



# Rethinking Cybersecurity for Healthcare

Chris Logan, MBA, CISSP  
Director Healthcare Industry Strategy  
VMware

## About Me

In the IT space for  
over 20 years



DoD, Higher  
Education,  
Banking and  
Healthcare

Last focus  
was  
Healthcare  
InfoSec

Digital Transformation is creating new opportunities not only for improved patient outcomes, but also the *business* of healthcare



## Target on Healthcare

Highly valuable data  
Complex environments  
Increasingly distributed  
Increasingly open  
Availability is priority



Ransomware

Malware

Insider Threats

Zero Day

# Current State

Growth in Yearly Breaches



7%

Over 360 in 2018

Source: <https://www.hipaajournal.com/healthcare-data-breach-statistics>, January 2019

Growth in Security Spend



10.2%  
(since 2017)

\$91.4 Billion in 2018

Source: IDC, Worldwide Semiannual Security Spending Guide, #US42570018, March 2018

Increase in Security Losses



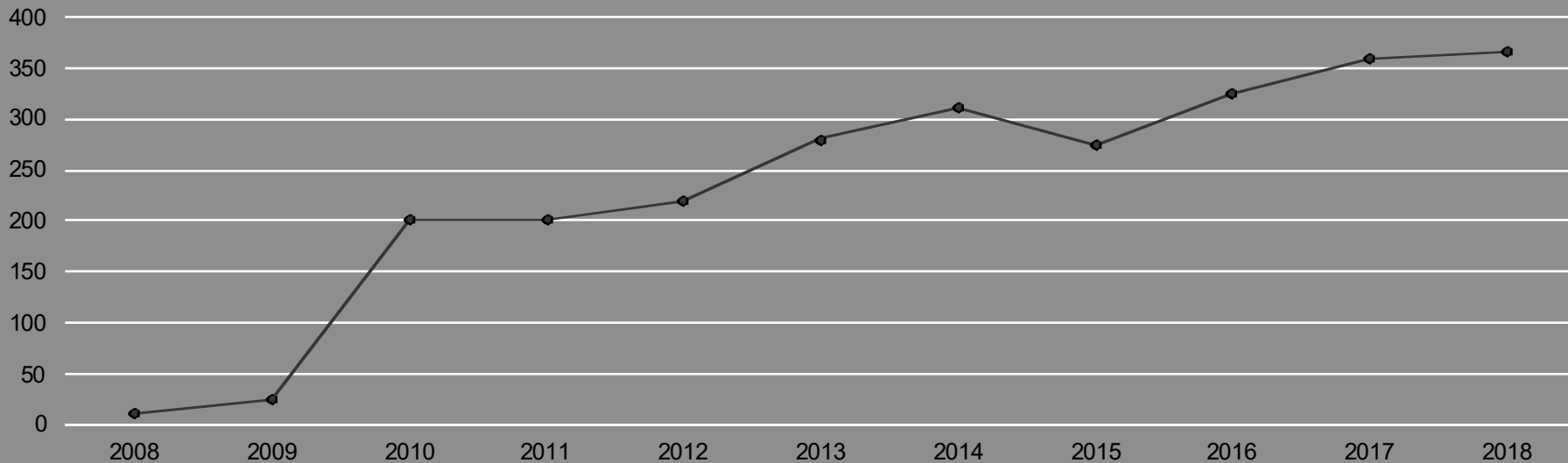
26%  
(since 2014)

\$600 Billion in 2017

Source: Center for Strategic and Int'l Studies, Economic Impact of Cybercrime, February, 2018

## Number of Healthcare Data Breaches by Year

Between 2009 and 2018 there have been 2,546 healthcare data breaches involving more than 500 records. Those breaches have resulted in the theft/exposure of 189,945,874 healthcare records. That equates to more than 59% of the population of the United States. Healthcare data breaches are now being reported at a rate of more than one per day.

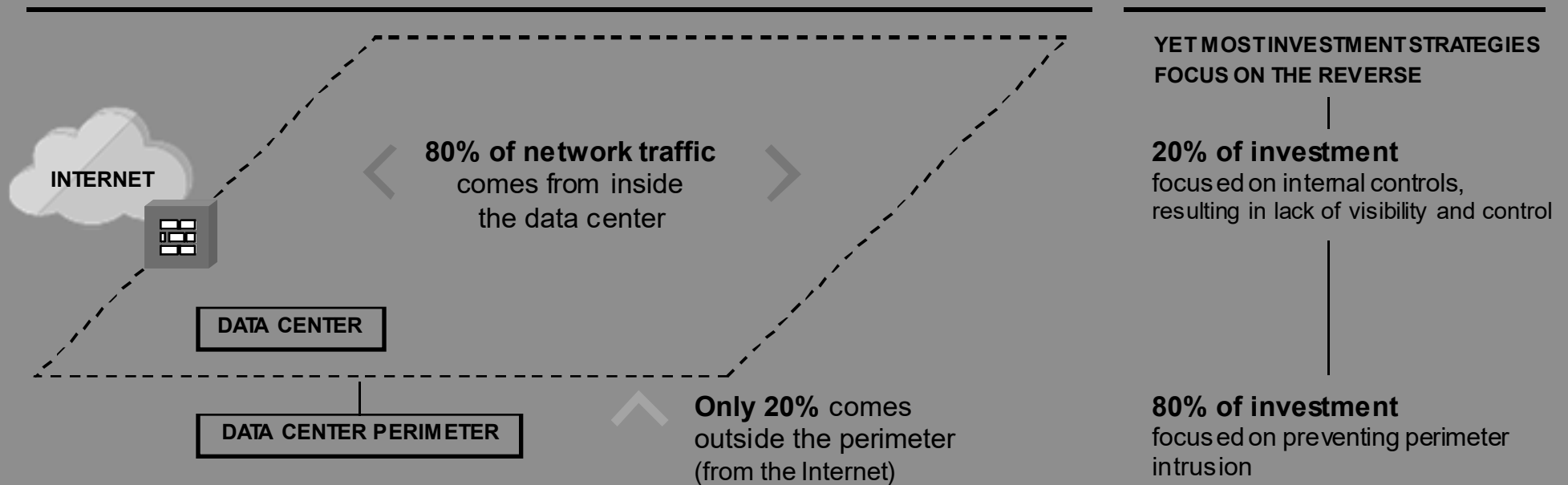


Source: <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

# Our Security Realities

- Security is a top priority, but investments are not aligned for success

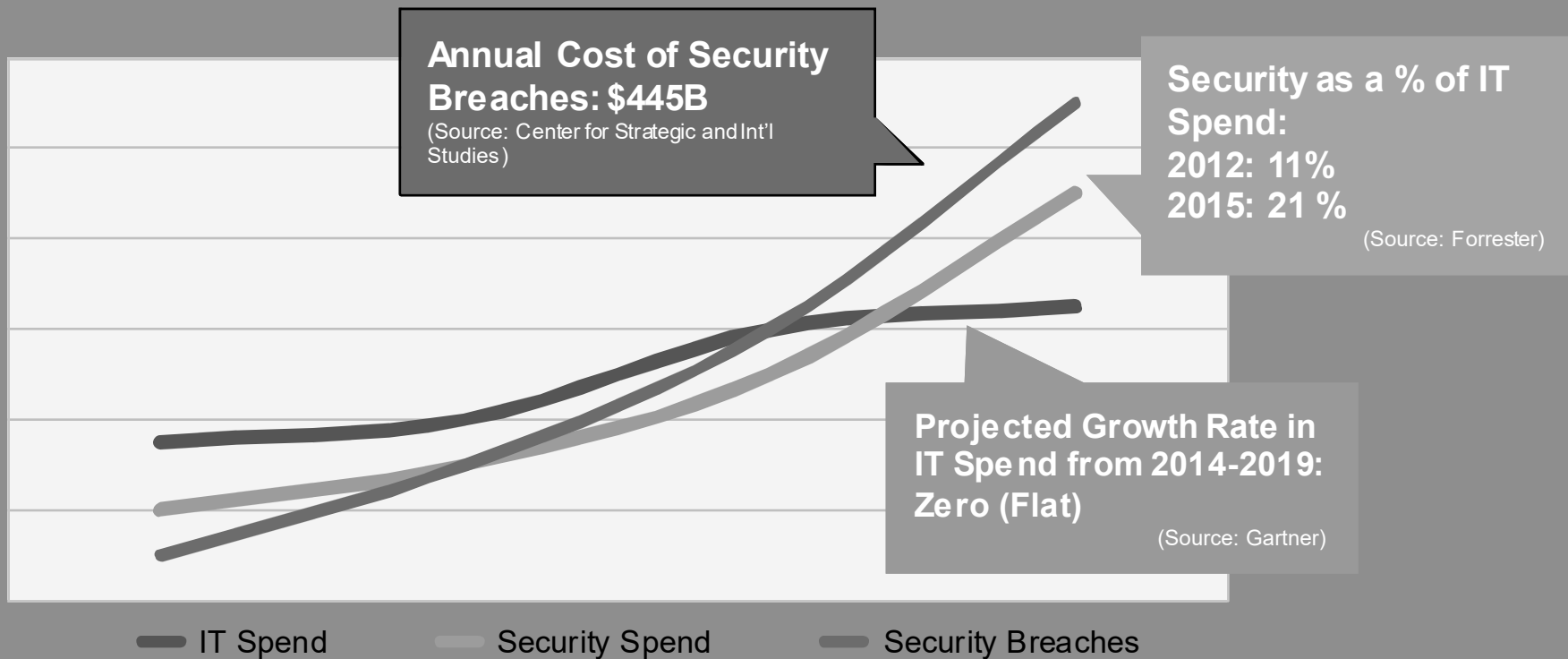
TODAY



We need a new strategy for security

# Digital Makes Reliance on Data Lucrative for Thieves

- Security investments are increasing, yet the costs of breaches are rising faster





## Digital Makes Reliance on Data Lucrative for Thieves

- Security investments are increasing, yet the cost of breaches are rising faster



Underfunding security  
isn't the problem.

# Transforming Cyber Security?

The image displays a comprehensive grid of cybersecurity vendors, organized into 18 distinct functional categories. Each category is represented by a box containing the logos of leading companies in that space. The categories include:

- Network Firewall:** Palo Alto Networks, Cisco, Fortinet, Juniper, H3C, Huawei, Mikrotik, SonicWall, WatchGuard, Check Point, Snort, Snort3, Snort-ng, Snort-Team, Snort-Community, Snort-Engine, Snort-Plugins, Snort-Tools, Snort-UI, Snort-Web, Snort-XML, Snort-JSON, Snort-REST, Snort-GraphQL, Snort-WebSocket, Snort-WebRTC, Snort-WebSockets, Snort-WebGL, Snort-WebGPU, Snort-WebAssembly, Snort-WebWorkers, Snort-WebVitals, Snort-WebFonts, Snort-WebImages, Snort-WebVideos, Snort-WebAudio, Snort-WebText, Snort-WebCode, Snort-WebData, Snort-WebEvents, Snort-WebErrors, Snort-WebWarnings, Snort-WebAlerts, Snort-WebNotifications, Snort-WebMessages, Snort-WebDialogs, Snort-WebModals, Snort-WebPopovers, Snort-WebToasts, Snort-WebSnackbars, Snort-WebAlerts, Snort-WebNotifications, Snort-WebMessages, Snort-WebDialogs, Snort-WebModals, Snort-WebPopovers, Snort-WebToasts, Snort-WebSnackbars.
- Network Monitoring:** BlueCat, XDR, IDS/IPS, Snort, Snort3, Snort-ng, Snort-Team, Snort-Community, Snort-Engine, Snort-Plugins, Snort-Tools, Snort-UI, Snort-Web, Snort-XML, Snort-JSON, Snort-REST, Snort-GraphQL, Snort-WebSocket, Snort-WebRTC, Snort-WebSockets, Snort-WebGL, Snort-WebGPU, Snort-WebAssembly, Snort-WebWorkers, Snort-WebVitals, Snort-WebFonts, Snort-WebImages, Snort-WebVideos, Snort-WebAudio, Snort-WebText, Snort-WebCode, Snort-WebData, Snort-WebEvents, Snort-WebErrors, Snort-WebWarnings, Snort-WebAlerts, Snort-WebNotifications, Snort-WebMessages, Snort-WebDialogs, Snort-WebModals, Snort-WebPopovers, Snort-WebToasts, Snort-WebSnackbars.
- Endpoint Protection & Anti-Virus:** McAfee, Symantec, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos.
- WAF & Application Security:** Akamai, Cloudflare, Imperva, Fortinet, Cisco, Palo Alto Networks, Arxan, Snyk, SonarQube, Checkmarx, SAST, DAST, SCA, IaC, Container Security, API Security, Bot Management, DDoS Protection, Cloud Managed Network, Zero Trust, SASE, SD-WAN, SD-Branch, SD-Wireless, SD-Perimeter, SD-Access, SD-Fabric, SD-Edge, SD-Cloud, SD-Data Center, SD-Application, SD-Device, SD-User, SD-Role, SD-Group, SD-Resource, SD-Service, SD-Process, SD-Task, SD-Workflow, SD-Event, SD-Alert, SD-Notification, SD-Message, SD-Dialog, SD-Modal, SD-Popup, SD-Toast, SD-Snackbar.
- Intrusion Prevention Systems:** Cisco, Fortinet, Palo Alto Networks, Snort, Snort3, Snort-ng, Snort-Team, Snort-Community, Snort-Engine, Snort-Plugins, Snort-Tools, Snort-UI, Snort-Web, Snort-XML, Snort-JSON, Snort-REST, Snort-GraphQL, Snort-WebSocket, Snort-WebRTC, Snort-WebSockets, Snort-WebGL, Snort-WebGPU, Snort-WebAssembly, Snort-WebWorkers, Snort-WebVitals, Snort-WebFonts, Snort-WebImages, Snort-WebVideos, Snort-WebAudio, Snort-WebText, Snort-WebCode, Snort-WebData, Snort-WebEvents, Snort-WebErrors, Snort-WebWarnings, Snort-WebAlerts, Snort-WebNotifications, Snort-WebMessages, Snort-WebDialogs, Snort-WebModals, Snort-WebPopovers, Snort-WebToasts, Snort-WebSnackbars.
- Endpoint Detection & Response:** CrowdStrike, SentinelOne, Microsoft Defender, Microsoft Sentinel, Palo Alto Networks, Cisco, Fortinet, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee.
- Vulnerability Assessment:** Rapid7, Qualys, Snyk, SonarQube, Checkmarx, SAST, DAST, SCA, IaC, Container Security, API Security, Bot Management, DDoS Protection, Cloud Managed Network, Zero Trust, SASE, SD-WAN, SD-Branch, SD-Wireless, SD-Perimeter, SD-Access, SD-Fabric, SD-Edge, SD-Cloud, SD-Data Center, SD-Application, SD-Device, SD-User, SD-Role, SD-Group, SD-Resource, SD-Service, SD-Process, SD-Task, SD-Workflow, SD-Event, SD-Alert, SD-Notification, SD-Message, SD-Dialog, SD-Modal, SD-Popup, SD-Toast, SD-Snackbar.
- Unified Threat Management:** Fortinet, Cisco, Palo Alto Networks, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee.
- SIEM:** Splunk, IBM, LogRhythm, Elastic, Microsoft Sentinel, Palo Alto Networks, Cisco, Fortinet, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee.
- Security Incident Response:** Rapid7, Palo Alto Networks, Cisco, Fortinet, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee.
- Other Categories:** Various other vendors including MOCANA, ARGUS, ARM, SecuriThings, CloudView, KActive, Splunk, TIBCO, Wipro, IBM, LogRhythm, Elastic, Microsoft Sentinel, Palo Alto Networks, Cisco, Fortinet, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee, Trend Micro, Avast, AVG, Avira, BitDefender, ESET, Kaspersky, Panda, Sophos, Symantec, McAfee.

Without context, our  
security strategies risk  
always being a step  
behind

The biggest threat  
to security is the  
hyper-focus on  
security threats.

## Reactive Vs. Preventive

Reactive:  
Chasing Threats

Preventive:  
Reduce Attack Surface

# Where Do We Currently Focus our Time, Investment and Innovation?

80%

of Enterprise IT's investment in security\*

72%

of Venture Capital investment in security start-ups\*\*

Reactive

Preventive

What Has the Biggest Impact on Reducing Risk?

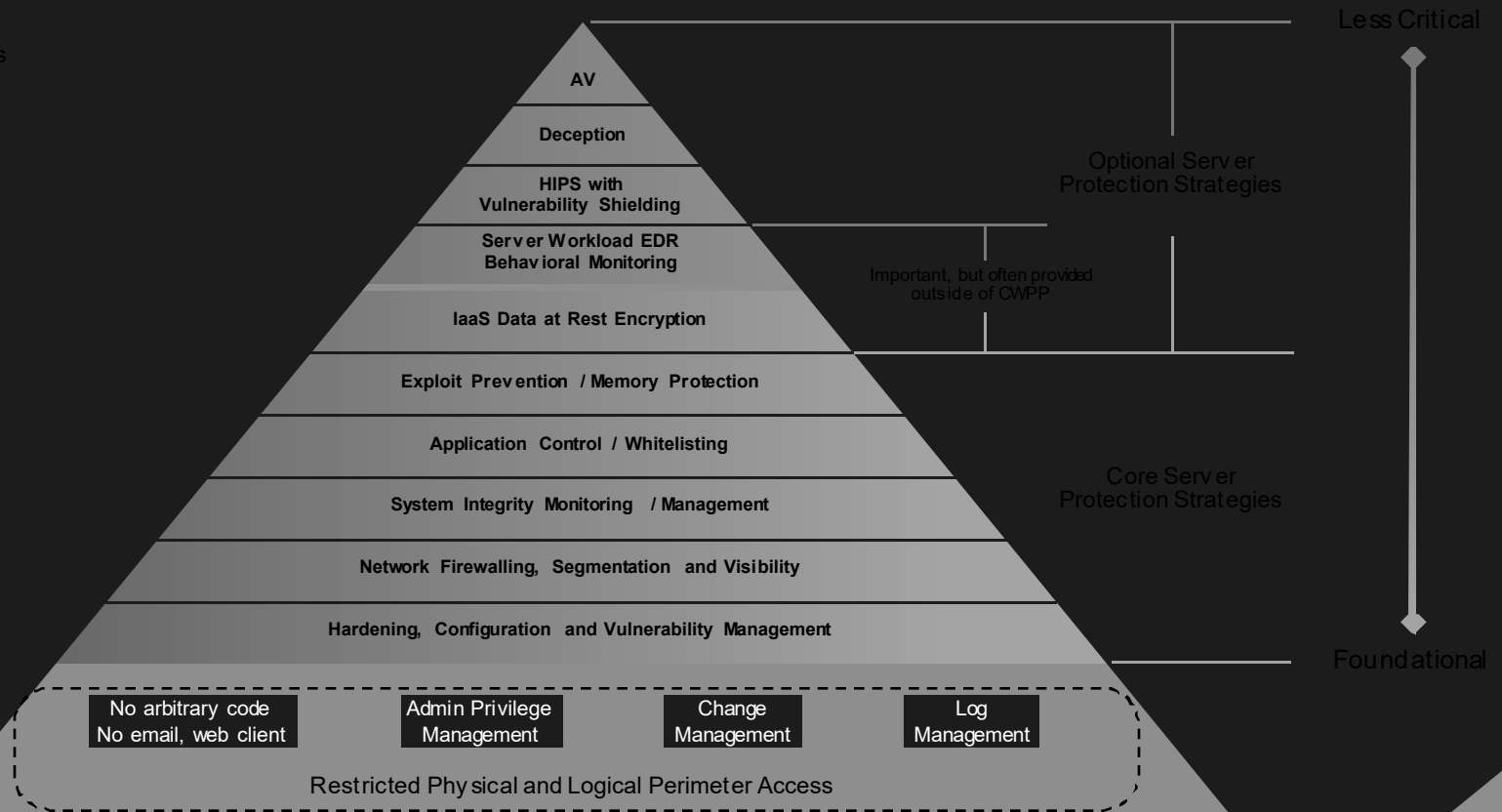


Reactive

Preventive

# Gartner: Cloud Workload Protection Controls Hierarchy

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



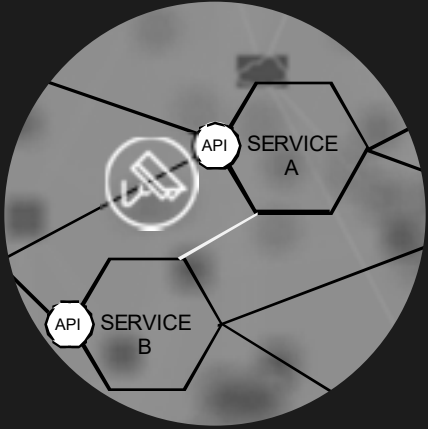
Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, March 26th 2018. Gartner does not endorse any vendor, product, or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. 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.



‘Application Awareness’  
lacks awareness of  
applications.



vmware®



Your most important  
security product won't  
be a security product.

# Transforming Security As We Know It

The image displays a comprehensive grid of security vendor logos, organized into various categories. The categories and their associated vendors are as follows:

- Network Firewall:** Check Point, Palo Alto Networks, Fortinet, Cisco, Juniper, HPE, Dell, Arista, and others.
- Network Monitoring:** BlueCat, XIRIA, IBM, and others.
- Endpoint Protection & Anti-Virus:** McAfee, Symantec, Trend Micro, Avast, Avira, and others.
- WAF & Application Security:** Akamai, Imperva, Cloudflare, and others.
- Intrusion Prevention Systems:** Palo Alto Networks, Fortinet, Cisco, and others.
- Endpoint Detection & Response:** CrowdStrike, SentinelOne, Microsoft, and others.
- Vulnerability Assessment:** McAfee, Rapid7, Veracode, and others.
- Unified Threat Management:** Fortinet, Endian, Palo Alto Networks, and others.
- SIEM:** Splunk, Tenable, IBM, and others.
- Security Incident Response:** Ghekarite, Proofpoint, and others.
- Other Security Solutions:** SailPoint, Symantec, Lookout, Secureworks, Arista, Carbon Black, Pingidentity, Okta, and others.

Several logos are highlighted with black boxes, including: Check Point, Palo Alto Networks, Fortinet, Akamai, Imperva, McAfee, Rapid7, Veracode, Splunk, Tenable, Symantec, Lookout, Secureworks, Arista, Carbon Black, Pingidentity, Okta, and Qualys.

# Security Requires Sharp Focus

1

**REDUCE  
THE ATTACK  
SURFACE**

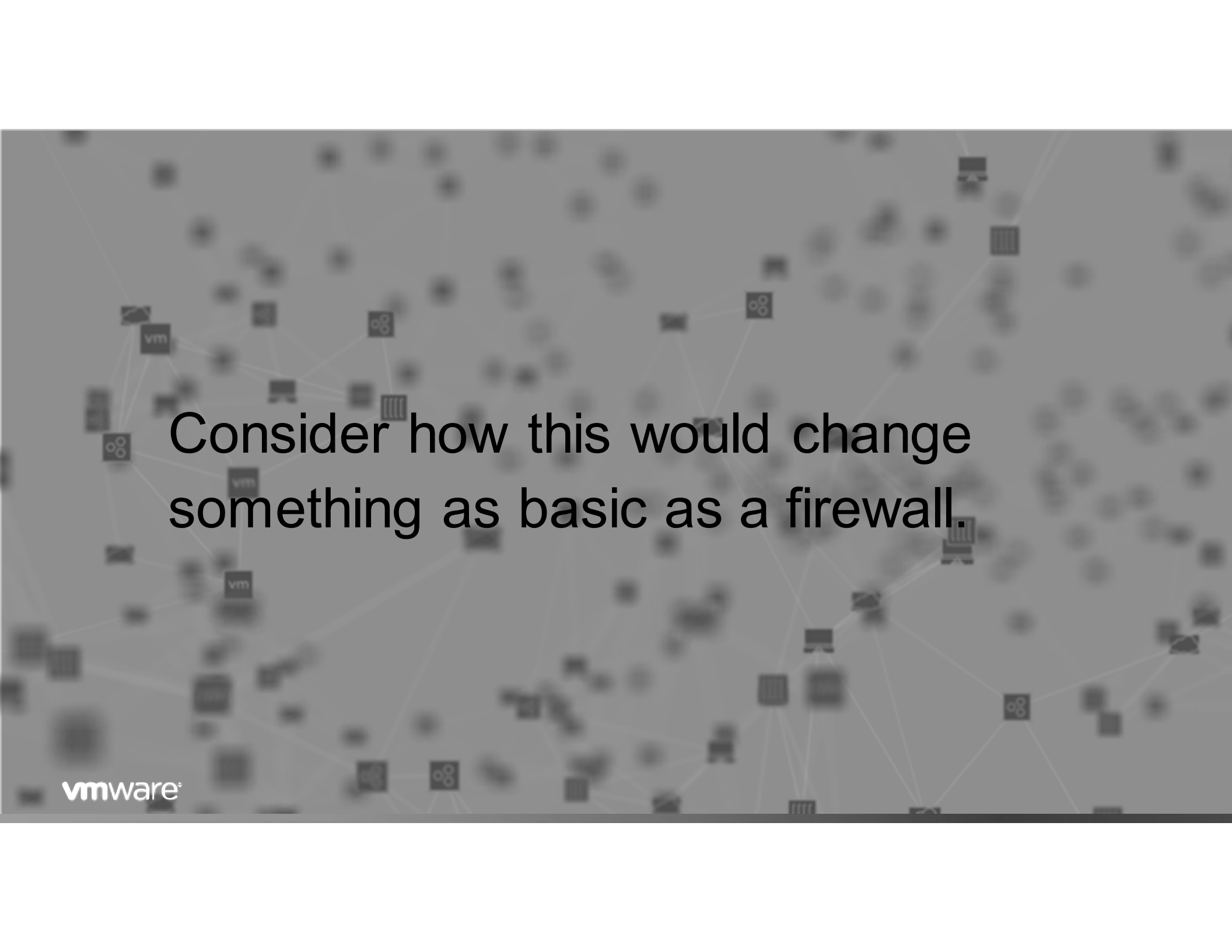
2

**SECURE  
APPLICATIONS  
AND DATA**

3

**MAKE  
SECURITY  
INTRINSIC**

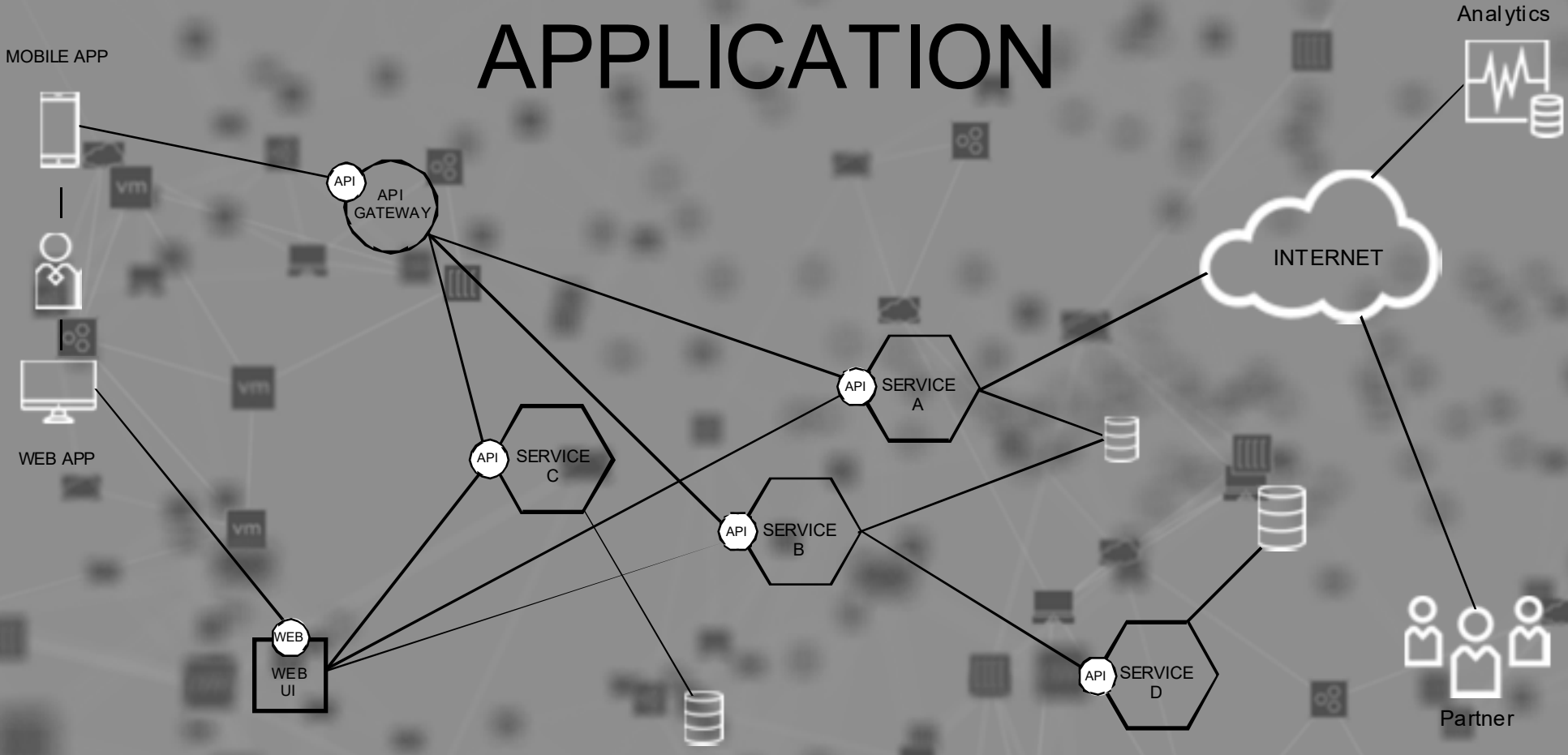
What does this shift in  
thinking look like?

A complex network diagram with various nodes and connections, overlaid with a semi-transparent gray box containing text. The nodes include icons for virtual machines (vm), servers, and other network components, all interconnected by a web of lines. The background is a light gray with a subtle pattern of these network elements.

Consider how this would change something as basic as a firewall.

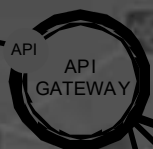


# APPLICATION



# KNOWN-GOOD

MOBILE APP



Analytics

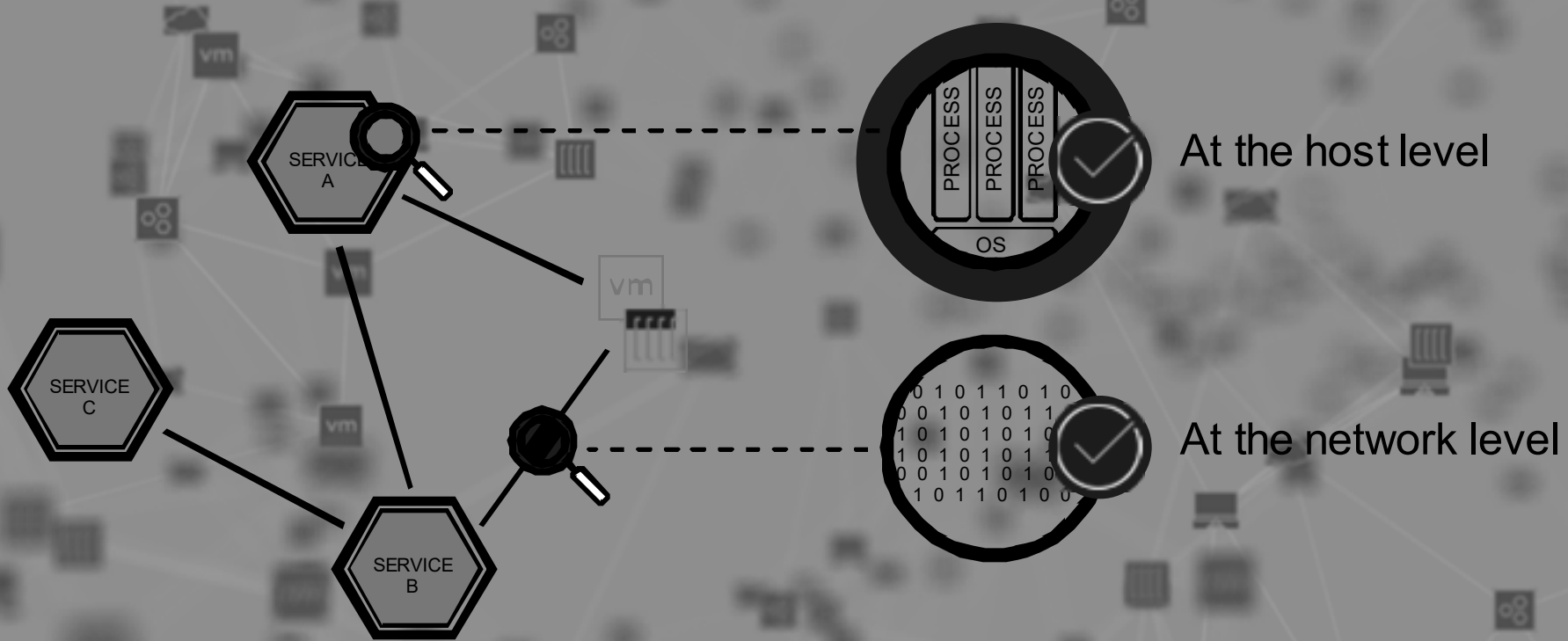


Partner

# KNOWN-GOOD



# KNOWN-GOOD



# IT LEARNS FROM ALL HOSTS

[GLOBAL MACHINE LEARNING]



**IT KNOWS  
THE HOST**

[IT BOOTED IT]



**IT IS OUTSIDE  
THE HOST**

[SUPER ROOT]



**IT IS  
EVERYWHERE**

[DISTRIBUTED SERVICES]

**IT LEARNS FROM  
ALL HOSTS**

[GLOBAL MACHINE LEARNING]



**Service-Defined**



**IT KNOWS  
THE HOST**

[IT BOOTED IT]

**IT IS OUTSIDE  
THE HOST**

[SUPER ROOT]

**IT IS  
EVERYWHERE**

[DISTRIBUTED SERVICES]



It dramatically reduces the attack surface

1,000,000,000,000,000

# Future Security Considerations for Healthcare - Actions You Can Take Immediately

**Invest in Prevention**

**Focus on Applications**

**Make Security Intrinsic**





# Thank You