

**DELL**Technologies /Forum

# REAL TRANSFORMATION

GLOBAL SPONSORS



# Cybersecurity: Prevention or Cure?

Dell Technology Forum, London

Scott McKinnon  
Security Architect  
VMware  
November 2019

1

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

# Reactive Vs. Preventive

Reactive:  
Chasing Threats

Preventive:  
Reduce Attack Surface



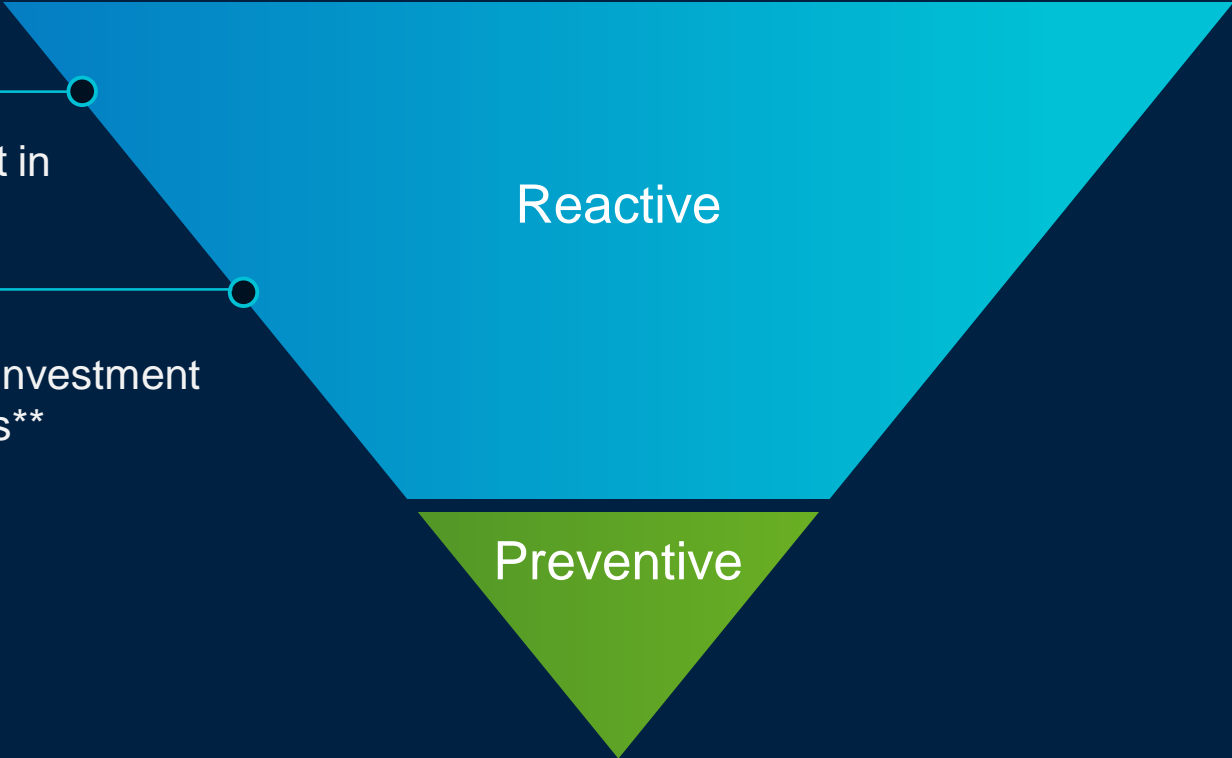
# Where Do We Currently Focus our Time, Investment and Innovation?

80%

of Enterprise IT's investment in security\*

72%

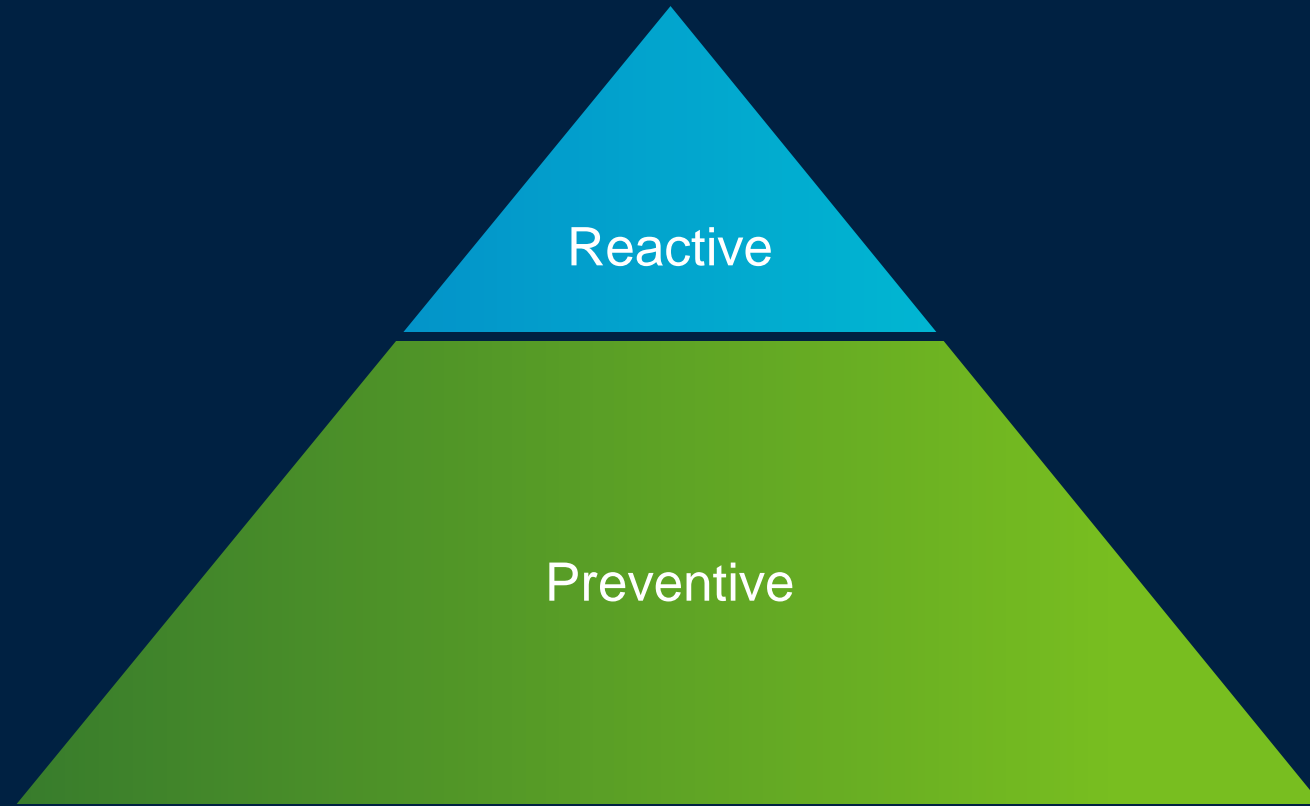
of Venture Capital investment in security start-ups\*\*



\*Source: VMware Analysis

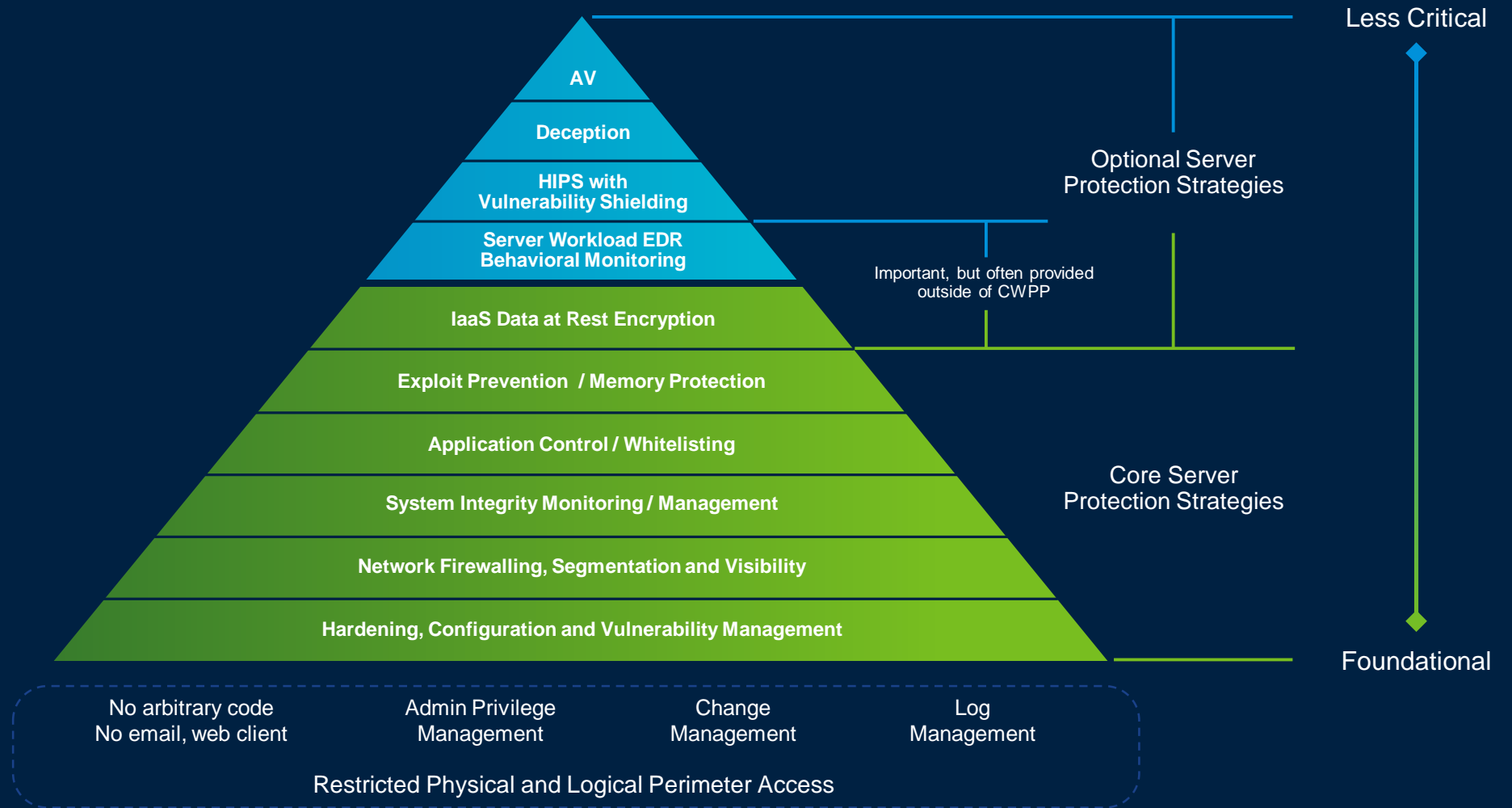
\*\*Source: 2018 Cyber Defenders Report and 2017 Cyber Defenders Report, CB Insights (2019 and 2018)

# 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.

2

‘Application Awareness’  
lacks awareness of  
applications.





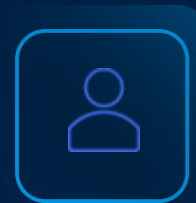


3

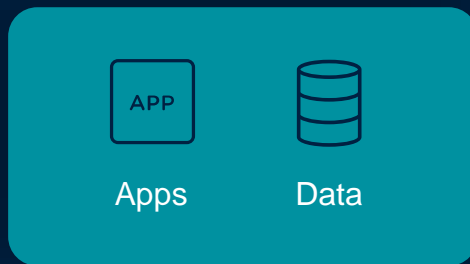
Your most important  
security product won't  
be a security product.



Endpoint



Identity



Apps



Data

Workload



Network



Cloud





# Security Controls

## Digital Risk Management

**crisp** **CYBERSPRINT** digital shadows\_ DigitalStakeout  
EXPANSE LOOKINGGLASS NAMO-G-O-O FISHLABS  
RISKIQ SafeGuard Cyber ZEROF0X

## Mobile Security

appdome BETTER BlackBerry blue cedar Fyde  
Check Point cellrox COMMUNITAKE CyberAdAPT  
INPEDIQ Lookout mobileiron  
pradoo PATAESA PSafe SaldINA SOTI  
Symantec TeleSign Tugersix TRUSTLOOK  
VAULTO wandora wickr ZIMPERIUM

## Endpoint Security

AhnLab avast Avecto Avira Barkly  
BLUERIDGE BUFFERZONE Carbon Black  
Check Point COMODO CROWDSTRIKE CYBERARK  
cybereason CYLANCE deepinstinct ENDGAME  
ERICOM ESAT F-Secure FARONICS FORTINET  
HYSOLATE Intego ivanti KASPERSKY McAfee  
Microsoft MORPHSEC HYTRON OPSWAT panda  
SentinelOne SOPHOS sparkcognition STORMSHIELD  
Symantec TEHRIS WEBROOT ZIO

## Data Security

ANJUNA baffle boxcryptor CipherCloud  
CryptoMove DATALOCKER Fortanix VIRTIV  
dearswift GDDK42 Fidelis McAfee  
Symantec BlueTalon druva opentext SECURE

## Block Chain

Chain guardtime IDEE NuID remme  
vchain ShoCard xage

## Security Operations & Incident Response

BlackStratus CORRELOG CYBRILANT DEVO  
exabeam FORTINET HarSIgn huntaman IBM RSA  
IGLOO logentrics logpoint iLogRhythm  
logz.io McAfee Palantir  
solarwinds splunk> sumologic TIBCO Trustwave  
atastaco ayehu CYBODIT Bay Dynamics BARKETAWAKE  
DEMISTO DEANS FAREYE mistnet  
Microsoft radar RAPID0  
Raytheon arisient SEC3 RSA FORTINET Reservoir Labs  
serviceNow SCALIFY SIFT THETARAY  
SWHPLANE INBATO PATTERNS Haystack Veriato  
ThreatConnect UPLEVEL VERINT VECTRA SECUREWORKS

## Threat Intelligence

4i@ Blueliv. ANOMALI  
Blueliv. Centripetal CUCO Second State RiskIQ  
digital shadows\_ DORHINTOOLS SentinelCy Sixgill SUPPLYWATKIN  
OEclecticIQ FRSIGHT PROFUSE SpyCloud ThreatConnect  
FLASHPOINT HarSIgn HYAS ThreatMetrix THREATQUINENT  
INTELLATL INTSIGHTS KELA Threat STOP TRUSTAR WEBROOT

## Cloud Security

anchore aqua deepfance EDGEWALL Guardicore MYTHUST  
NeuVector PAYVERSE portshift Invisi Stack AVANIAN  
Quyls StackRox Sysdig Microsoft REDSCAPE  
Twintlock IBM Illumio Lacework SHIELD  
BRACKET cavirin Check Point bitglass CipherCloud IBM CISCO CROMET  
CLOUDWAY

## Risk and Compliance

AXONIUS Bolbix cavirin OVERSERVER  
GRX DELVE KENNA  
NEHEMIAH NOPSEC OPAQ Output24  
panabeer OPENAGENT REDSEAL riskrecon  
SKYBOX tenable UpGuard VENAFI  
zeguro BITSIGHT CORAX FICO WALENS  
SecurityScorecard Cobalt CRUIZ  
CYBERRAT CYBERMILL CVMULATE DEPTH tuin  
MAZEBOLT PCSYS PICUS  
RAPID0 SafeBreach VERODIM  
algosec secure Lockpath MetricStream  
neturix Despring RESOLVER RSA  
Barracuda Cymon CyberVista SAI GLOBAL  
IRONSCALE proofpoint PARADEFORCE

## WAF and Application Security

ALERTLOGIC  
Barracuda BRIDGE citrix ergon THREATX  
CyKickLabs FORTINET SH-PE  
imperva NETSPI onepark TEMPLARBIT  
netasparkr CONTRAST zego Synack STACKPATH  
Qualys ORACLE wallarm IBM  
portshift PURESEC luckezone VICTORIS  
RAPID0 Reblaze riverbed riverbed SUCURI  
PentestLABS Radware Signal Sciences sgreen  
waratek Wazuh Trustwave VERACODE  
sentryo AWAKE BRIDATR CGS  
DARETRACE ExtraHop GEMINI  
PERCH Plixer SEC3 SSR

## Identity & Access Management

Accepto Auth0 averyon BehaviorSec BIOATCH CallSign  
CLEF CORE EXOSTAR FORGEROCK FUDO Google  
IDEE Imprivata INTRINSIC ID nok nok pindrop plainID SAASPASS  
transmit SECUREPUSH SILVERFORT tascant ThreatMetrix  
TransUnion TRUSONA UNBJUND UNIKEN V-KEY VIRSH  
Centrify  
Centrify IBM idaptive Microsoft okta RSA HPR  
onelogin ORACLE THALES BeyondTrust MICRO FOCUS  
CYBERARK HITACHI ManageEngine ONE IDENTITY  
Remediant SECURELINK thycotid AXIOMATICS DigiIdentity  
helpsystems SailPoint simelo Akamai IDExperts  
logradius Truloo vchain verato VERIFF ID.me

## Network & Infrastructure Security

Barracuda BLUEHEXAGON BLUVECTOR CISCO CORSA  
FIREEYE FORTINET HUAWEI HYSOLATE JOESecurity JUNIPER  
mimecast OPSWAT paloalto RESEC GATESCANNER SONICWALL SOPHOS  
Symantec VOTRO WIZATGuard orubo AUCONET AXONIUS CyberArk Cytora  
Extreme FORESCOUT NANOSEC SKYPORT NETSHEL pornox NEXLINE  
Trustwave centera Geniens TEMPERED VERSA ZENITH  
Check Point Imperva neustar HERUSGUARD NSFOCUS ORACLE corelight  
SECUREIT STACKPATH BLUECAT neustar Threat STOP VERAN Quad9 MixMode  
efficient IP infoblox NEWNET algosec CATO CLOVISTOP PERKIN  
endian FORCEPOINT GAUSHIELD Hillstone OPAQ SANGFOR McAfee  
secucloud SONICWALL STORMSHIELD tuin Fidelis WUNBUNGA ACALYPTO SPANISH RAS  
AVIVA Blueive Counter Craft VIBRANT VIPER CyberTrap SMOKESCREEN VERINT  
Cymmetria TRAPX APERIO DAYSHORE BELDEN CRIBFENCE NOOPM  
CYBERBIT FIRMITAS Indegy dimension SCADAfence Corvil NETSCOUT  
CyberX DRAGOS PEP radilow Rhebo CORE IronNet  
CloudShark utimaco OREYCORTEX

## Digital Risk Management



## Mobile Security



## Endpoint Security



## Data Security



## Block Chain



## Threat Intelligence



## Security Operations & Incident Response



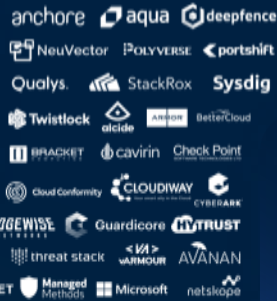
### Endpoint



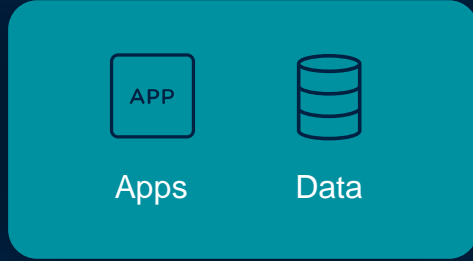
### Workload



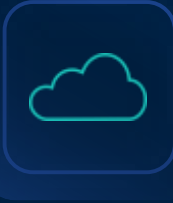
## Cloud Security



## Risk and Compliance



## WAF and Application Security



## Identity & Access Management



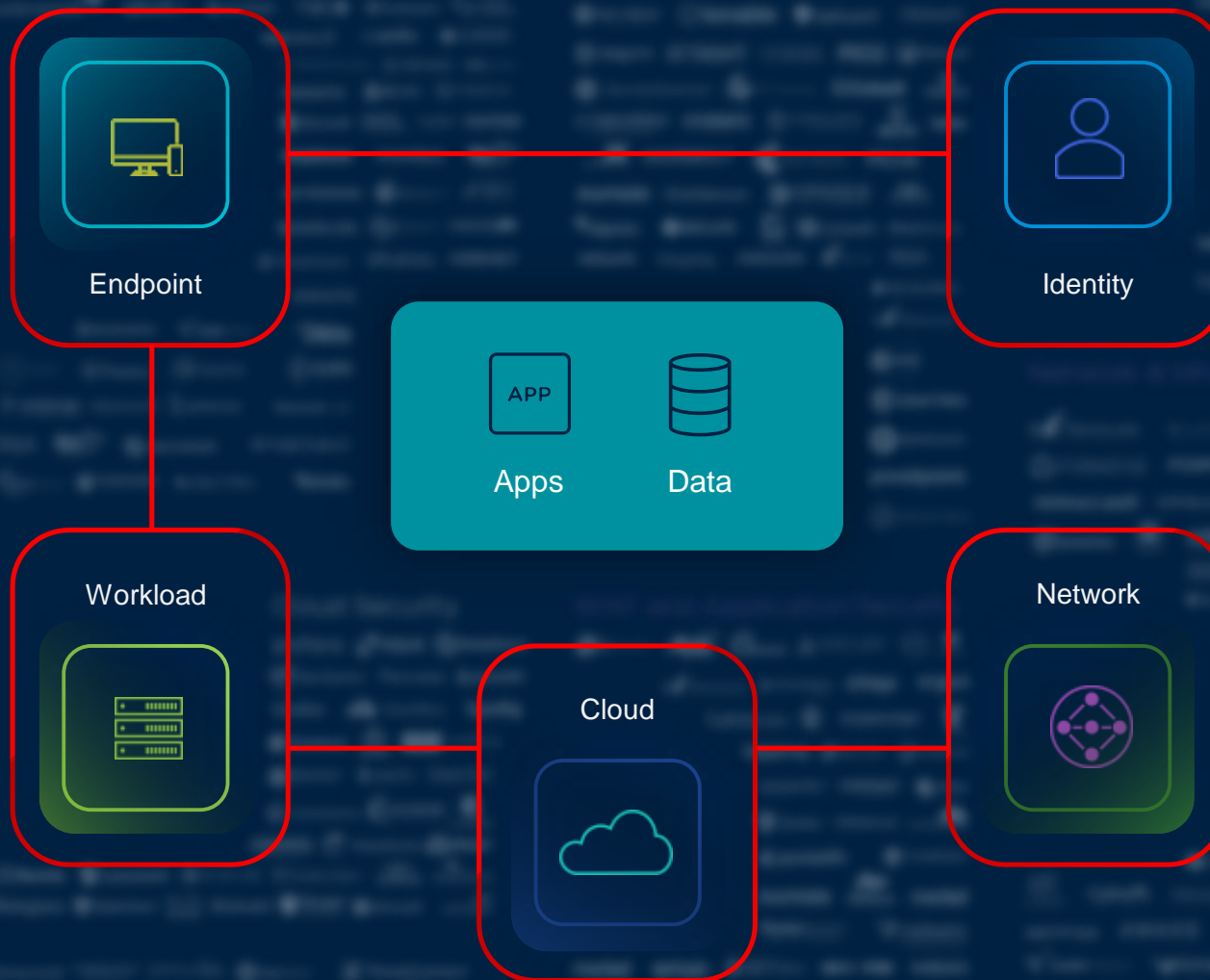
### Identity

## Network & Infrastructure Security



### Network





# Security Must Be Transformed



Built-in  
Bolted-on



Proactive  
Reactive




Aligned  
Siloed



# VMware Vision

The essential, ubiquitous digital foundation

Any Device



---

Any Application



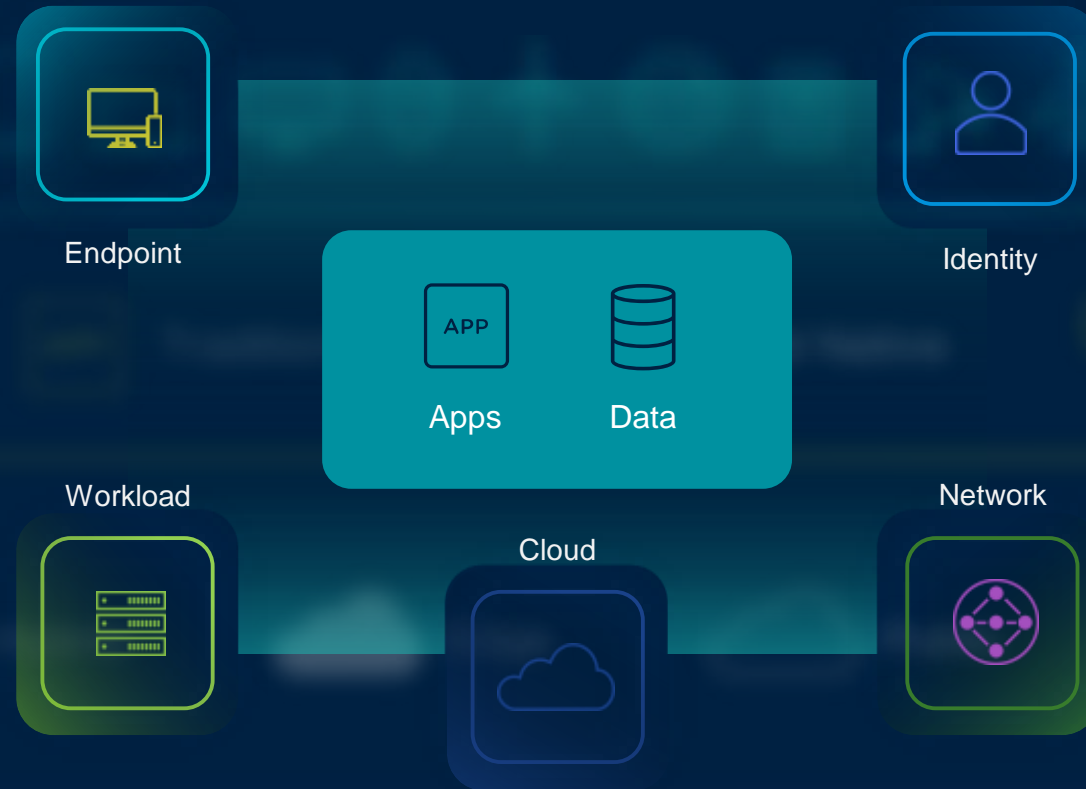
---

Any Cloud

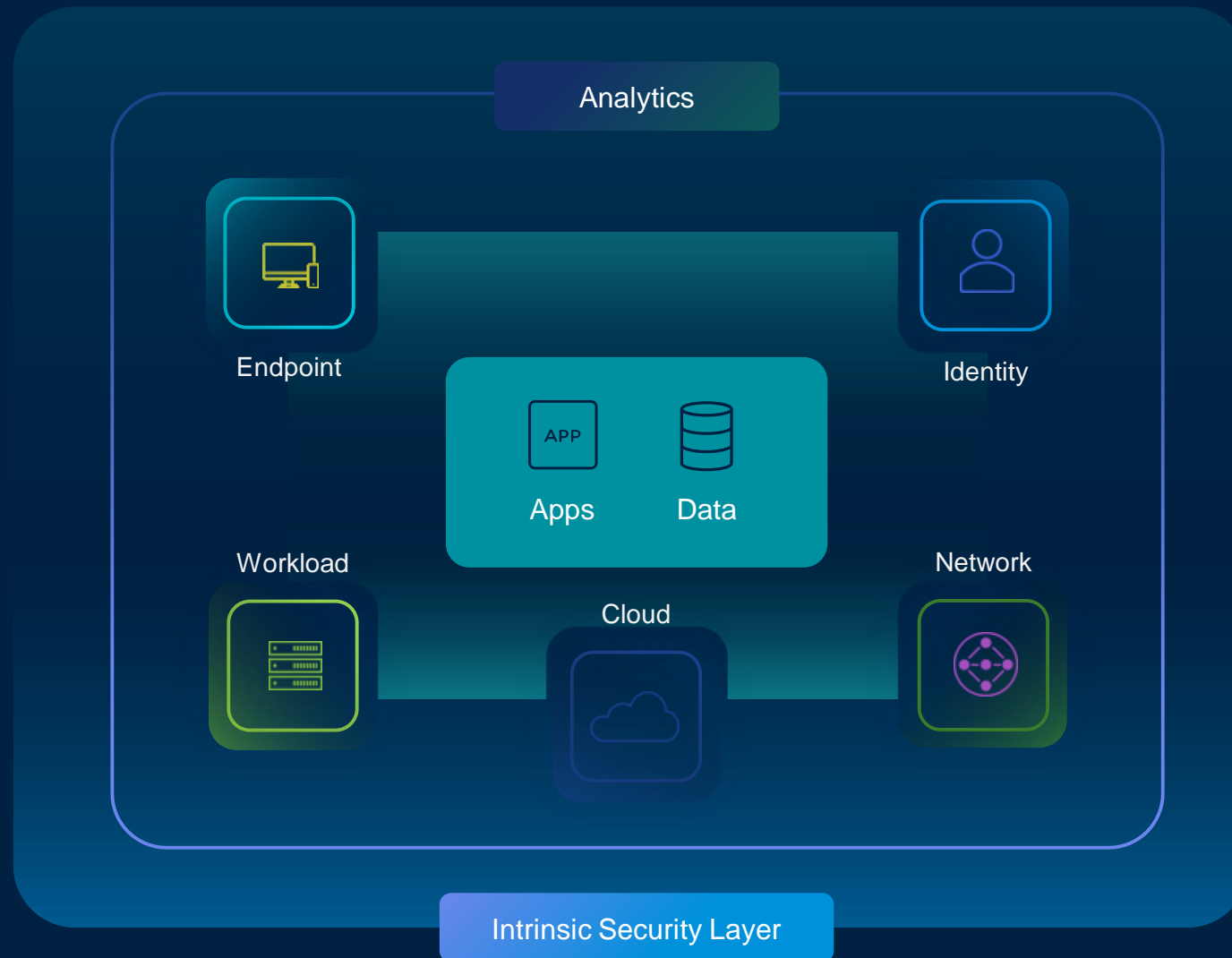


---

# VMware Security Vision

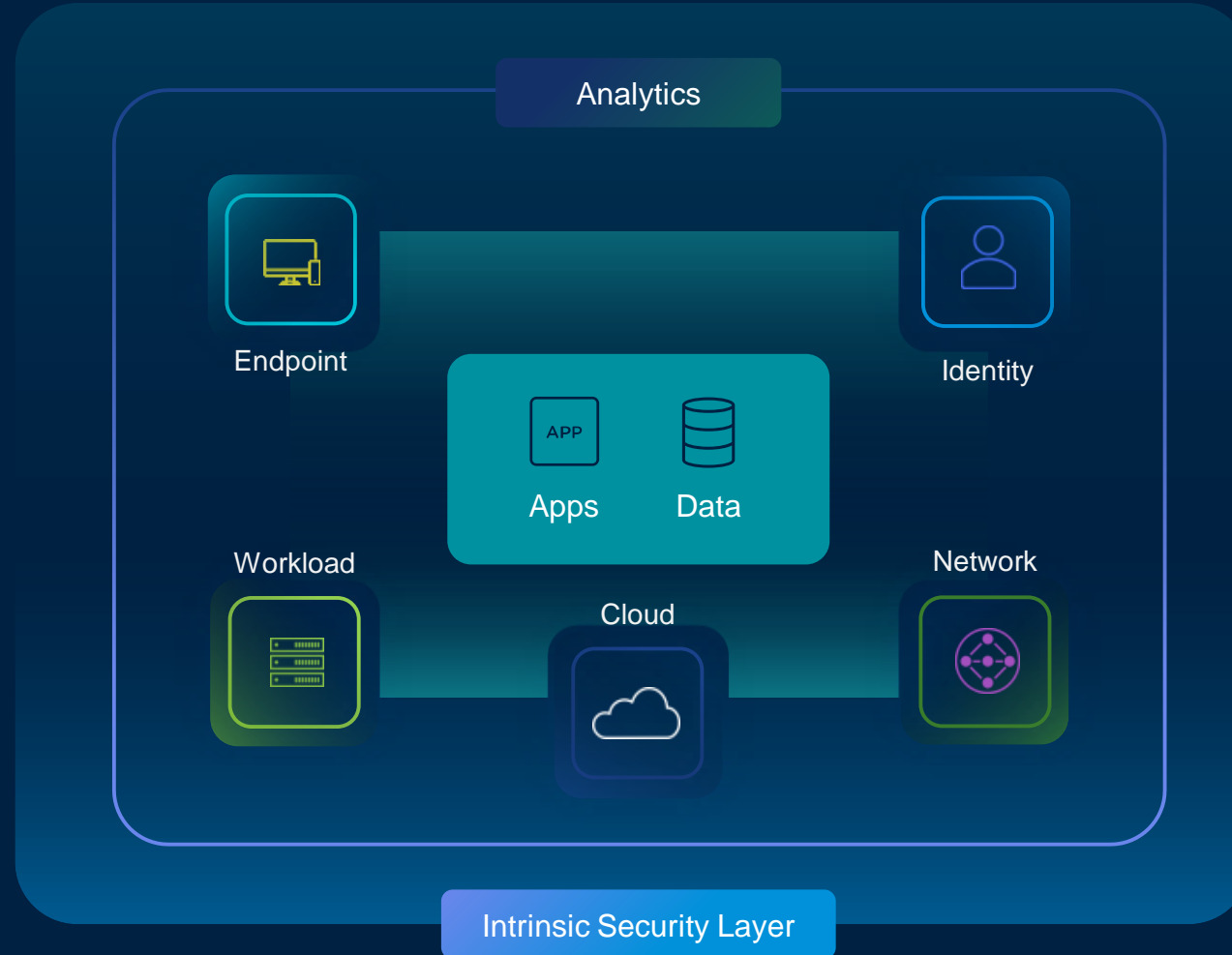


# The Intrinsic Security Layer



# The Security Ecosystem

IBM Security  
splunk>  
Carbon Black.  
RSA  
Secureworks



okta  
netskope  
zscaler™  
paloalto  
NETWORKS  
Check Point  
SECURITY SOFTWARE TECHNOLOGIES LTD.



# Carbon Black.



5,600+  
Customers



500+  
Partners



Leader  
Endpoint Detection Response \*

# Carbon Black.

A Leading Security Cloud



Endpoint  
Detection  
Response



Next Gen  
Anti-Virus



Device  
Control



Rogue Device  
Detection



App  
Defense



Vulnerability  
Management



Audit and  
Remediation



Compliance  
Reporting

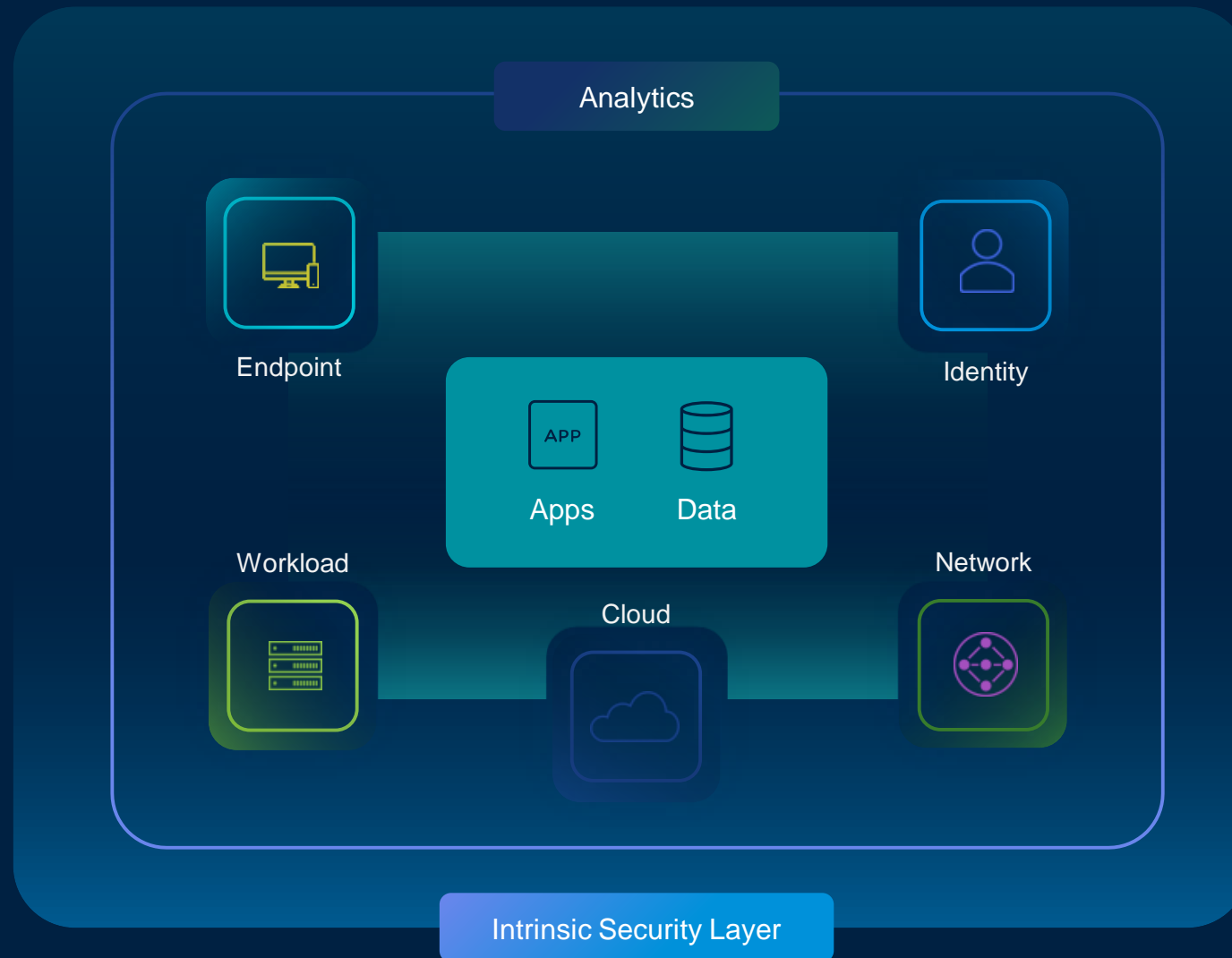


Managed  
Detection

# VMware + Carbon Black + Ecosystem = Better Together



# The Intrinsic Security Layer



What does this shift in  
thinking look like?

A complex network diagram in light blue on a dark blue background. It features various nodes such as servers, clouds, and VMs, all interconnected by thin lines representing network connections. The text is centered over this network.

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

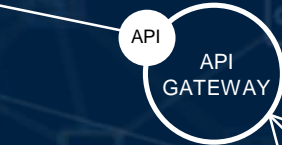


# APPLICATION

MOBILE APP



WEB APP



Partner

Analytics



# KNOWN-GOOD

MOBILE APP



Analytics



WEB APP



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]

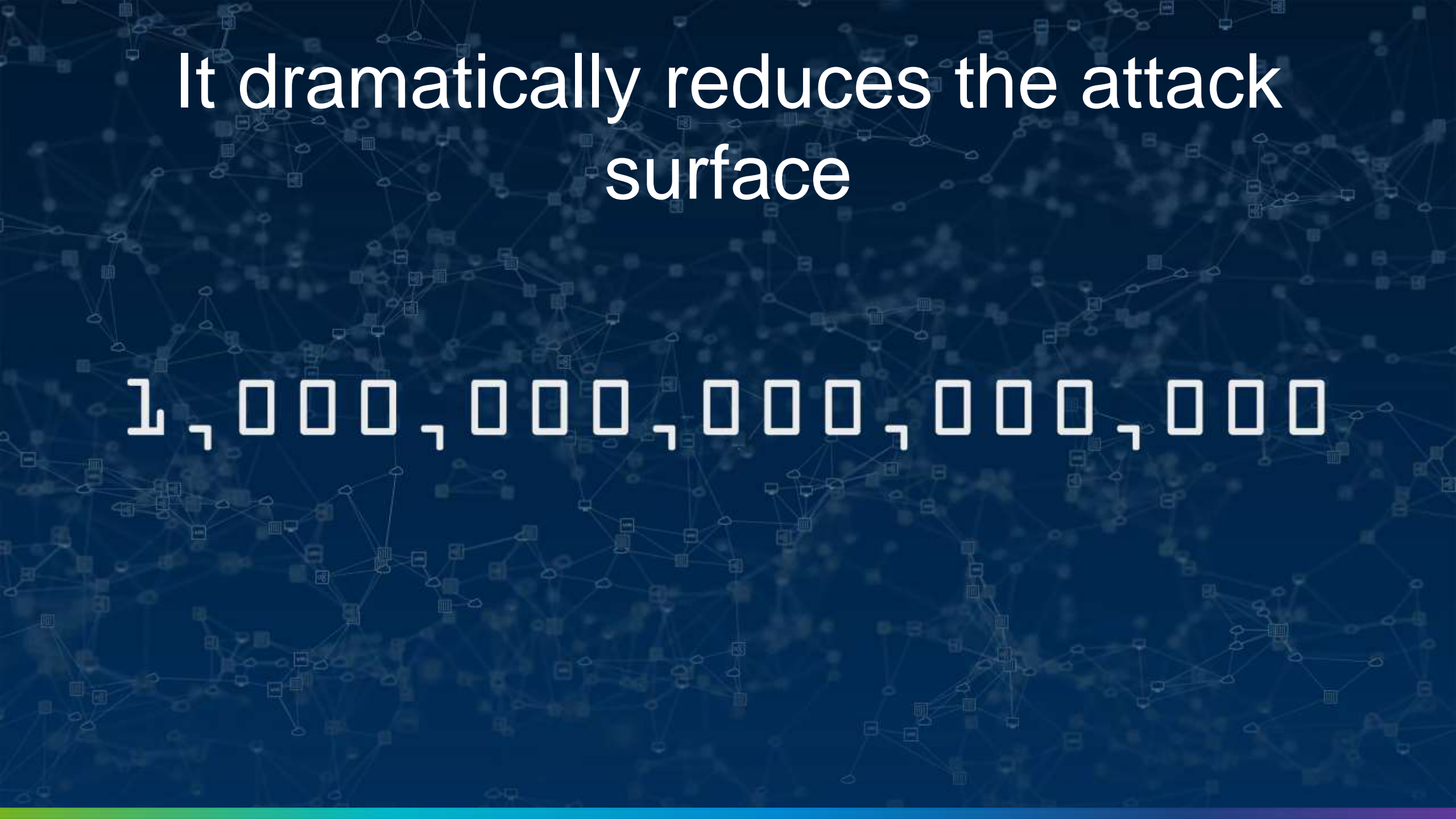
**IT IS OUTSIDE THE HOST**

[SUPER ROOT]

**IT IS EVERYWHERE**

[DISTRIBUTED SERVICES]



A background network diagram with a dark blue gradient. It features a complex web of interconnected nodes and edges. The nodes are represented by small squares and circles, and the edges are thin white lines. The overall pattern is dense and irregular, suggesting a large-scale network structure.

It dramatically reduces the attack  
surface

1,000,000,000,000,000

# Actions You Can Take Immediately

**Invest in Prevention**

**Focus on Applications**

**Make Security Intrinsic**

**Visit the VMware in the Expo**

Thank You



# DELL Technologies



DELL EMC

Pivotal

RSA

Secureworks

virtustream

vmware