

# 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

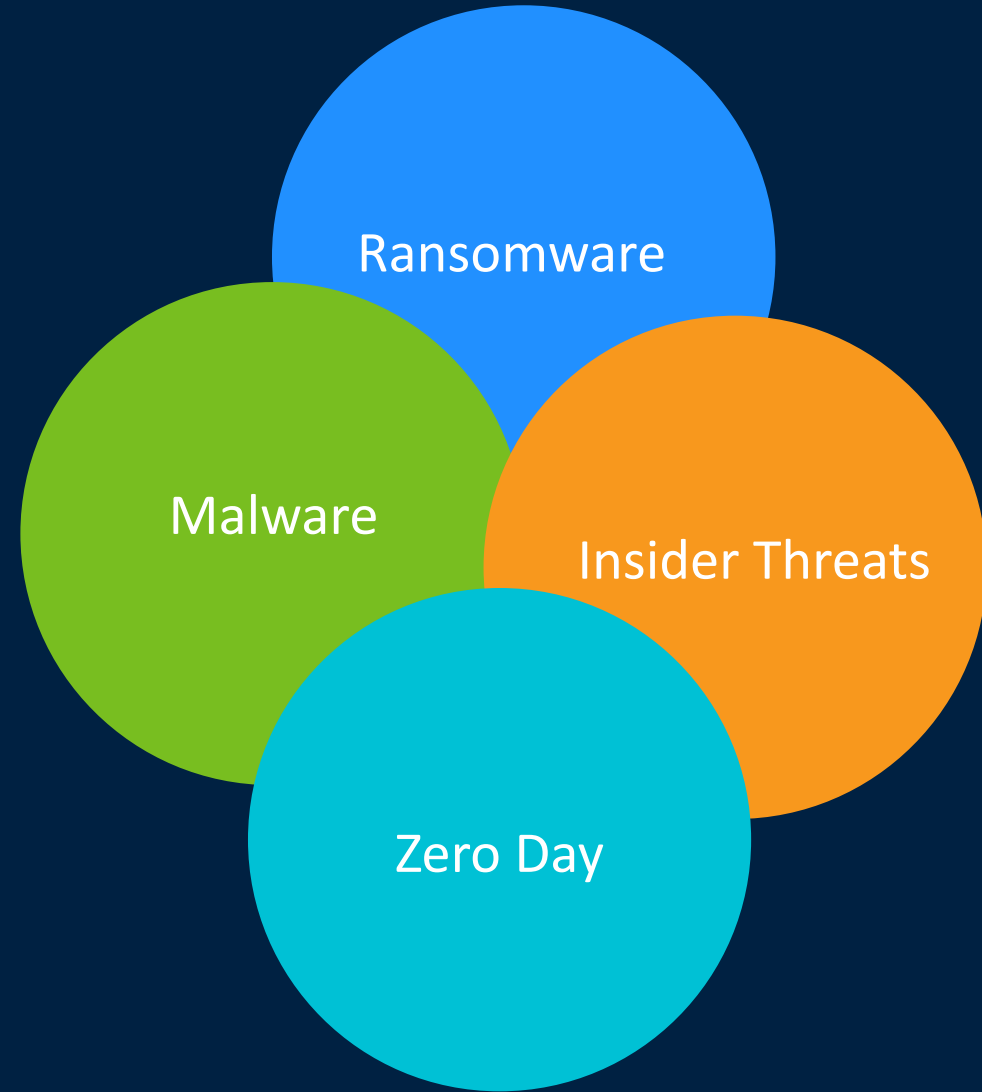


Digital Transformation is creating new opportunities not only for improved patient outcomes, but also the *business* of healthcare



# Target on Healthcare

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



# 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



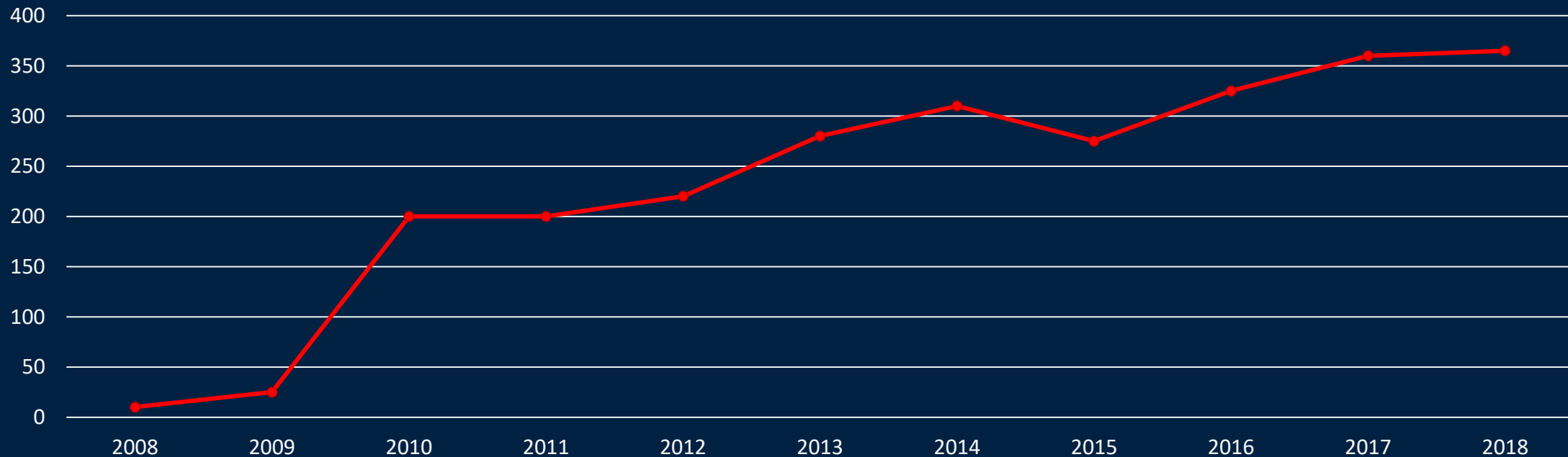
26%  
(since 2014)

\$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.

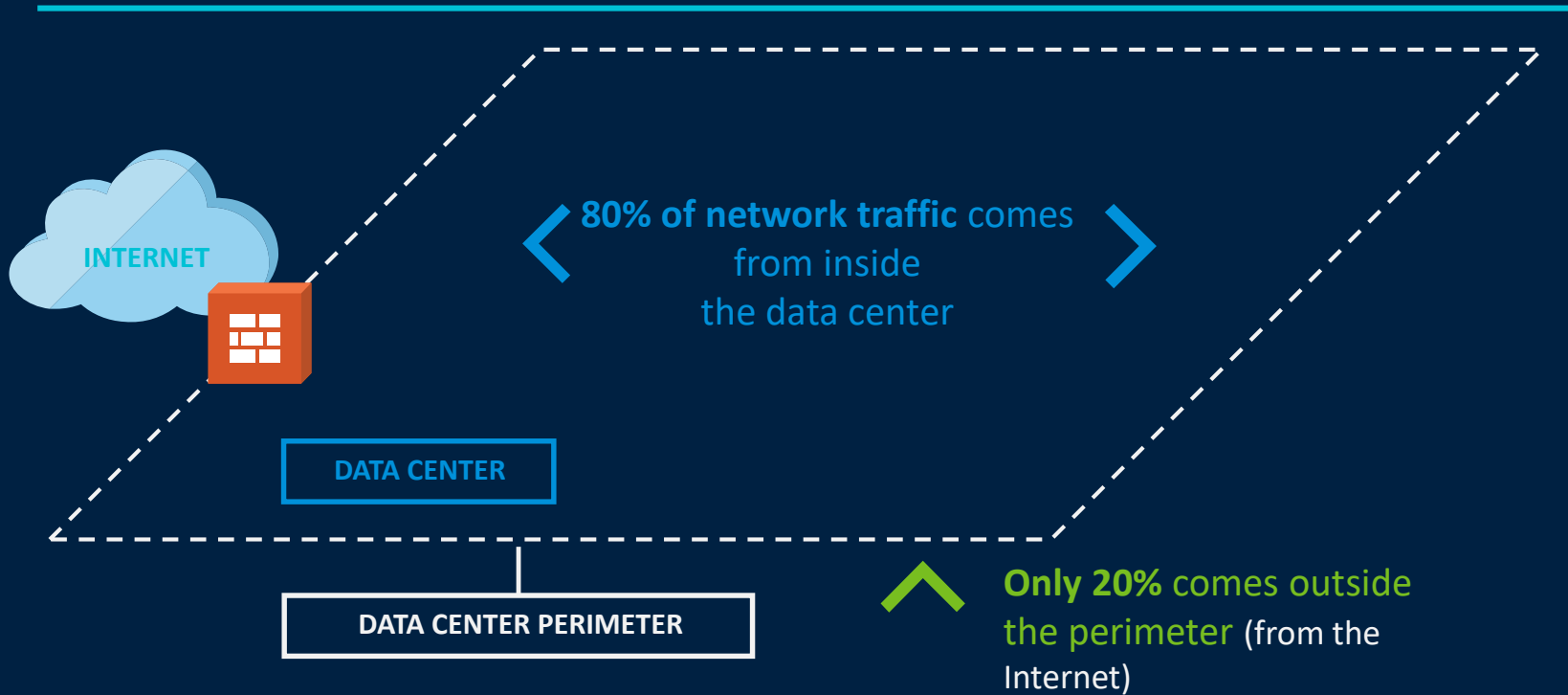


Source: <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

# Our Security Realities

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

TODAY



YET MOST INVESTMENT STRATEGIES FOCUS ON THE REVERSE

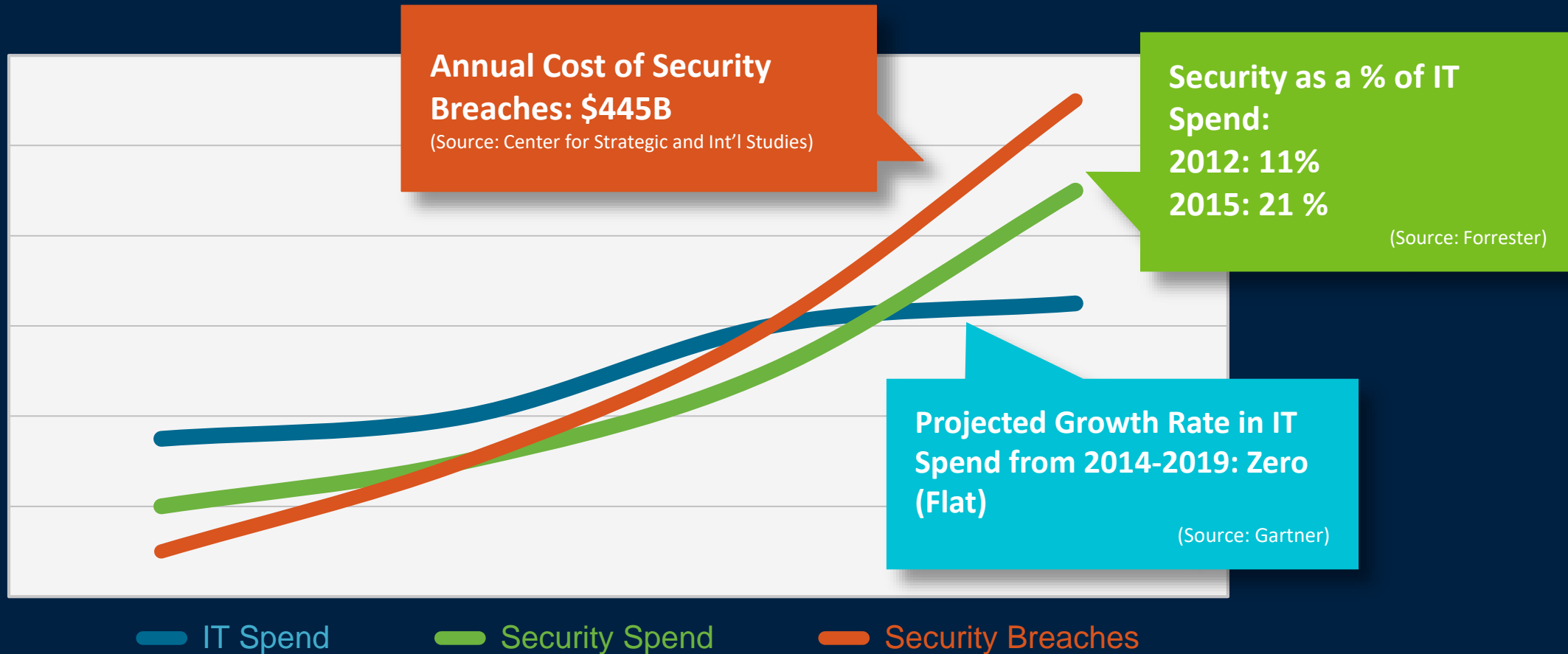
20% of investment focused on internal controls, resulting in lack of visibility and control

80% of investment focused on preventing perimeter intrusion

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

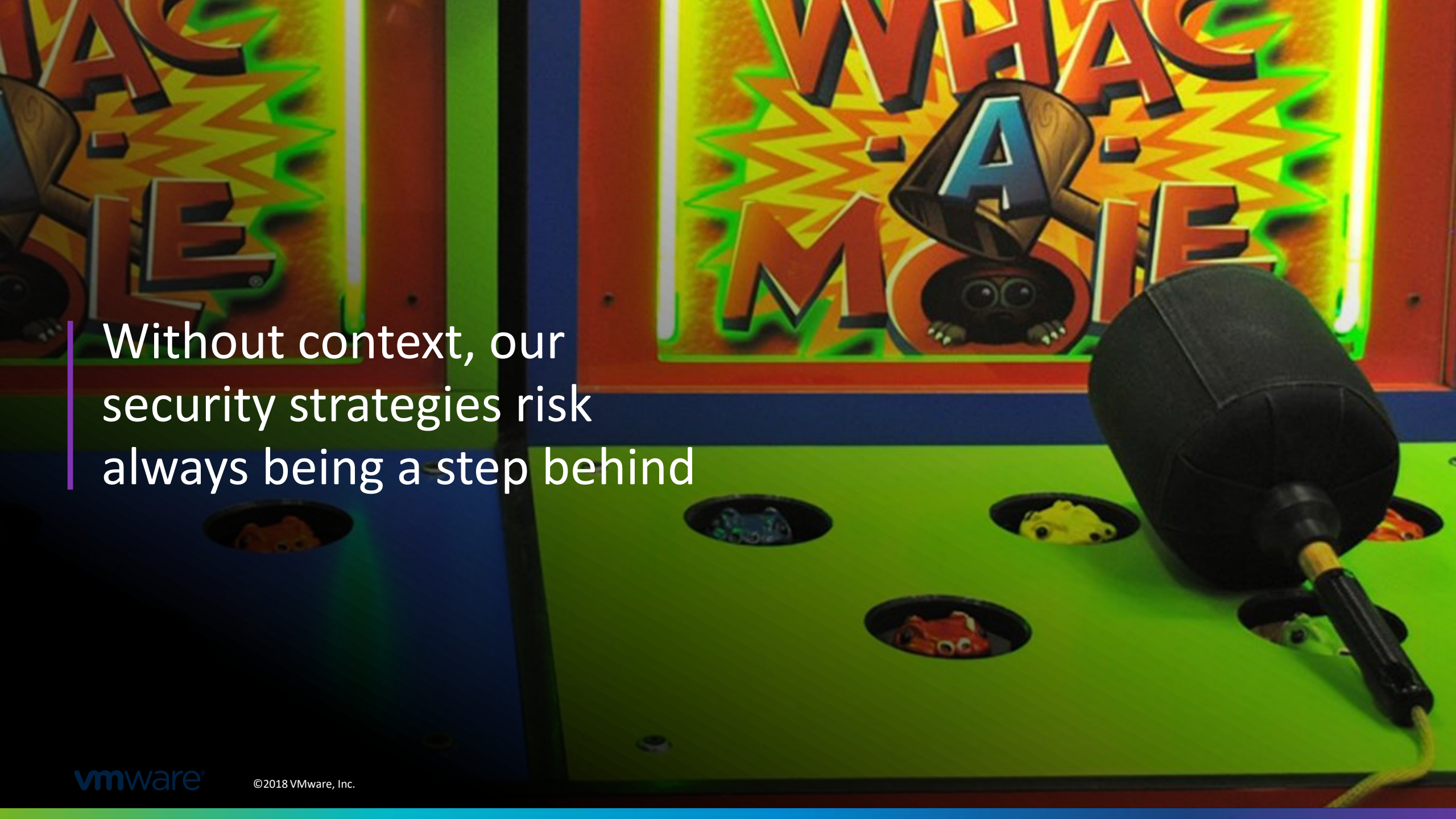


Underfunding security  
isn't the problem.

# Transforming Cyber Security?

The image displays a comprehensive grid of cybersecurity vendors, organized into 21 distinct functional categories. Each category is represented by a rectangular box containing the logos of leading companies in that space. The categories include:

- Network Firewall:** Check Point, Palo Alto Networks, Juniper, Fortinet, Cisco, etc.
- Network Monitoring:** Blue Coat, Cisco, Xixia, StillSecure, etc.
- Endpoint Protection & Anti-Virus:** McAfee, Symantec, Avast, Trend Micro, etc.
- WAF & Application Security:** Akamai, Cloudflare, Imperva, etc.
- Intrusion Prevention Systems:** Snort, Snort3, Suricata, etc.
- Endpoint Detection & Response:** CrowdStrike, SentinelOne, Microsoft Defender, etc.
- Vulnerability Assessment:** Rapid7, Qualys, Nessus, etc.
- Unified Threat Management:** Palo Alto Networks, Fortinet, Cisco, etc.
- SIEM:** Splunk, IBM QRadar, Microsoft Sentinel, etc.
- Security Incident Response:** Rapid7, Palo Alto Networks, etc.
- Other categories:** Identity management (Okta, Ping Identity), Cloud security (Sift Science, Cloudflare), and various specialized security solutions.



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

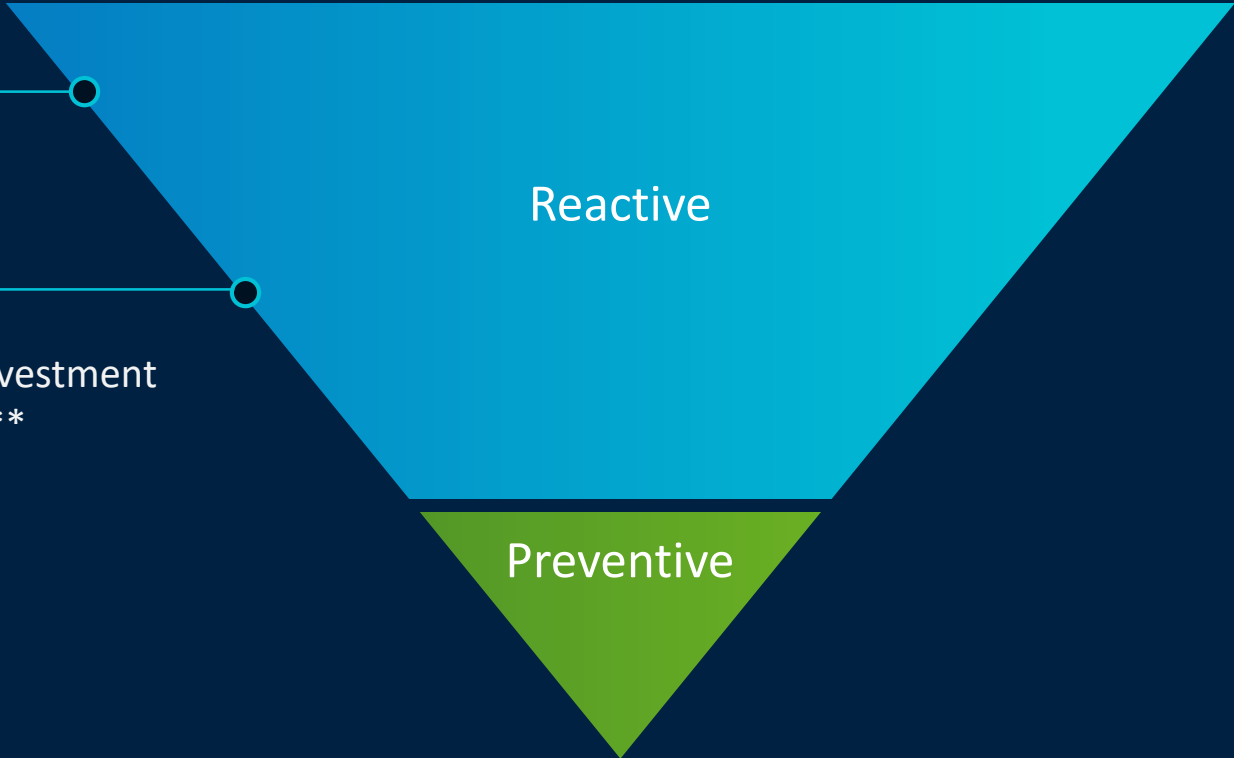
# Where Do We Currently Focus our Time, Investment and Innovation?

80%

of Enterprise IT's investment in security\*

72%

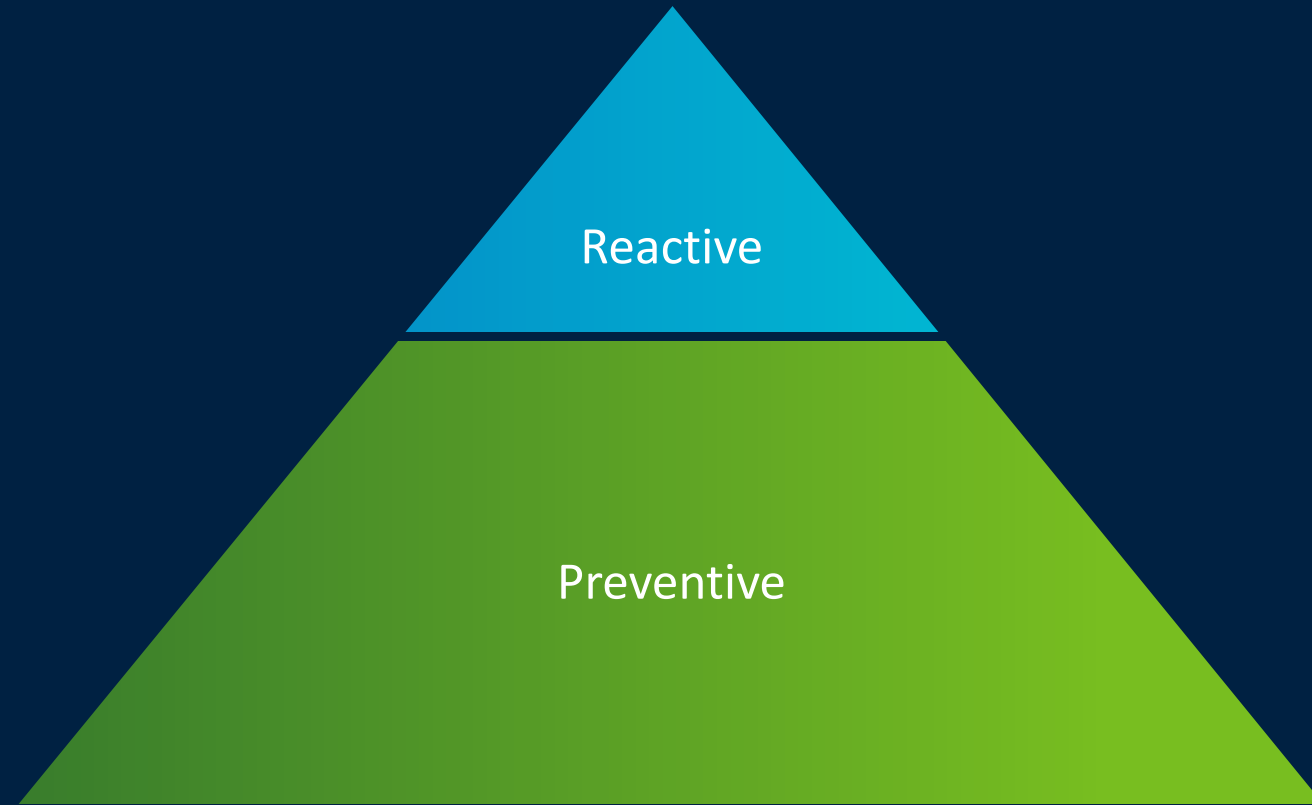
of Venture Capital investment in security start-ups\*\*



\*Source: VMware Analysis

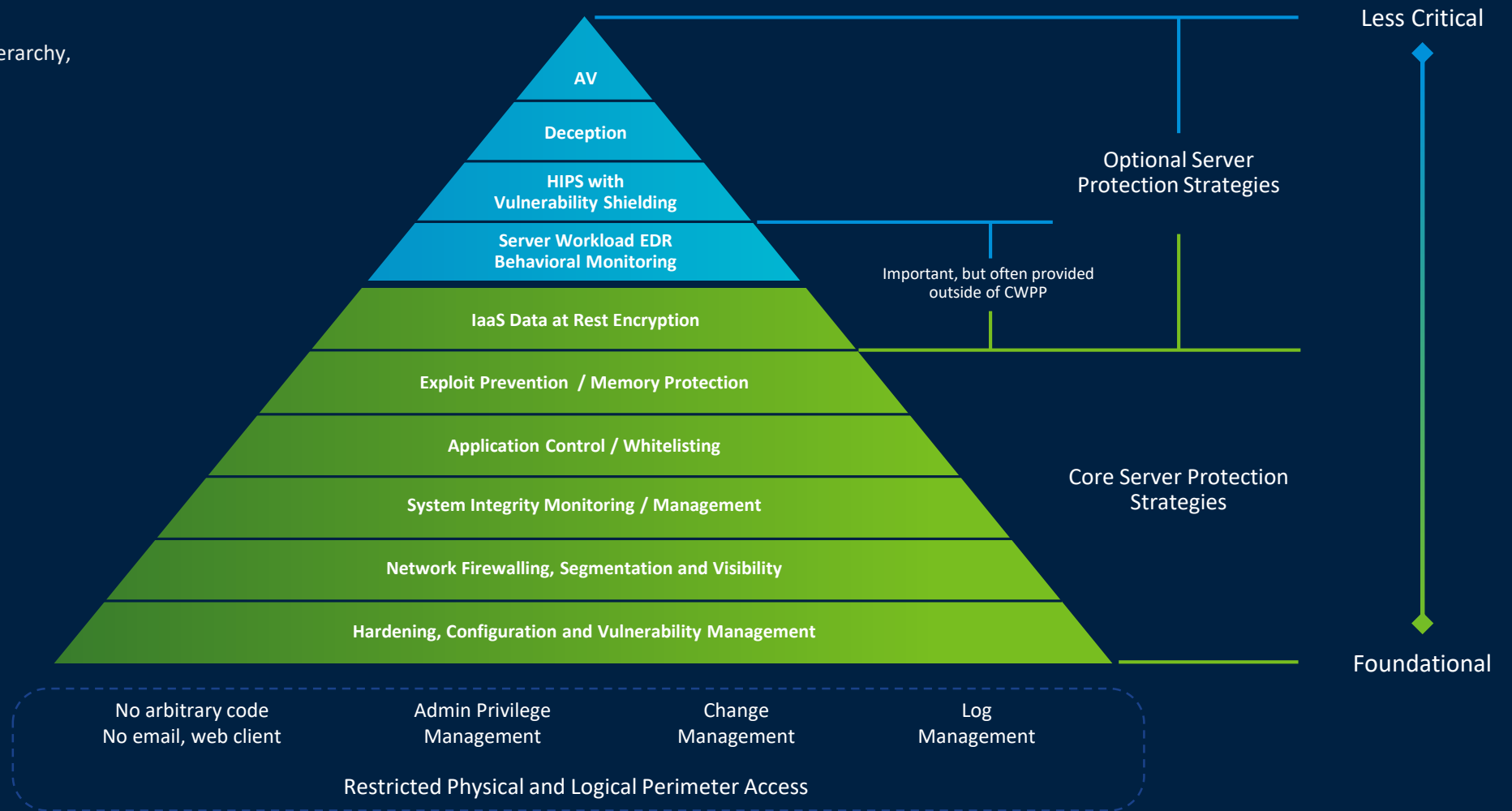
\*\*Source: 2018 Cyber Defenders Report and 2017 Cyber Defenders Report, CB Insights (2019 and 2018)

# What Has the Biggest Impact on Reducing Risk?



# 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.





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

# Transforming Security As We Know It



# Security Requires Sharp Focus

1

**REDUCE THE  
ATTACK  
SURFACE**

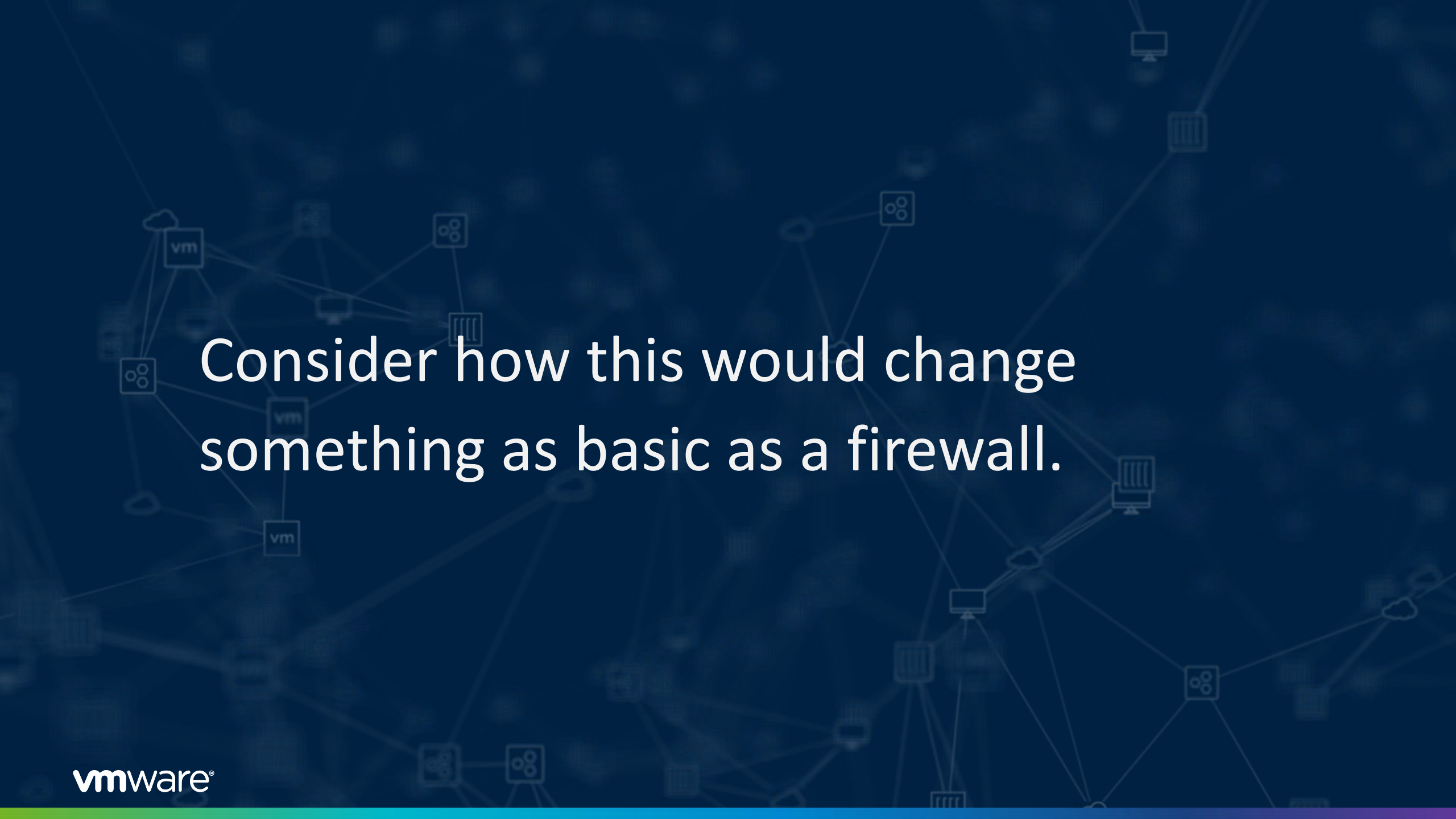
2

**SECURE  
APPLICATIONS  
AND DATA**

3

**MAKE  
SECURITY  
INTRINSIC**

What does this shift in  
thinking look like?

A complex network diagram is visible in the background, consisting of various nodes connected by lines. Some nodes are labeled 'vm', and others represent different types of network components like servers, clouds, and routers. The overall theme is network architecture and virtualization.

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

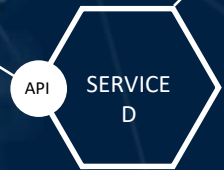
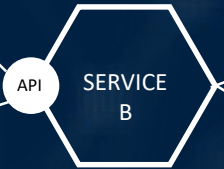
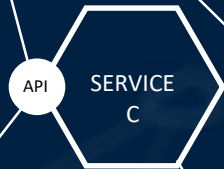
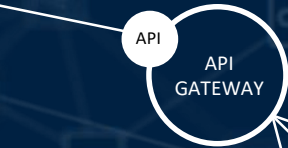


# APPLICATION

MOBILE APP



WEB APP



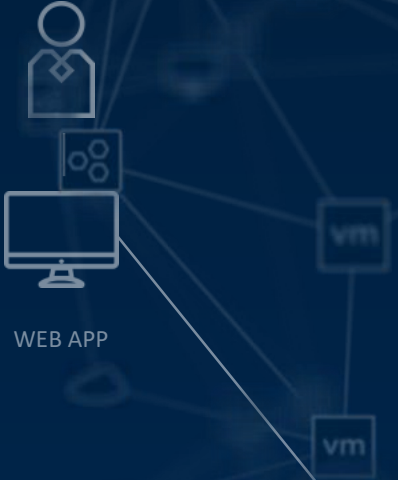
Analytics



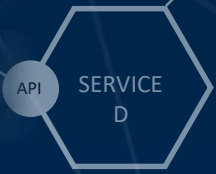
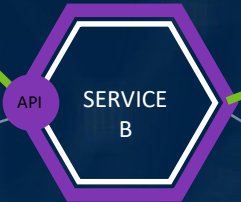
Partner

# KNOWN-GOOD

MOBILE APP



WEB 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]

A complex network diagram with various nodes (squares, circles, clouds) and connecting lines, set against a dark blue background. The nodes are interconnected, forming a dense web of connections.

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