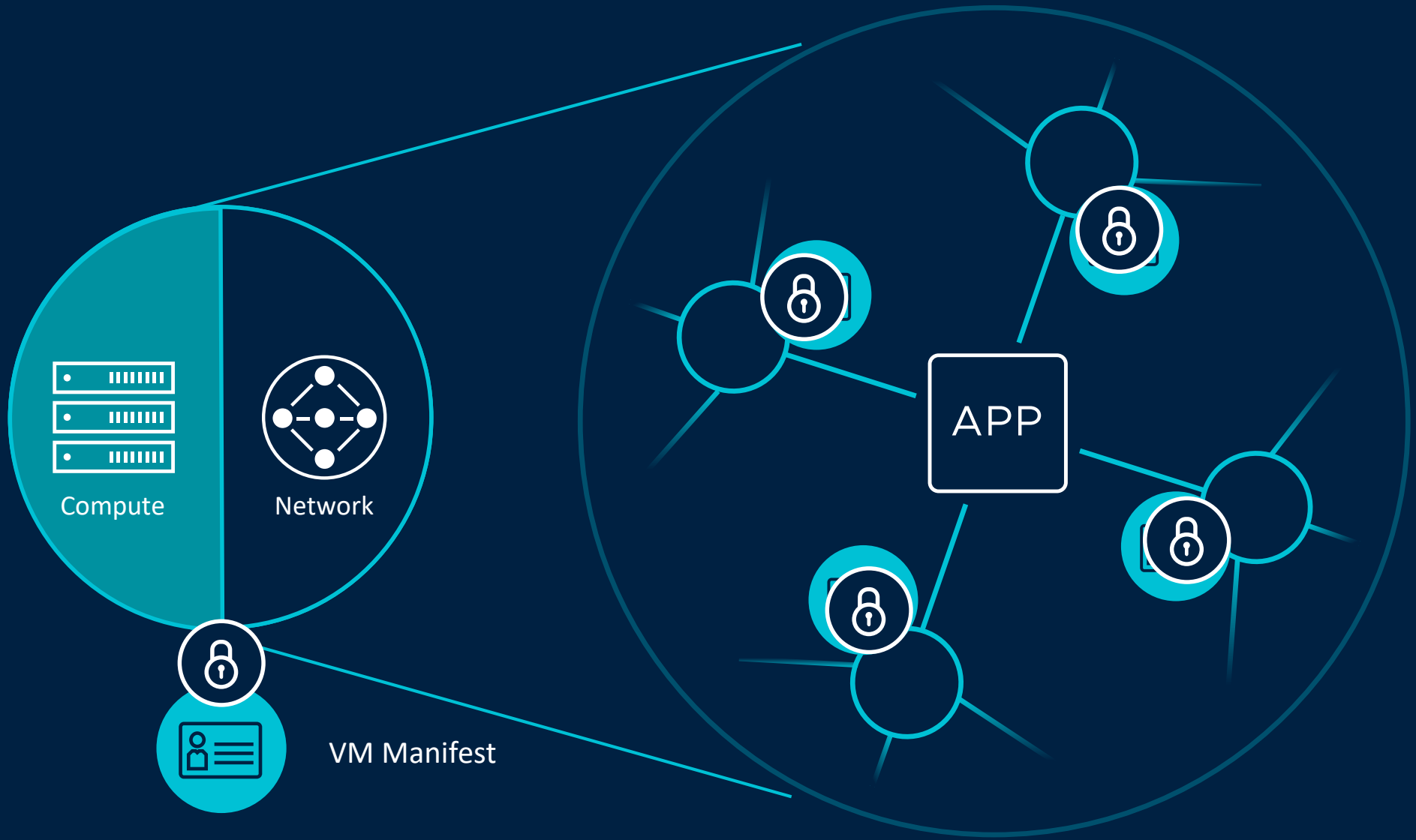
Automation

Intrinsic

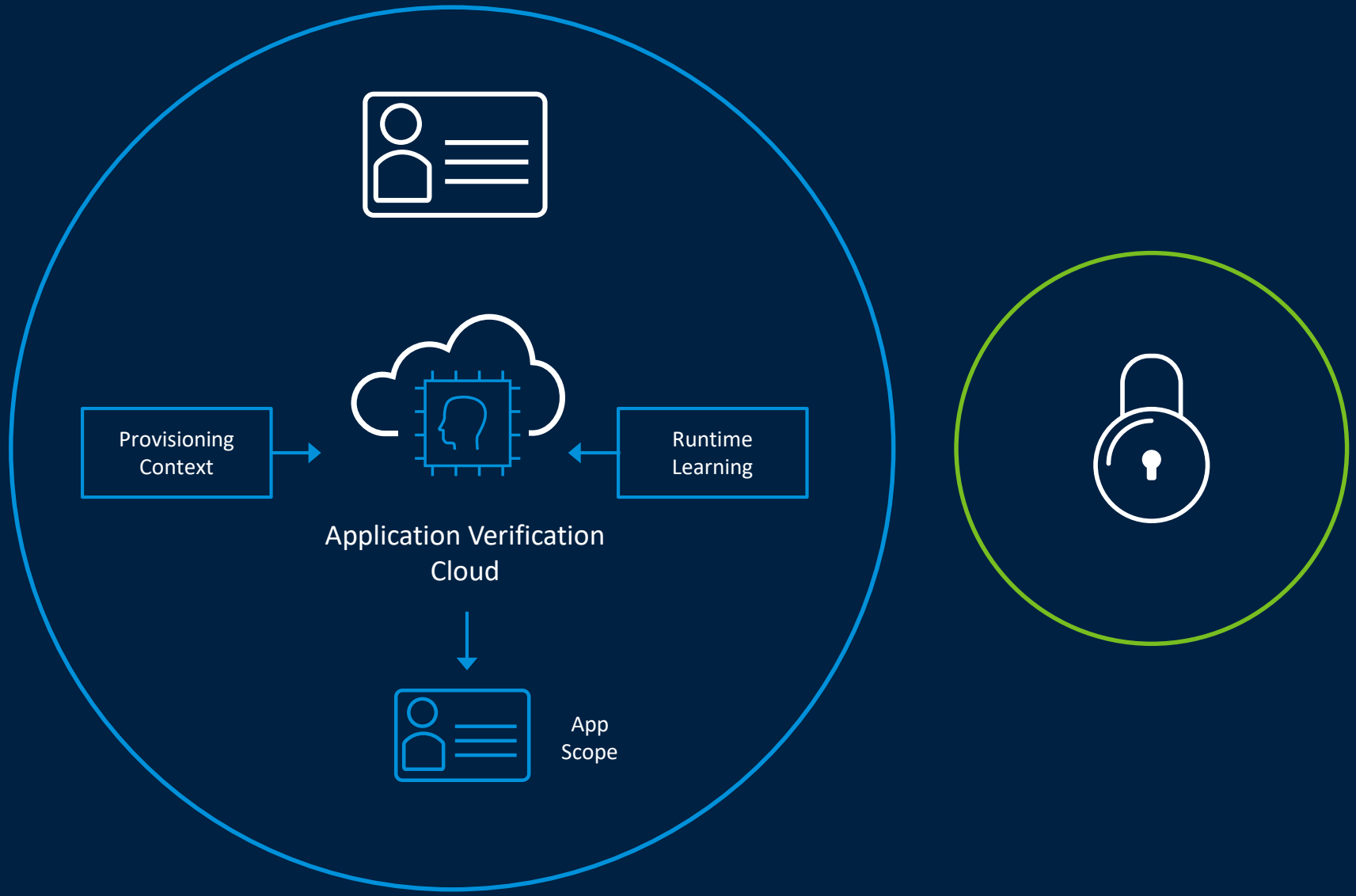


What does that look like?


APP
Application
Automation
Intrinsic


Compute
Network
VM Manifest
APP

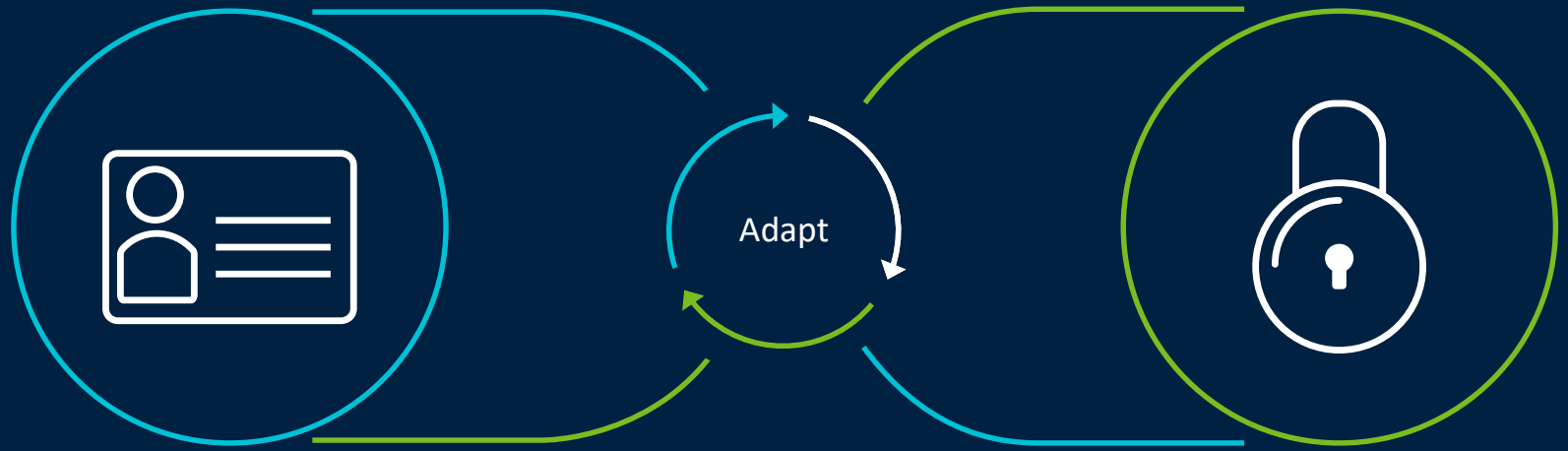
Learn


Provisioning Context
Runtime Learning
Application Verification Cloud
App Scope

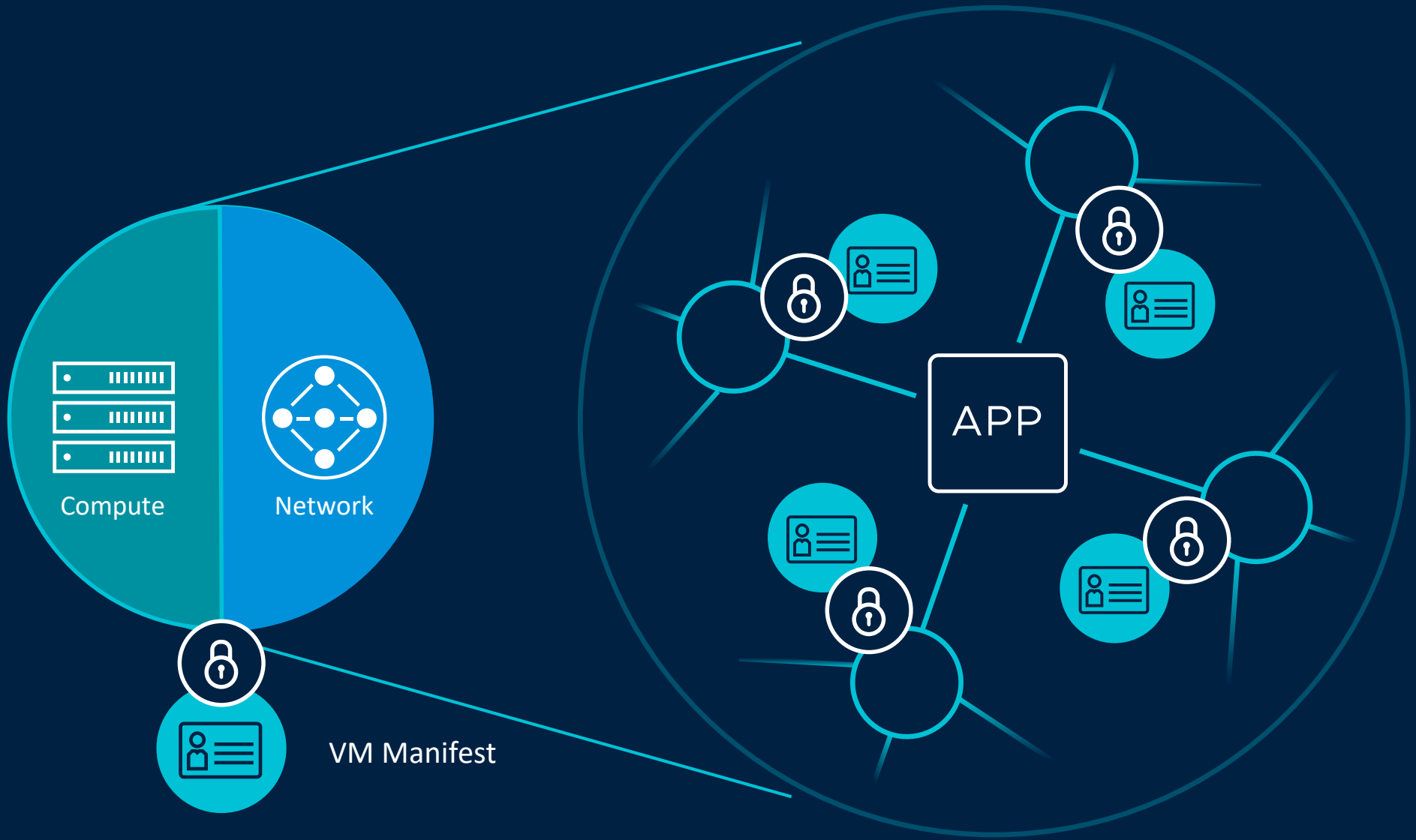
Learn

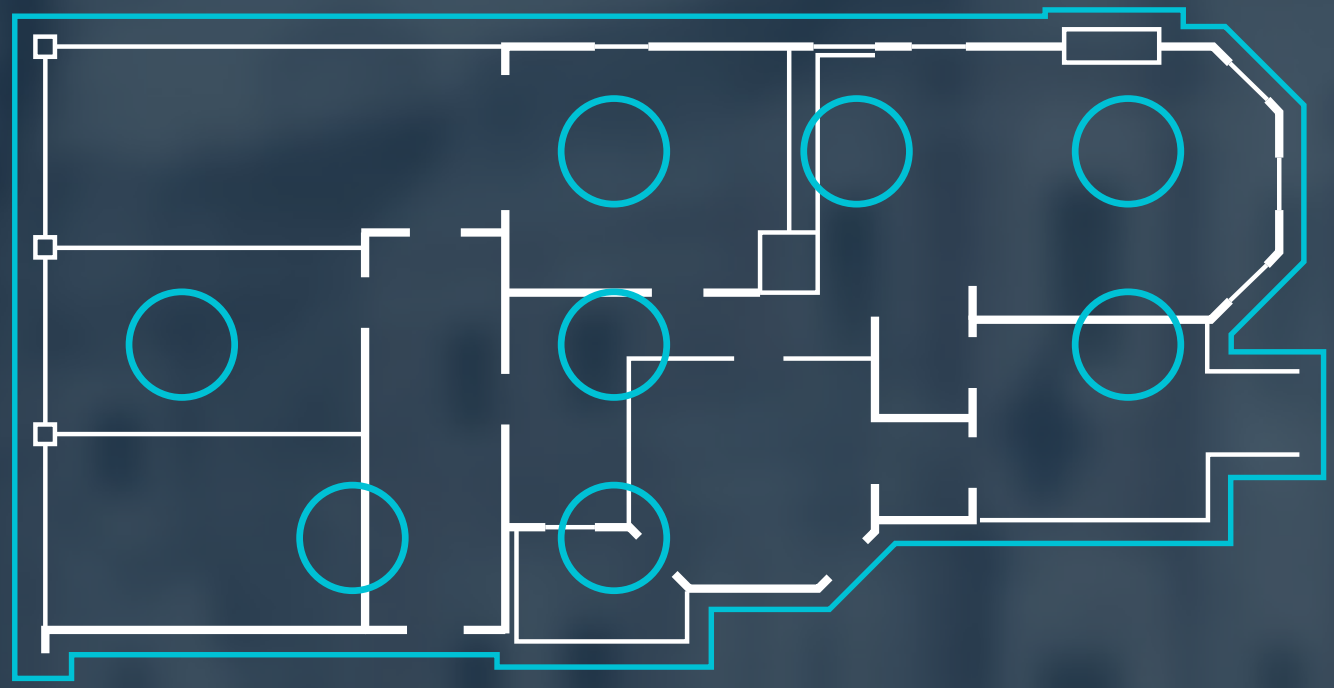

Workload
AppD Monitor
Protected zone
Leverage the virtual infrastructure
Monitor
Lock

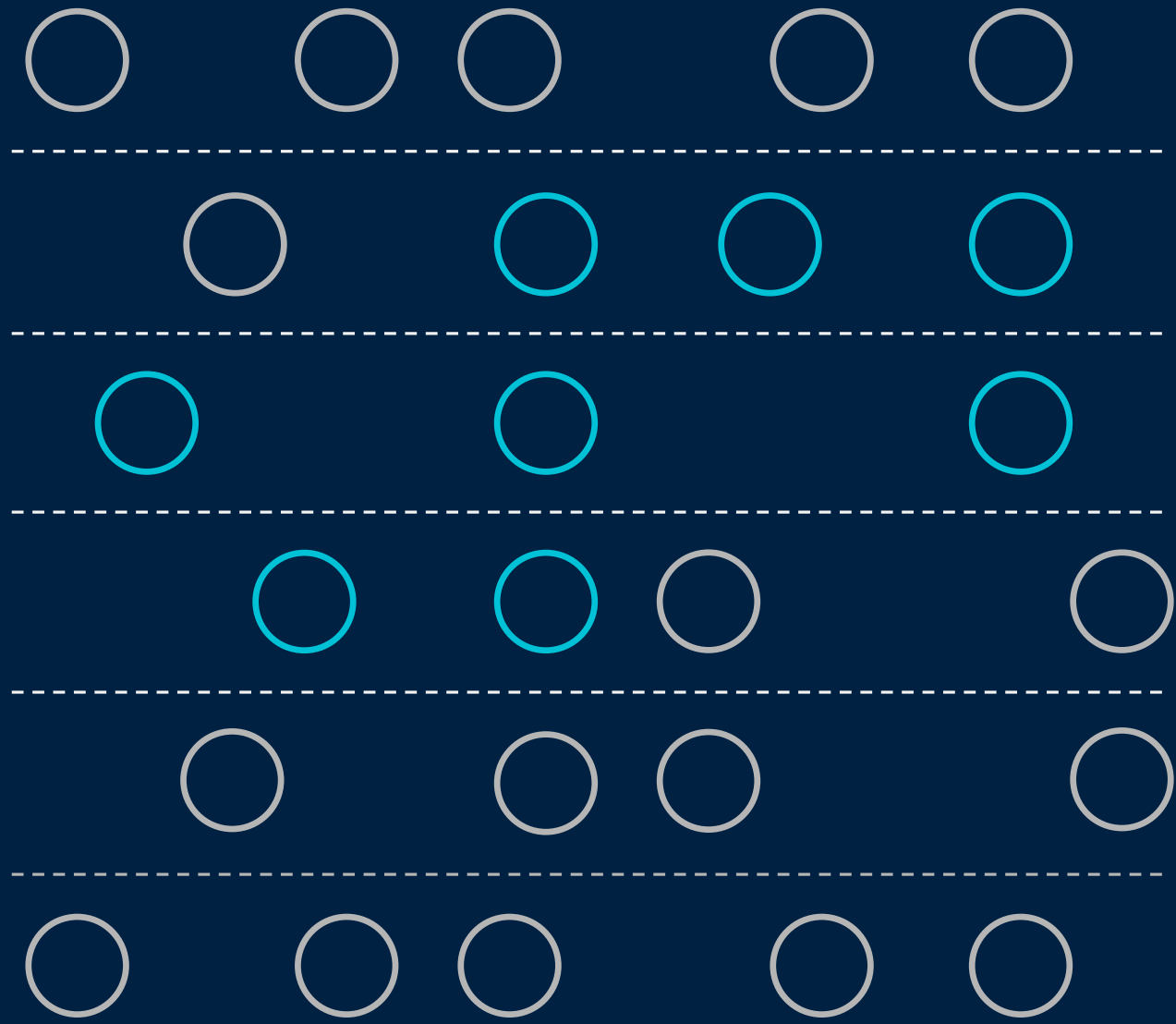
Adapt

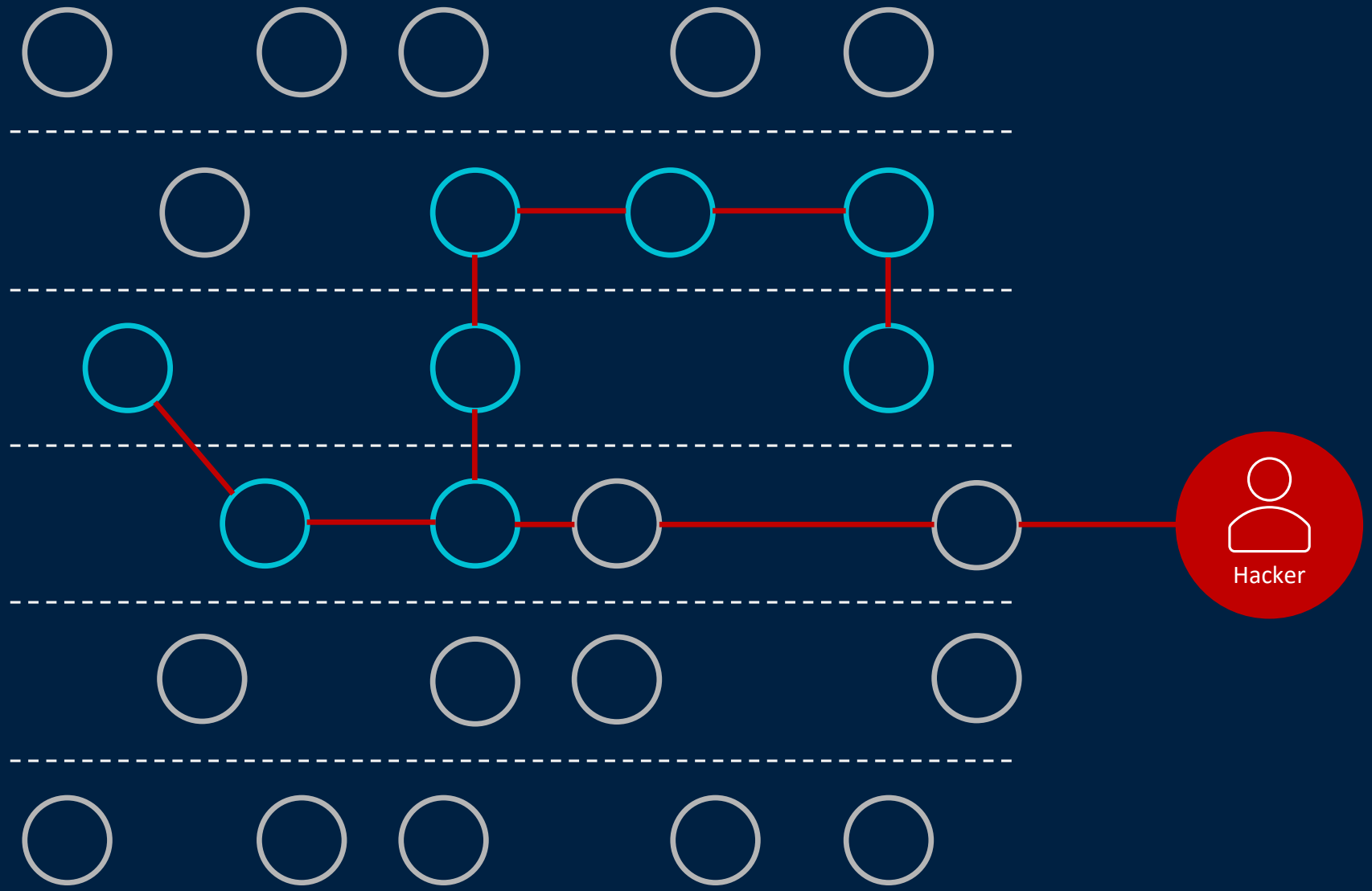


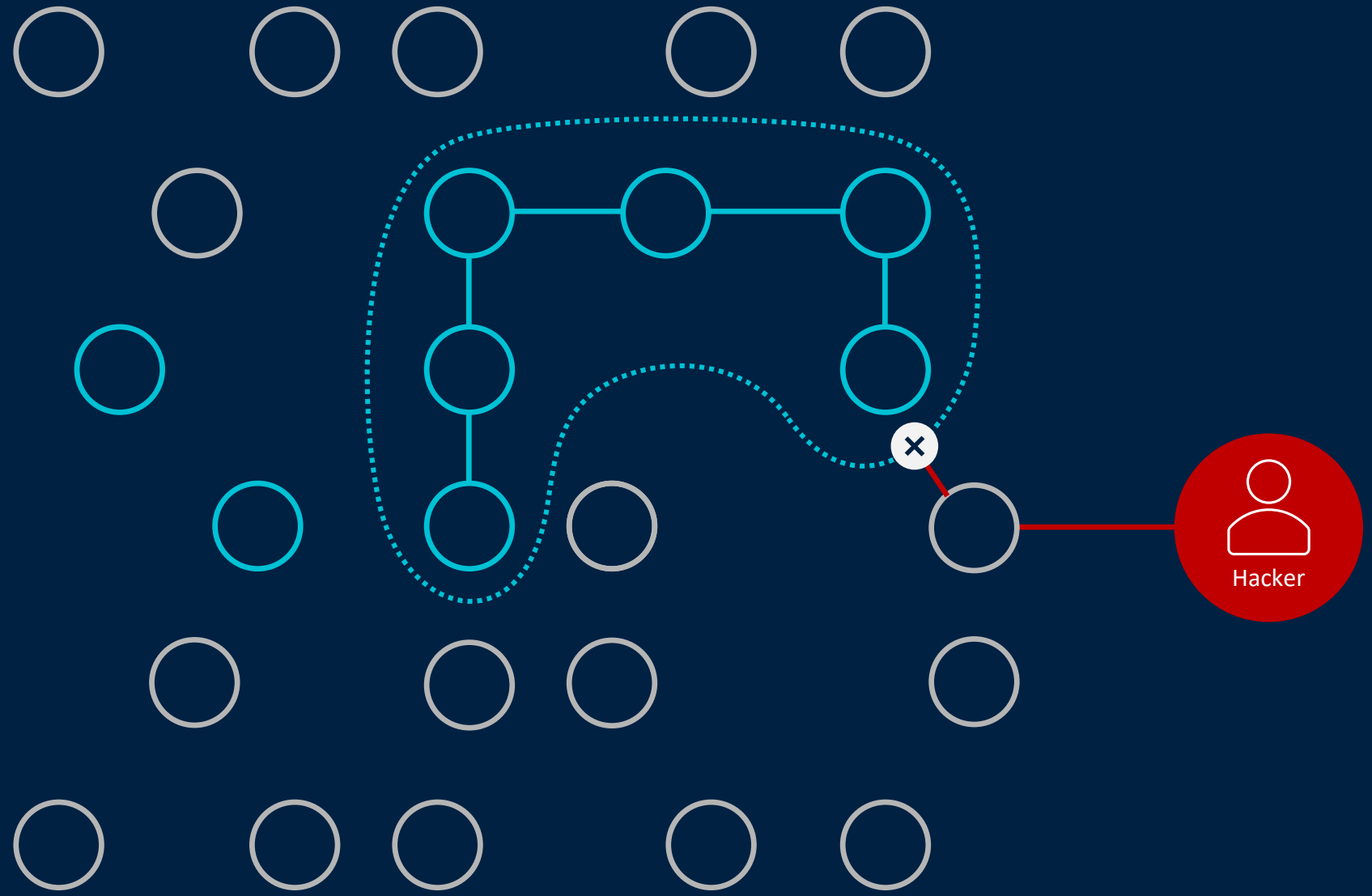
Learn / Lock / Adapt

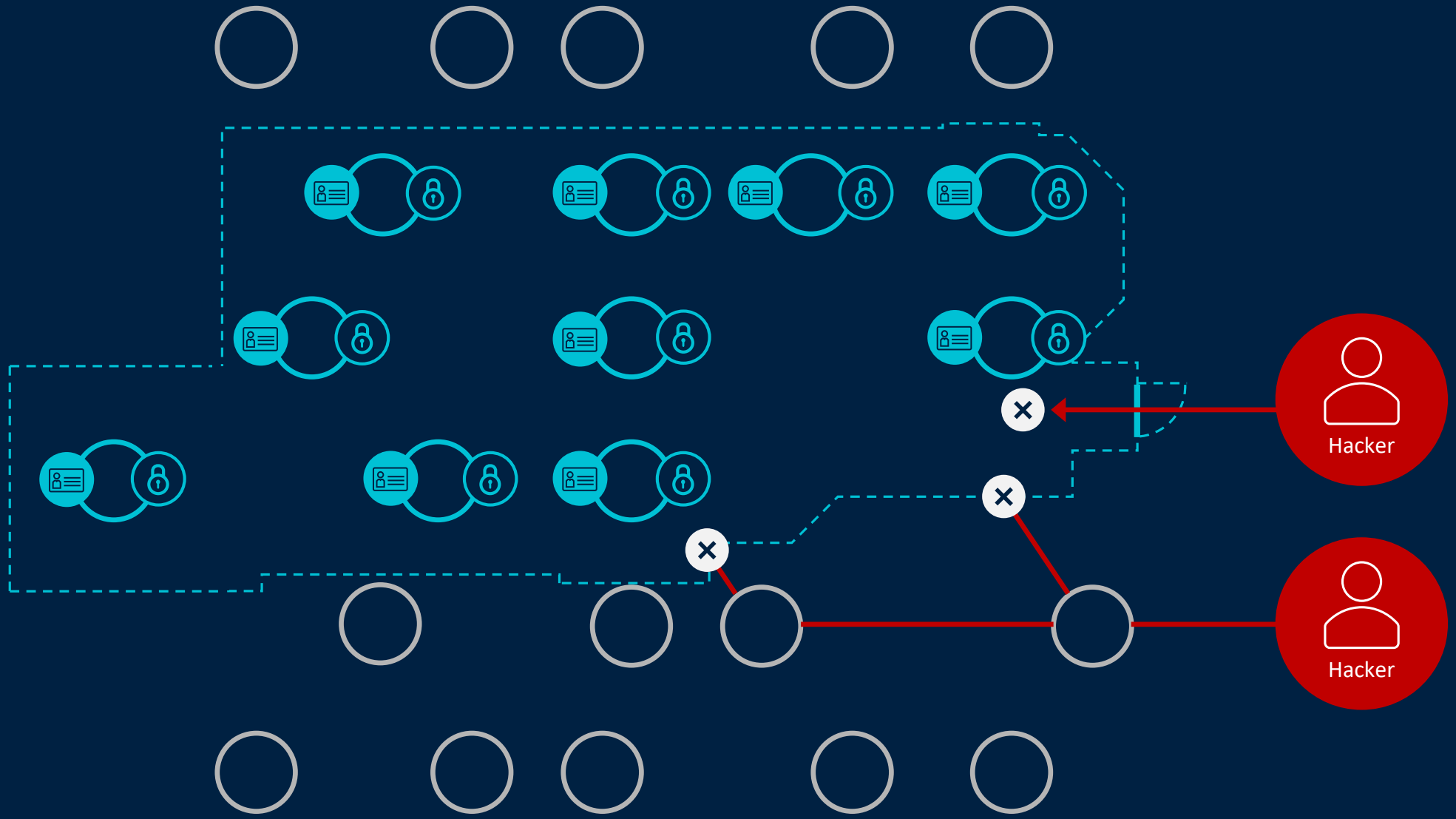

Compute
Network
VM Manifest
APP



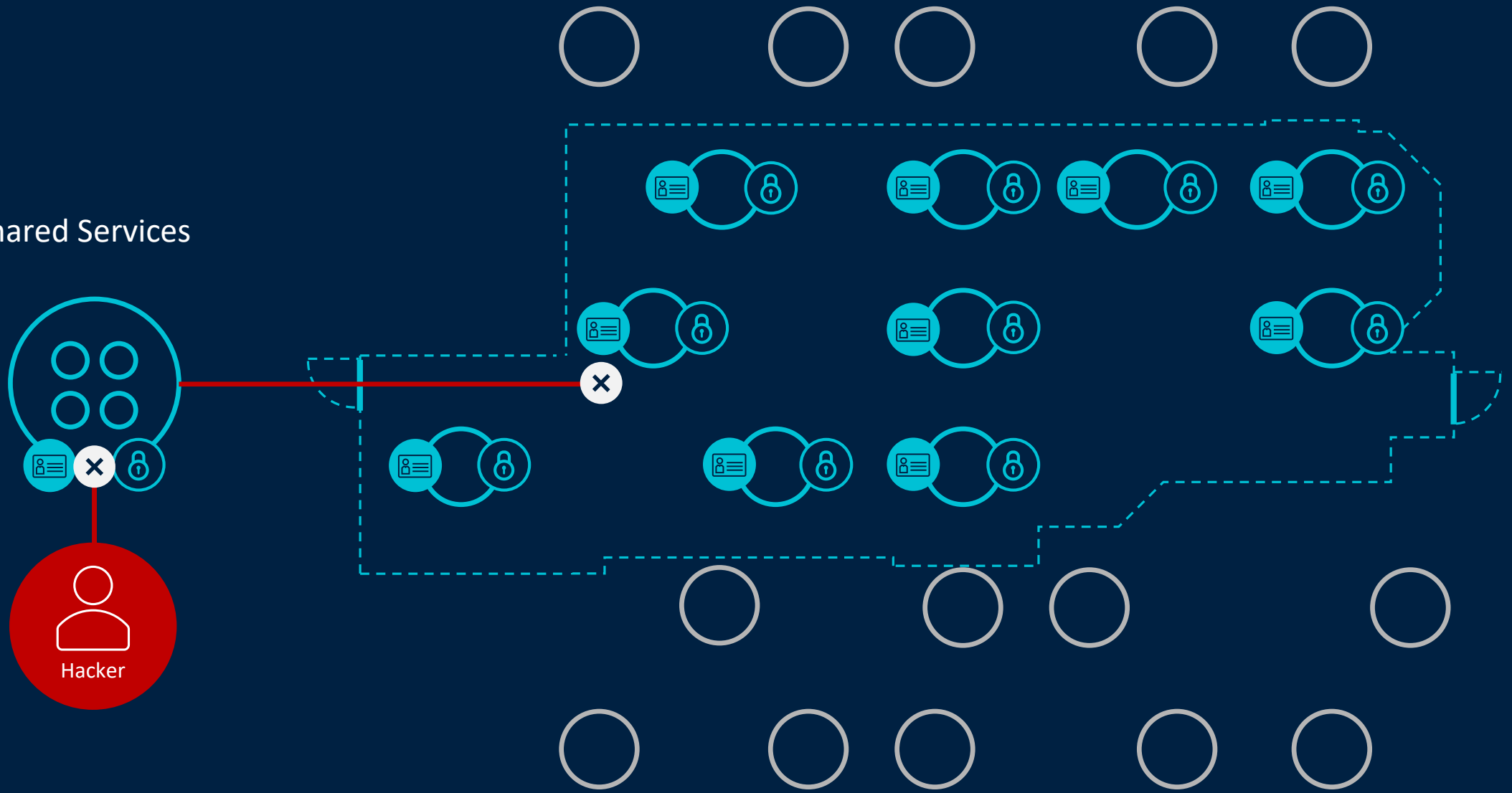





Hacker


Hacker
Hacker

Shared Services



North / South

East / West

How effective is this in real world situations?

VERODIN

Christopher Key

CEO & Co-Founder Verodin

vmware

VERODIN PLATFORM

VERODIN'S SECURITY INSTRUMENTATION PLATFORM (SIP)

Enables customers to prove the effectiveness of the cybersecurity controls within their production environment

Moves cybersecurity from a "magic black box" to a quantifiable business function

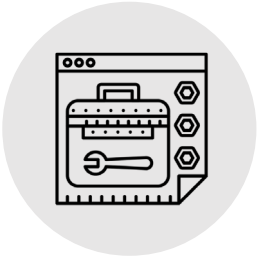
VERODIN PLATFORM

VERODIN'S SECURITY INSTRUMENTATION PLATFORM (SIP)

Enables customers to prove the effectiveness of the cybersecurity controls within their production environment

Moves cybersecurity from a "magic black box" to a quantifiable business function

CONTROL EFFECTIVENESS / CONFIGURATION ASSURANCE



OPTIMIZATION

RATIONALIZATION

KNOWN GOOD BASELINE

VERODIN PLATFORM

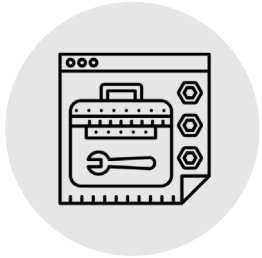
VERODIN'S SECURITY INSTRUMENTATION PLATFORM (SIP)

Enables customers to prove the effectiveness of the cybersecurity controls within their production environment

Moves cybersecurity from a "magic black box" to a quantifiable business function

CONTINUOUS VALIDATION

CONTROL EFFECTIVENESS / CONFIGURATION ASSURANCE

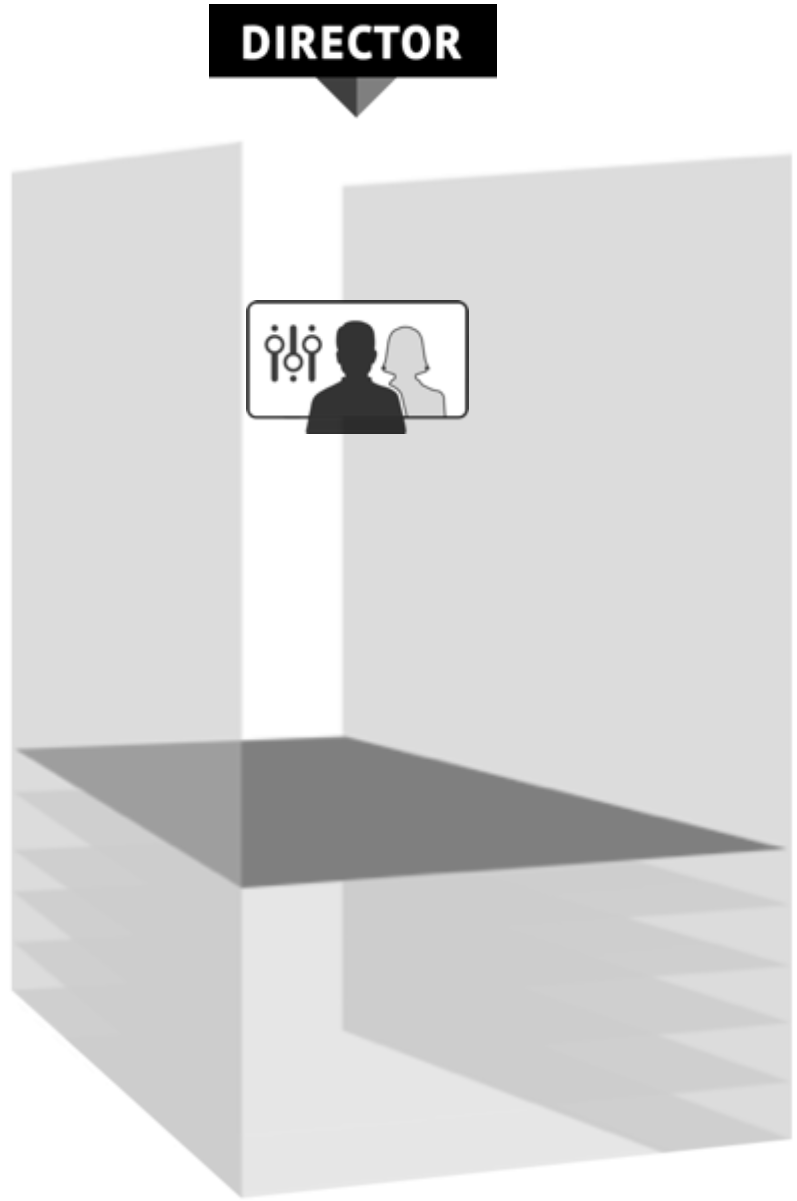


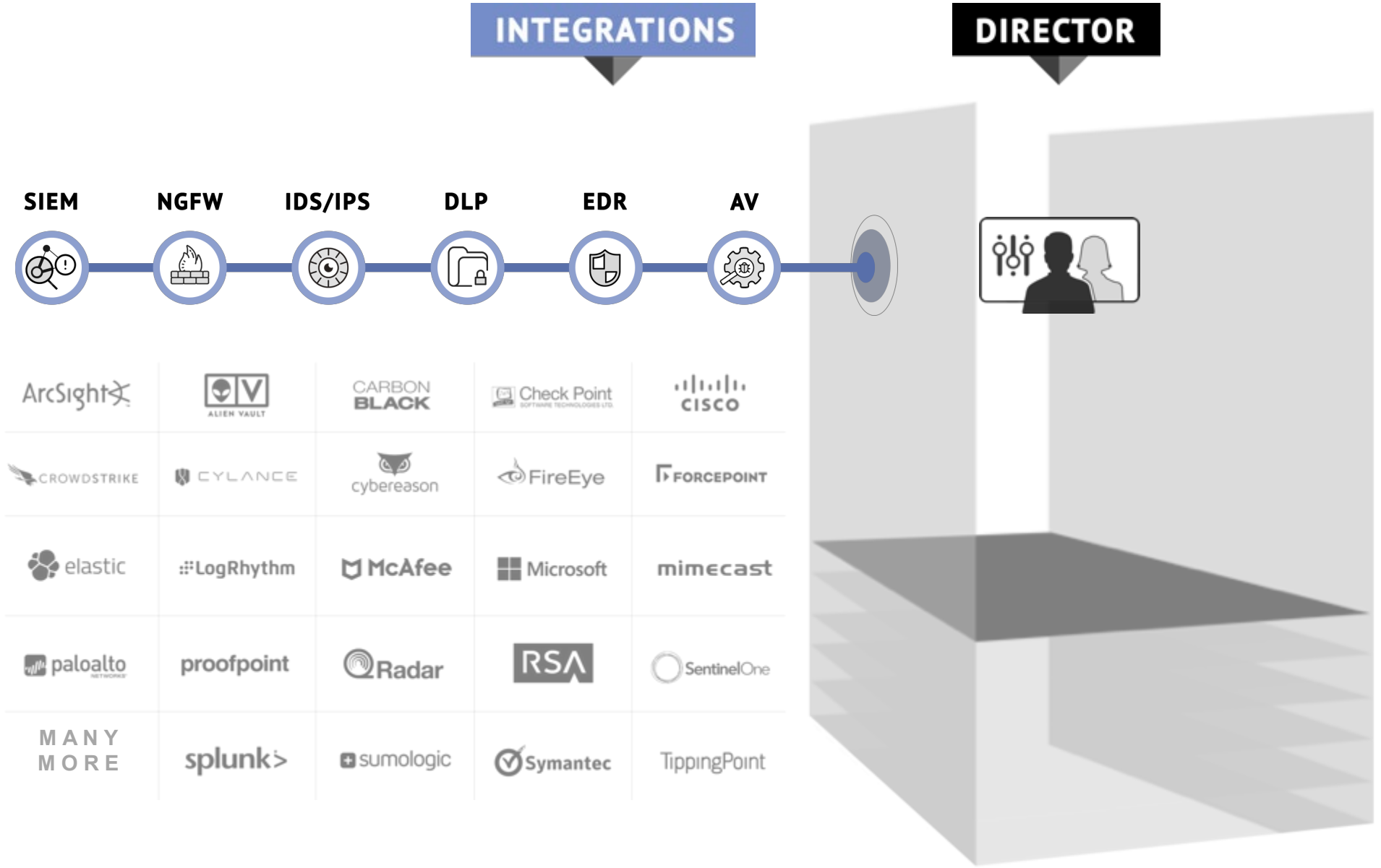
OPTIMIZATION

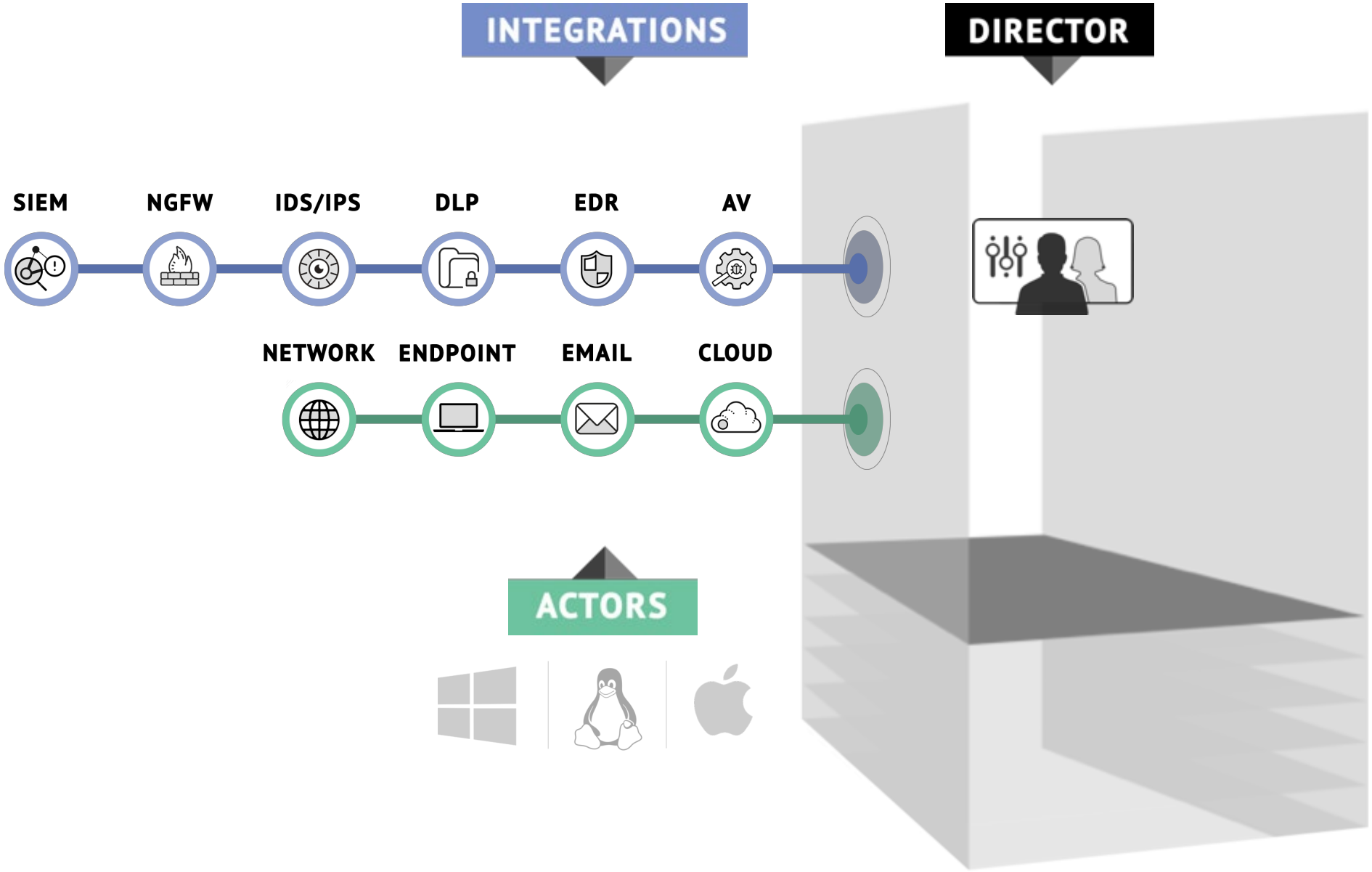
RATIONALIZATION

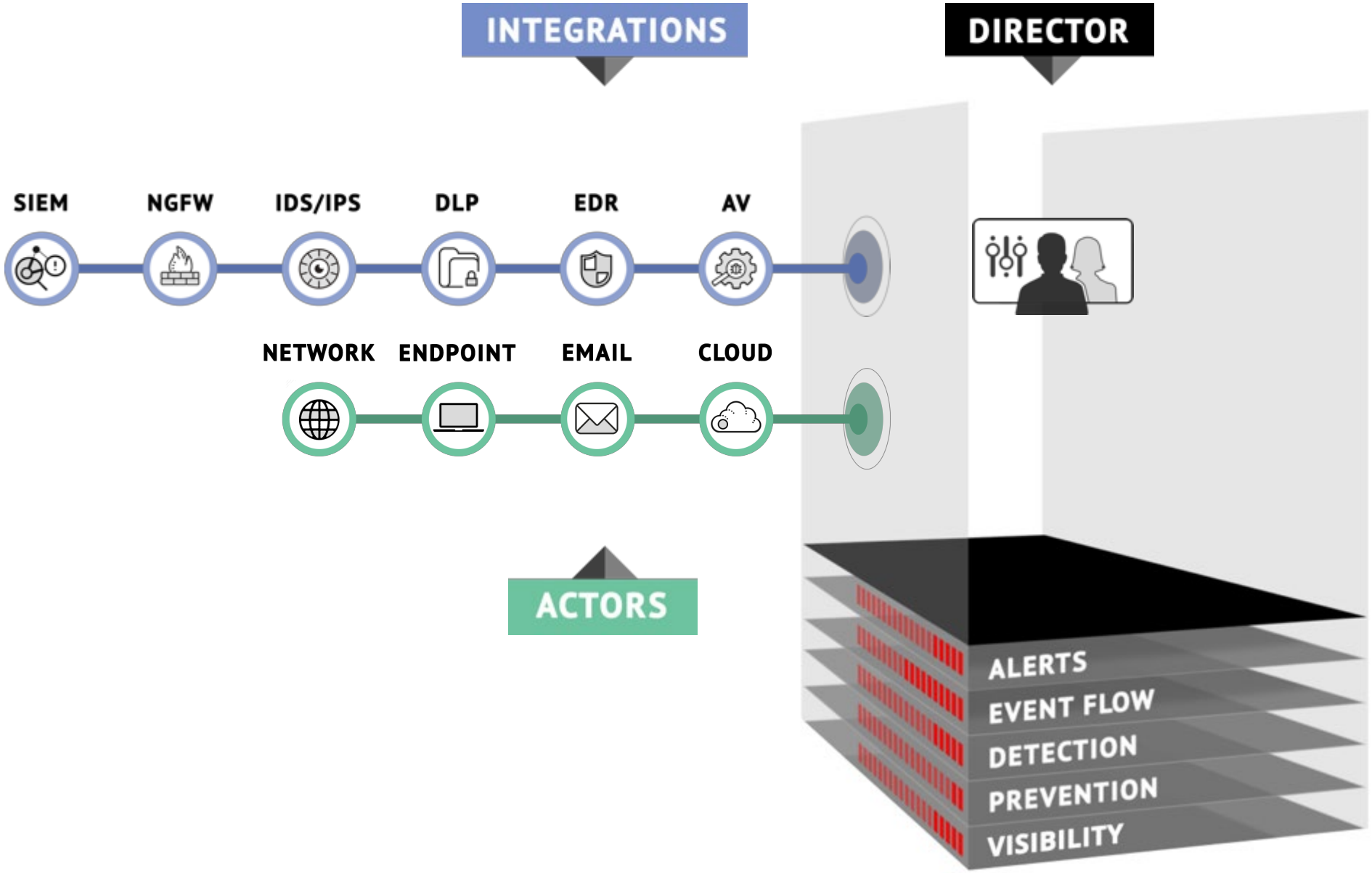
KNOWN GOOD BASELINE

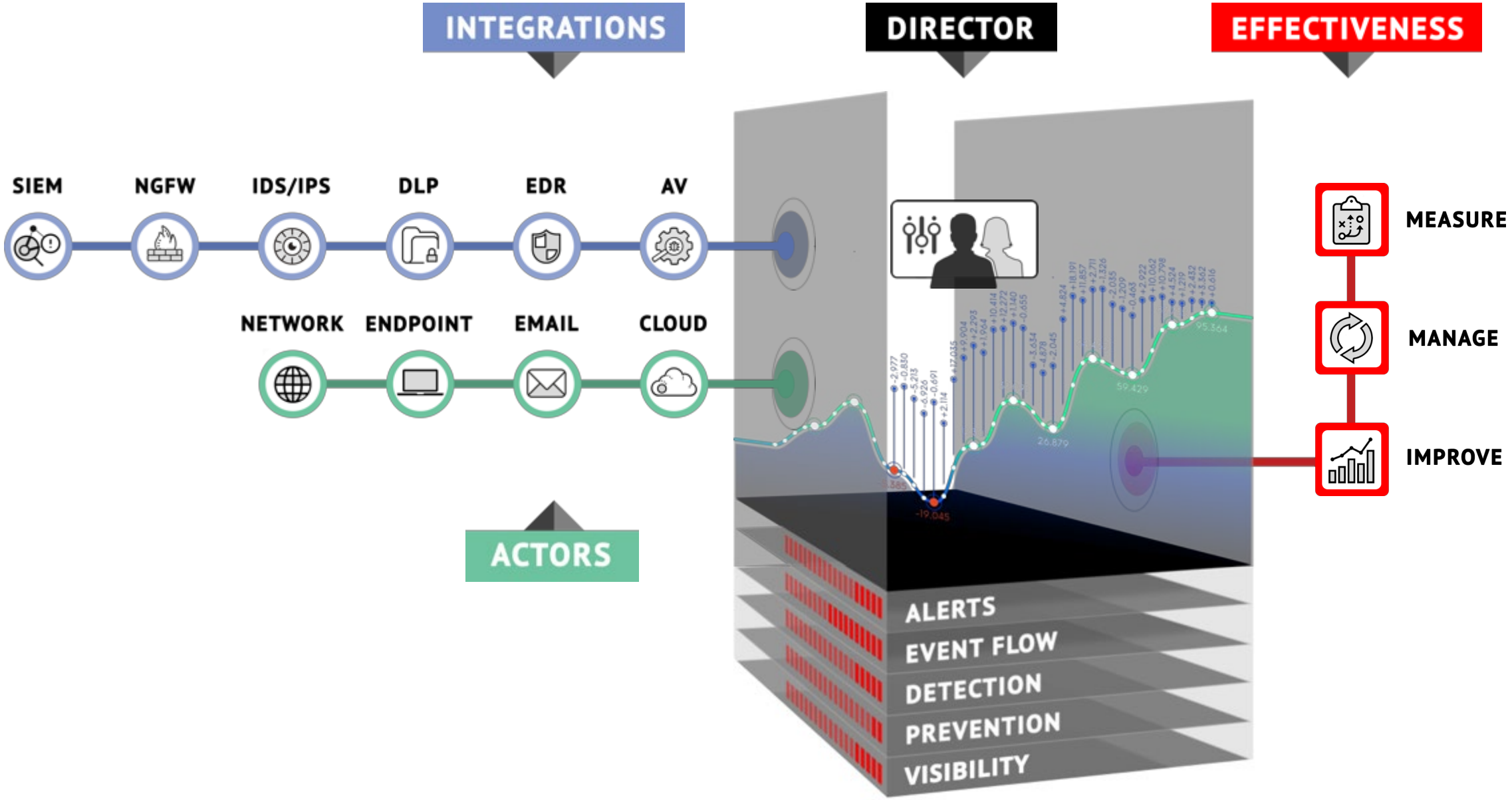
ENVIRONMENTAL DRIFT DETECTION


DIRECTOR

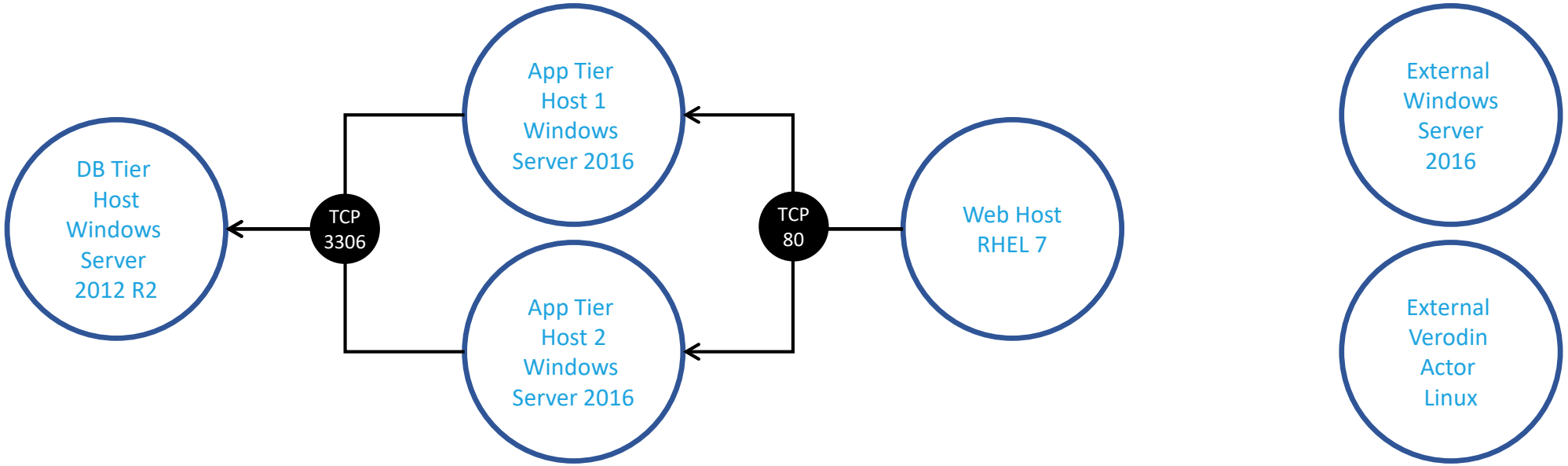

INTEGRATIONS
DIRECTOR
SIEM
NGFW
IDS/IPS
DLP
EDR
AV
ArcSight
ALIEN VAULT
CARBON BLACK
Check Point
CISCO
CROWDSTRIKE
CYLANCE
cybereason
FireEye
FORCEPOINT
elastic
LogRhythm
McAfee
Microsoft
mimecast
paloalto
proofpoint
Radar
RSA
SentinelOne
MANY MORE
splunk>
sumologic
Symantec
TippingPoint


INTEGRATIONS
DIRECTOR
SIEM
NGFW
IDS/IPS
DLP
EDR
AV
NETWORK
ENDPOINT
EMAIL
CLOUD
ACTORS


INTEGRATIONS
DIRECTOR
SIEM
NGFW
IDS/IPS
DLP
EDR
AV
NETWORK
ENDPOINT
EMAIL
CLOUD
ACTORS
ALERTS
EVENT FLOW
DETECTION
PREVENTION
VISIBILITY


INTEGRATIONS
DIRECTOR
EFFECTIVENESS
SIEM
NGFW
IDS/IPS
DLP
EDR
AV
NETWORK
ENDPOINT
EMAIL
CLOUD
ACTORS
ALERTS
EVENT FLOW
DETECTION
PREVENTION
VISIBILITY
MEASURE
MANAGE
IMPROVE

APPLICATION SETUP



DB Tier

App Tier

Web Tier

MySQL

Drupal™

NGINX

Verodin Actor

Verodin Actor

Verodin Actor

MITRE ATT&CK VISIBILITY

PRE-ATT&CK

ENTERPRISE ATT&CK

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

Initial access
Execution
Persistence
Privilege escalation
Defense evasion
Credential access
Discovery
Lateral movement
Collection
Exfiltration
Command & control

8 OUT OF 11

OF THE MITRE TACTICS
WERE TESTED AGAINST

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access

Execution

Persistence

Privilege escalation

Defense evasion

Credential access

Discovery

Lateral movement

Collection

Exfiltration

Command & control

EXECUTION TECHNIQUES

- Host CLI – Defense Evasion, Execution: RegAsm Bypass
- Host CLI – Defense Evasion, Execution: rundll32.exe
- Host CLI – Defense Evasion, Execution, Persistence, Privilege Escalation: New Service
- Host CLI – Execution, Credential Access: Remote Execution of Mimikatz using PaExec
- Host CLI – Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using Powershell
- Host CLI – Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using cU

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access

Execution

Persistence

Privilege escalation

Defense evasion

Credential access

Discovery

Lateral movement

Collection

Exfiltration

Command & control

PERSISTENCE TECHNIQUES

- Host CLI – Persistence: Scheduled Task
- Host CLI – Defense Evasion, Execution, Persistence, Privilege Escalation: New Service

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access
Execution
Persistence
Privilege escalation
Defense evasion
Credential access
Discovery
Lateral movement
Collection
Exfiltration
Command & control

PRIVILEGE ESCALATION TECHNIQUES

- Host CLI – Defense Evasion, Execution, Persistence, Privilege Escalation: New Service

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access
Execution
Persistence
Privilege escalation
Defense evasion
Credential access
Discovery
Lateral movement
Collection
Exfiltration
Command & control

DEFENSE EVASION TECHNIQUES

- Host CLI – Defense Evasion, Execution: RegAsm Bypass
- Host CLI – Defense Evasion, Execution: rundll32.exe
- Host CLI – Defense Evasion, Execution, Persistence, Privilege Escalation: New Service
- Host CLI – Defense Evasion: Removal of Network Share Connection
- Host CLI – Credential Access, Defense Evasion: Mimikatz W/ UPX Packing (2.1.1)
- Host CLI – Credential Access, Defense Evasion: Mimitaz W/ String Change

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access
Execution
Persistence
Privilege escalation
Defense evasion
Credential access
Discovery
Lateral movement
Collection
Exfiltration
Command & control

CREDENTIAL ACCESS TECHNIQUES

- Host CLI – Credential Access: Mimikatz (2.1.1)
- Host CLI – Credential Access: Mimikatz W/ 10MB padding (2.1.1)
- Host CLI – Credential Access, Defense Evasion: Mimikatz W/ UPX Packing (2.1.1)
- Host CLI – Credential Access, Defense Evasion: Mimitaz W/ String Change
- Host CLI – Execution, Credential Access: Remote Execution of Mimikatz using PaExec

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access

Execution

Persistence

Privilege escalation

Defense evasion

Credential access

Discovery

Lateral movement

Collection

Exfiltration

Command & control

DISCOVERY TECHNIQUES

- Host CLI – Discovery: Enumerate Local Administrators

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access
Execution
Persistence
Privilege escalation
Defense evasion
Credential access
Discovery
Lateral movement
Collection
Exfiltration
Command & control

LATERAL MOVEMENT TECHNIQUES

- Host CLI – Lateral Movement: Copy Mimikatz using Mapped Network Drive

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access

Execution

Persistence

Privilege escalation

Defense evasion

Credential access

Discovery

Lateral movement

Collection

Exfiltration

Command & control

EXFILTRATION TECHNIQUES

- Host CLI – Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using Powershell
- Host CLI – Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using cU

MITRE ATT&CK VISIBILITY

AREA OF FOCUS WITH MITRE

RECON | WEAPONIZE | DELIVER | EXPLOIT | CONTROL | EXECUTE | MAINTAIN

MITRE ATT&CK

Initial access

Execution

Persistence

Privilege escalation

Defense evasion

Credential access

Discovery

Lateral movement

Collection

Exfiltration

Command & control

APP TIER

VID	Action Name
A104-167	Host CLI - Credential Access: Mimikatz (2.1.1)
A104-166	Host CLI - Credential Access: Mimikatz W/ 10MB padding (2.1.1)
A104-165	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ UPX Packing (2.1.1)
A104-059	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ String Change
A104-351	Host CLI - Discovery: Enumerate Local Administrators
A104-218	Host CLI - Defense Evasion, Execution: RegAsm Bypass
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe
A104-010	Host CLI - Persistence: Scheduled Task
A104-164	Host CLI - Defense Evasion, Execution, Persistence, Privilege Escalation: New Service

APP TIER > APP TIER

VID	Action Name
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection

APP TIER > EXTERNAL

VID	Action Name
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec

EVALUATION METHODOLOGY

NSX	APPDEFENSE
DISABLED	DISABLED

VERODIN TESTS FOR BASELINE

NSX	APPDEFENSE
ENABLED	ENABLED IN DETECTION MODE

NSX PREVENT/ DETECT, AD DETECT

SELF LEARNING ENABLED

NSX	APPDEFENSE
ENABLED	ENABLED IN PROTECTION MODE

AD/NSX PREVENT/ DETECT MODE

Three-phase testing approach to establish and prove against known baseline

(2.1.1)

EVALUATION RESULTS

PHASE-1: NSX DISABLED AD DISABLED

		VERODIN TESTS FOR BASELINE		NSX PREVENT/ DETECT, AD DETECT	AD/NSX PREVENT/ DETECT MODE
APP TIER					
VID	**Action Name**	**DETECTED**	**BLOCKED**		
A104-167	Host CLI - Credential Access: Mimikatz (2.1.1)	●	●		
A104-166	Host CLI - Credential Access: Mimikatz W/ 10MB padding (2.1.1)	●	●		
A104-165	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ UPX Packing (2.1.1)	●	●		
A104-059	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ String Change	●	●		
A104-351	Host CLI - Discovery: Enumerate Local Administrators	●	●		
A104-218	Host CLI - Defense Evasion, Execution: RegAsm Bypass	●	●		
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe	●	●		
A104-010	Host CLI - Persistence: Scheduled Task	●	●		
A104-164	Host CLI - Defense Evasion, Execution, Persistence, Privilege Escalation: New Service	●	●		
APP TIER > APP TIER					
VID	**Action Name**				
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●		
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●		
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●		
APP TIER > EXTERNAL					
VID	**Action Name**				
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●		
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●		
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●		
APP TIER > DB					
VID	**Action Name**				
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●		
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●		
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●		
DB > EXTERNAL					
VID	**Action Name**				
A104-010	Host CLI - Persistence: Scheduled Task	●	●		
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe	●	●		
A104-345	Host CLI - Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using Powershell	●	●		
A104-344	Host CLI - Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using cU	●	●		

EVALUATION RESULTS

PHASE-2: NSX PREVENT AD DETECT

APP TIER

VID	Action Name	VERODIN TESTS FOR BASELINE: DETECTED	VERODIN TESTS FOR BASELINE: BLOCKED	NSX PREVENT/ DETECT, AD DETECT: DETECTED	NSX PREVENT/ DETECT, AD DETECT: BLOCKED	AD/NSX PREVENT/ DETECT MODE
A104-167	Host CLI - Credential Access: Mimikatz (2.1.1)	●	●	●	●	
A104-166	Host CLI - Credential Access: Mimikatz W/ 10MB padding (2.1.1)	●	●	●	●	
A104-165	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ UPX Packing (2.1.1)	●	●	●	●	
A104-059	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ String Change	●	●	●	●	
A104-351	Host CLI - Discovery: Enumerate Local Administrators	●	●	●	●	
A104-218	Host CLI - Defense Evasion, Execution: RegAsm Bypass	●	●	●	●	
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe	●	●	●	●	
A104-010	Host CLI - Persistence: Scheduled Task	●	●	●	●	
A104-164	Host CLI - Defense Evasion, Execution, Persistence, Privilege Escalation: New Service	●	●	●	●	

APP TIER > APP TIER

VID	Action Name					
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●	●	●	
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●	●	●	
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●	●	●	

APP TIER > EXTERNAL

VID	Action Name					
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●	●	●	
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●	●	●	
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●	●	●	

APP TIER > DB

VID	Action Name					
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●	●	●	
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●	●	●	
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●	●	●	

DB > EXTERNAL

VID	Action Name					
A104-010	Host CLI - Persistence: Scheduled Task	●	●	●	●	
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe	●	●	●	●	
A104-345	Host CLI - Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using Powershell	●	●	●	●	
A104-344	Host CLI - Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using cU	●	●	●	●	

EVALUATION RESULTS

PHASE-3: NSX PREVENT AD PREVENT

		VERODIN TESTS FOR BASELINE		NSX PREVENT/ DETECT, AD DETECT		AD/NSX PREVENT/ DETECT MODE	
APP TIER		DETECTED	BLOCKED	DETECTED	BLOCKED	**DETECTED**	**BLOCKED**
VID	**Action Name**						
A104-167	Host CLI - Credential Access: Mimikatz (2.1.1)	●	●	●	●	●	●
A104-166	Host CLI - Credential Access: Mimikatz W/ 10MB padding (2.1.1)	●	●	●	●	●	●
A104-165	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ UPX Packing (2.1.1)	●	●	●	●	●	●
A104-059	Host CLI - Credential Access, Defense Evasion: Mimikatz W/ String Change	●	●	●	●	●	●
A104-351	Host CLI - Discovery: Enumerate Local Administrators	●	●	●	●	●	●
A104-218	Host CLI - Defense Evasion, Execution: RegAsm Bypass	●	●	●	●	●	●
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe	●	●	●	●	●	●
A104-010	Host CLI - Persistence: Scheduled Task	●	●	●	●	●	●
A104-164	Host CLI - Defense Evasion, Execution, Persistence, Privilege Escalation: New Service	●	●	●	●	●	●
APP TIER > APP TIER							
VID	**Action Name**						
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●	●	●	●	●
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●	●	●	●	●
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●	●	●	●	●
APP TIER > EXTERNAL							
VID	**Action Name**						
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●	●	●	●	●
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●	●	●	●	●
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●	●	●	●	●
APP TIER > DB							
VID	**Action Name**						
A104-341	Host CLI - Lateral Movement: Copy Mimikatz using Mapped Network Drive	●	●	●	●	●	●
A104-342	Host CLI - Execution, Credential Access: Remote Execution of Mimikatz using PaExec	●	●	●	●	●	●
A104-343	Host CLI - Defense Evasion: Removal of Network Share Connection	●	●	●	●	●	●
DB > EXTERNAL							
VID	**Action Name**						
A104-010	Host CLI - Persistence: Scheduled Task	●	●	●	●	●	●
A104-096	Host CLI - Defense Evasion, Execution: rundll32.exe	●	●	●	●	●	●
A104-345	Host CLI - Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using Powershell	●	●	●	●	●	●
A104-344	Host CLI - Execution, Exfiltration: HTTP Exfil/Upload of PCI Data using cU	●	●	●	●	●	●

VERODIN

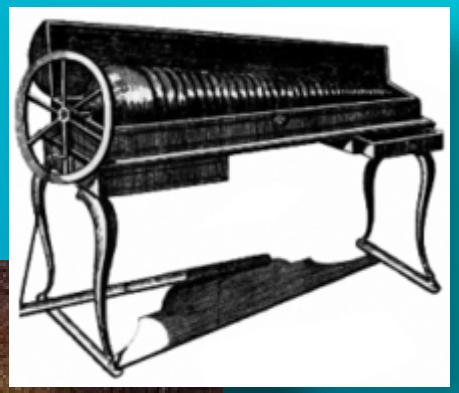
Christopher Key

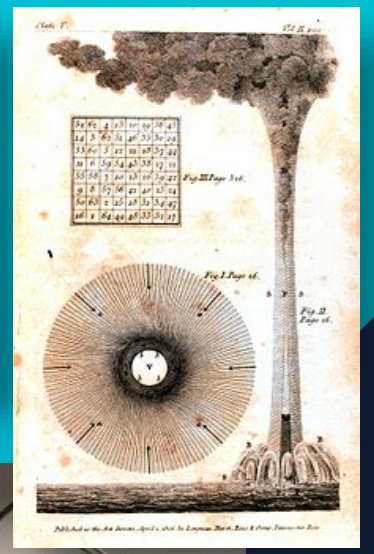
CEO & Co-Founder Verodin

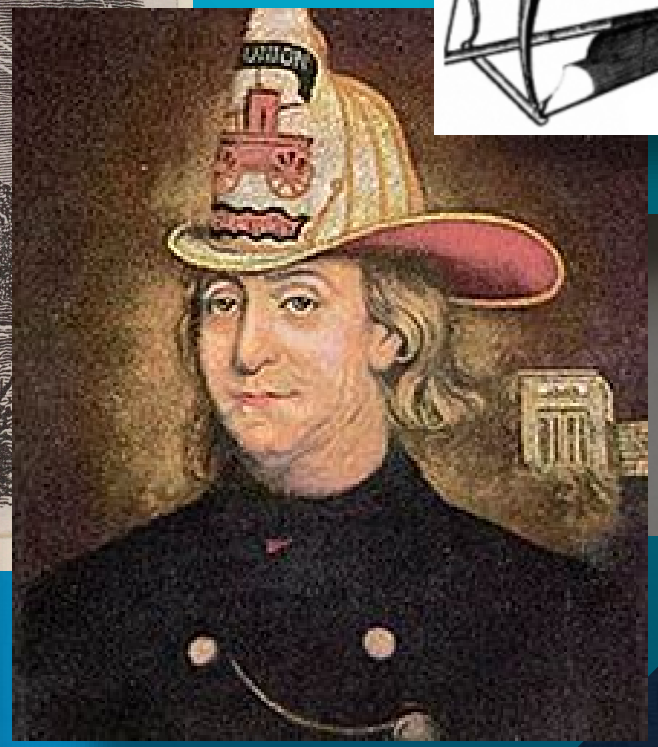
vmware

an Ounce of Prevention is worth a Pound of Cure

Benjamin Franklin







Unconventional Thinking Often Comes From Unconventional Sources

Unconventional Thinking Often Comes From
Unconventional Sources

Where Can You Learn More?

Watch

"Three Things the Security Industry Isn't Talking About (but Should Be)"

Thursday, Mar 07
04:00 P.M. - 04:25 P.M.
Pat Gelsinger, Chief Executive Officer, Vmware
Shannon Lietz, Director, Intuit

Experience

See these strategies in action at:

VMware Booth:
North Hall #5655

VERODIN at Booth #4214

Learn

Learn more at www.vmware.com/enterprise-security-solutions

vmware.com/go/service-defined-firewall

https://www.verodin.com

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SPO2-T08

Using the Cloud to Secure Versus Securing the Cloud

Tom Corn

SVP/GM Security Products
VMware
@therealtomcorn