

La Distribución de la Seguridad en DC y Nube

El poder de la seguridad intrínseca

Daniel Aguirre
Solution Engineer Network Security

Carlos Alcaraz
Network Security Specialist

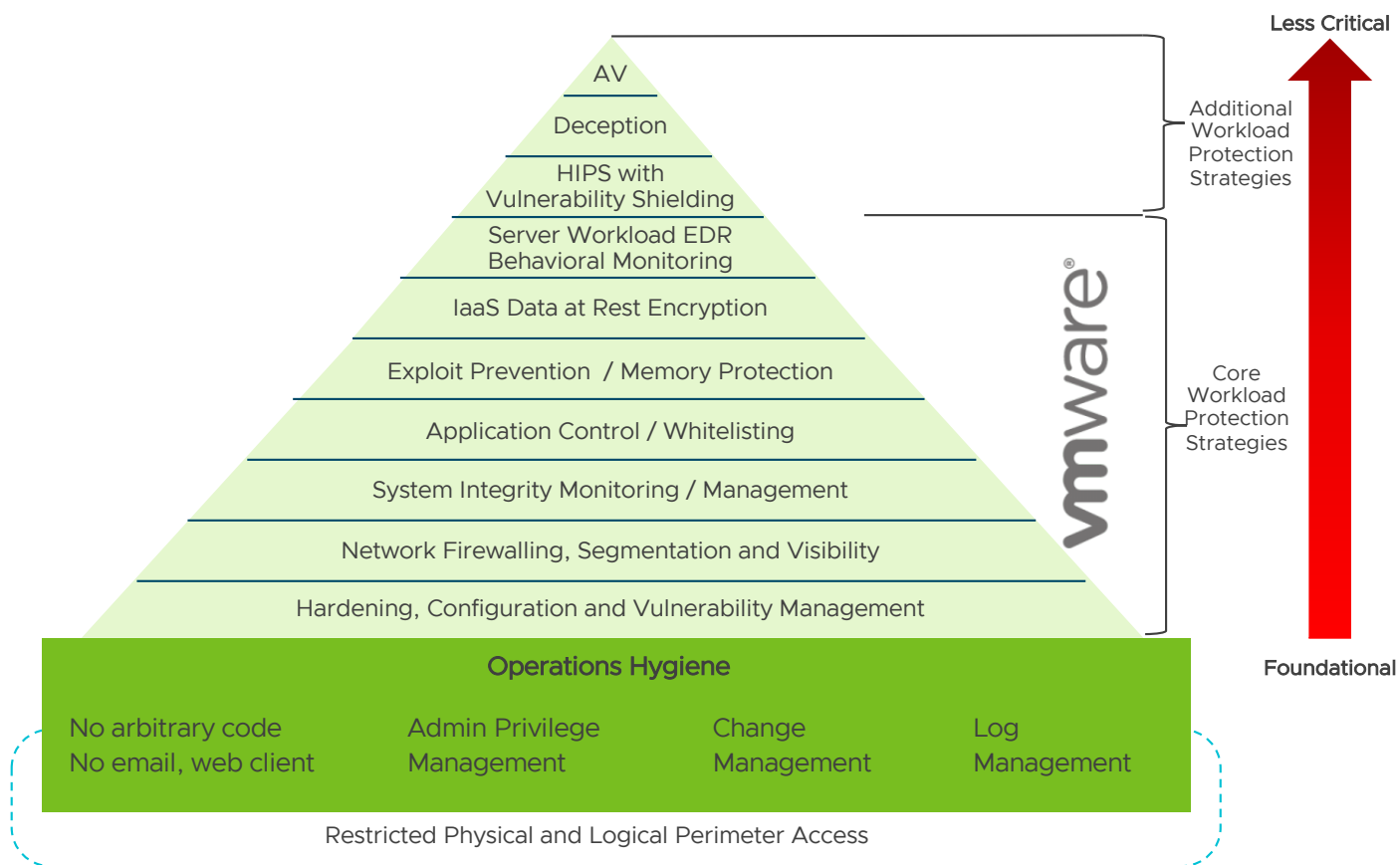
21 Julio 2020

Security Capabilities

Reduce Attack Surface

Respond To Attacks

Gartner Cloud Workload Protection Framework




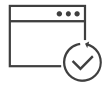


Cyber Threats

Residual Risk




Micro-Segmentation


Least Privilege


Encryption


Multi-Factor Authentication


Patching

Cyber Hygiene

Attack Surface



Security is Fundamentally Broken

Digital Risk Management



Mobile Security



Endpoint Security



Data Security



Block Chain



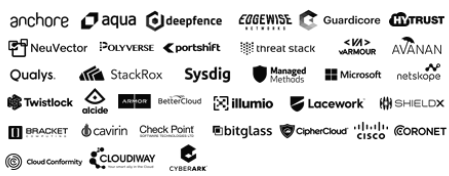
Security Operations & Incident Response



Threat Intelligence



Cloud Security



Risk and Compliance



WAF and Application Security



Identity & Access Management

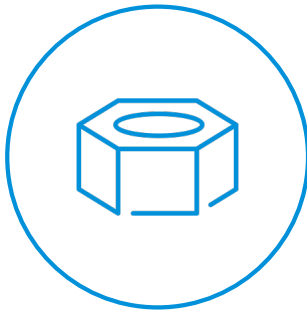


Network & Infrastructure Security



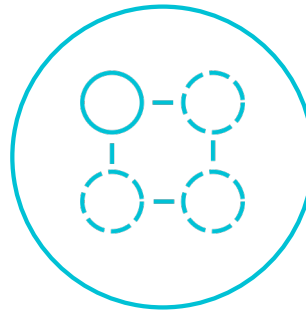
Three Factors Inhibit Security Breakthroughs

Bolted-on



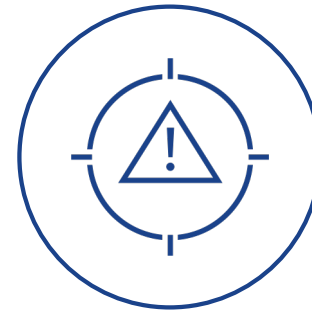
Too many products, agents, and policies

Siloed



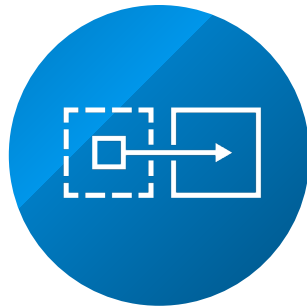
Siloed and misaligned across tools and teams

Threat-centric

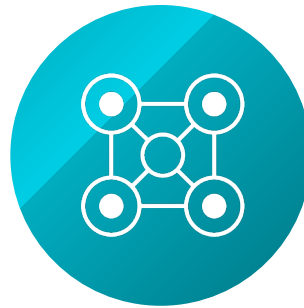


Reactive and too focused on previous threats

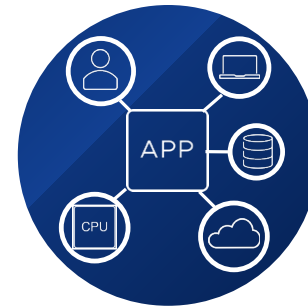
Security Must be Transformed



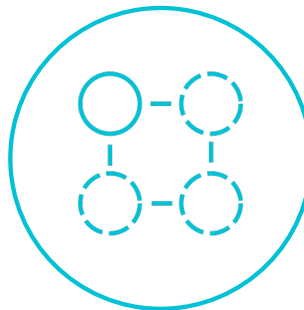
Built-in
Bolted-on



Unified
Siloed

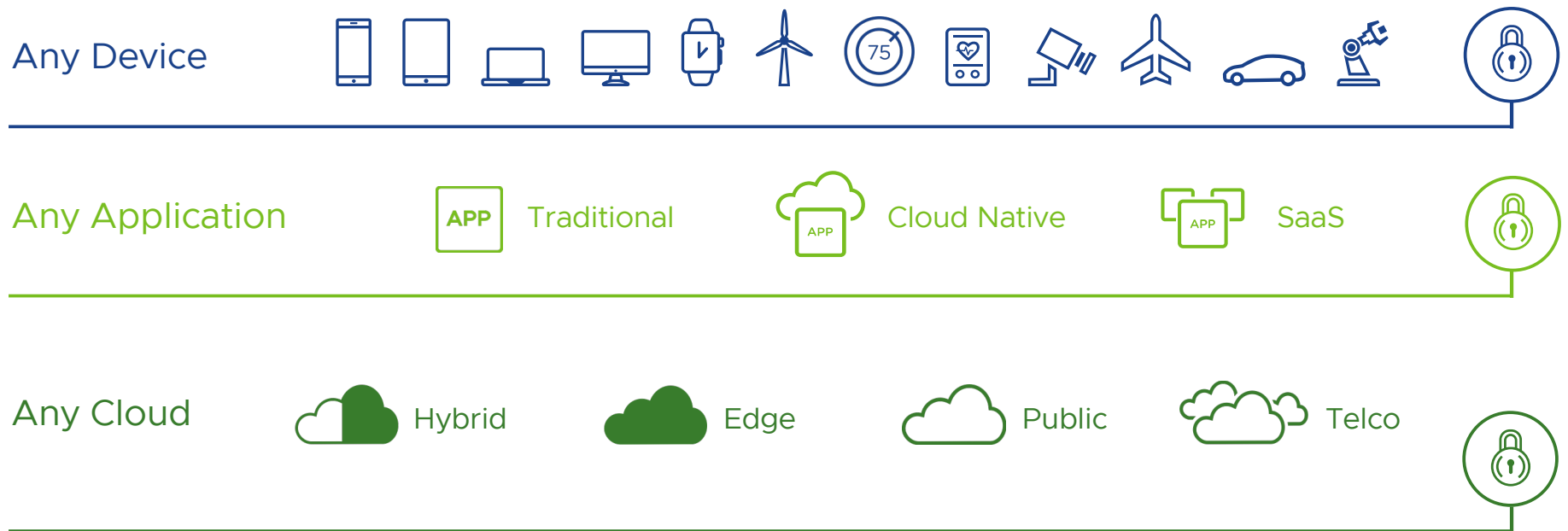


Context-centric
Threat-centric



VMware Vision

The essential, ubiquitous digital foundation



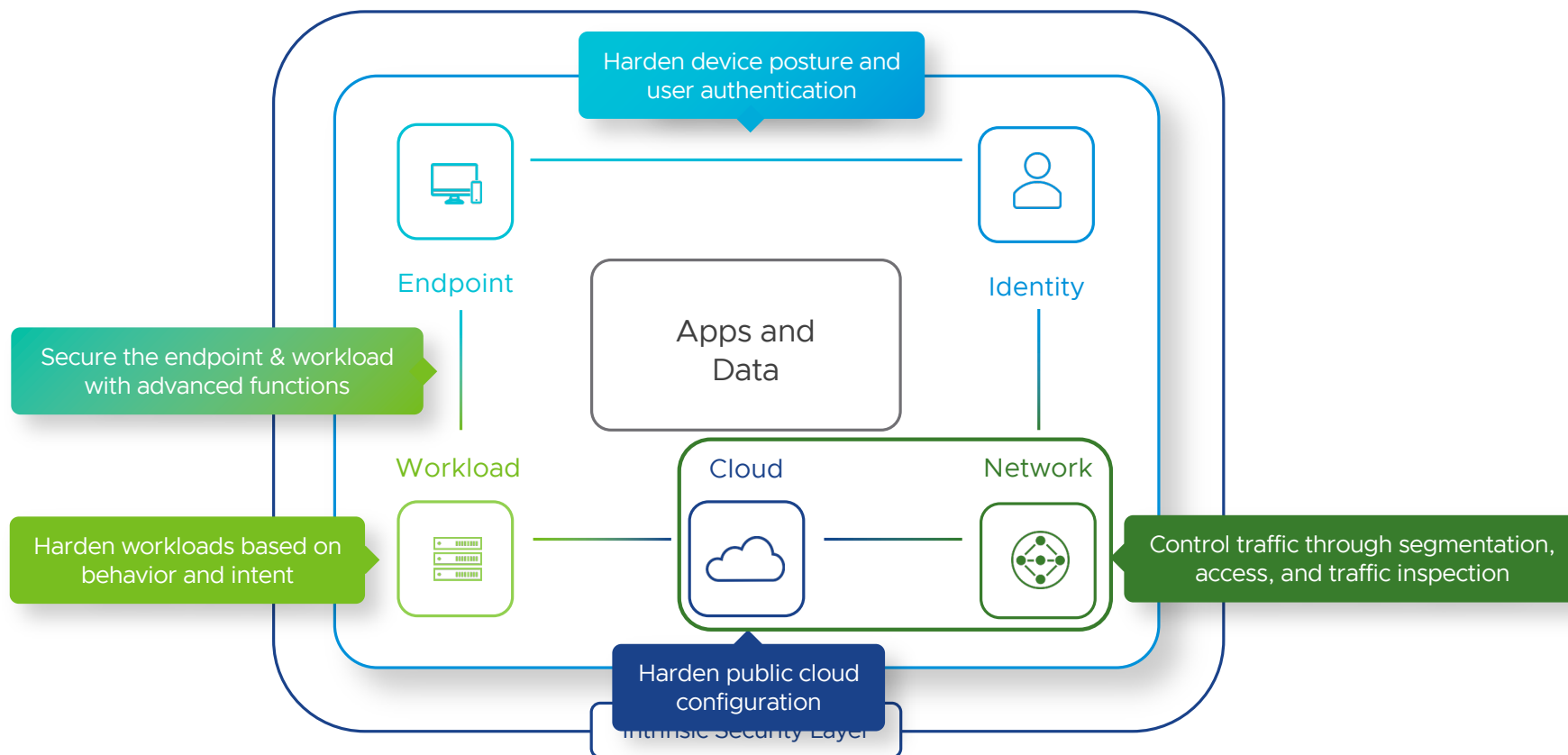
Intrinsic Security

Leveraging your infrastructure across any app, any cloud, and any device to protect your apps and data everywhere.

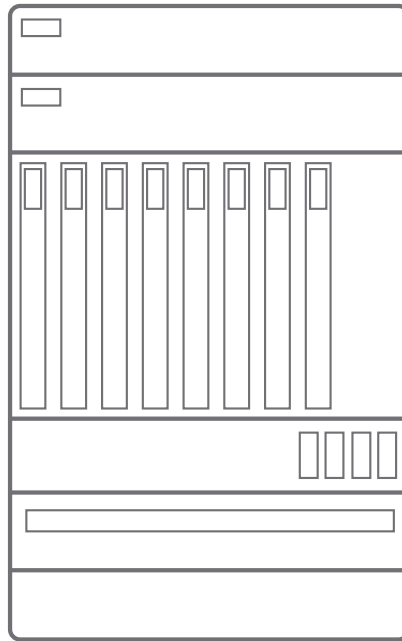


Intrinsic Security

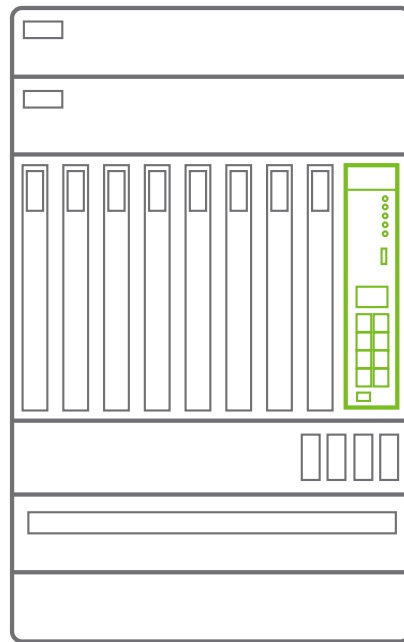
Leveraging your infrastructure to secure your business



INTEGRATED = BOLTED ON

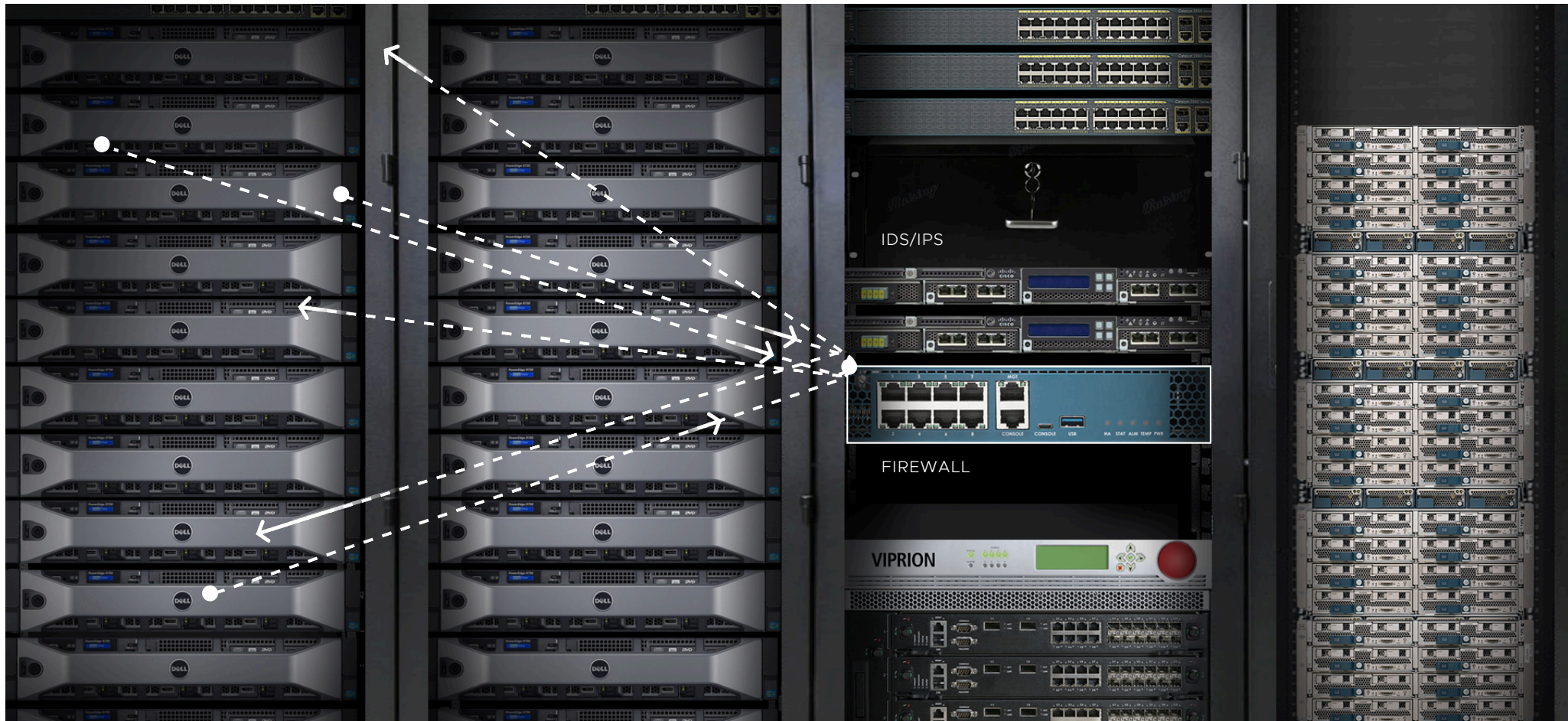


INTEGRATED = BOLTED ON



Same firewall...
...repackaged.

Traditional E/W Firewalls Hairpin



VMware NSX Service-Defined Firewall



VMware NSX Service-Defined Firewall



Inspection at each workload removes blind spots

True stateful, layer 7 inspection

Deep service/application context

Introducing VMware NSX IDS/IPS



Introducing VMware NSX IDS/IPS



Introducing VMware NSX IDS/IPS



Eliminates “bump on the wire” boxes

Distributed analysis at every hop

Application-specific signatures reduce false positives

Distributed Analytics with NSX Intelligence



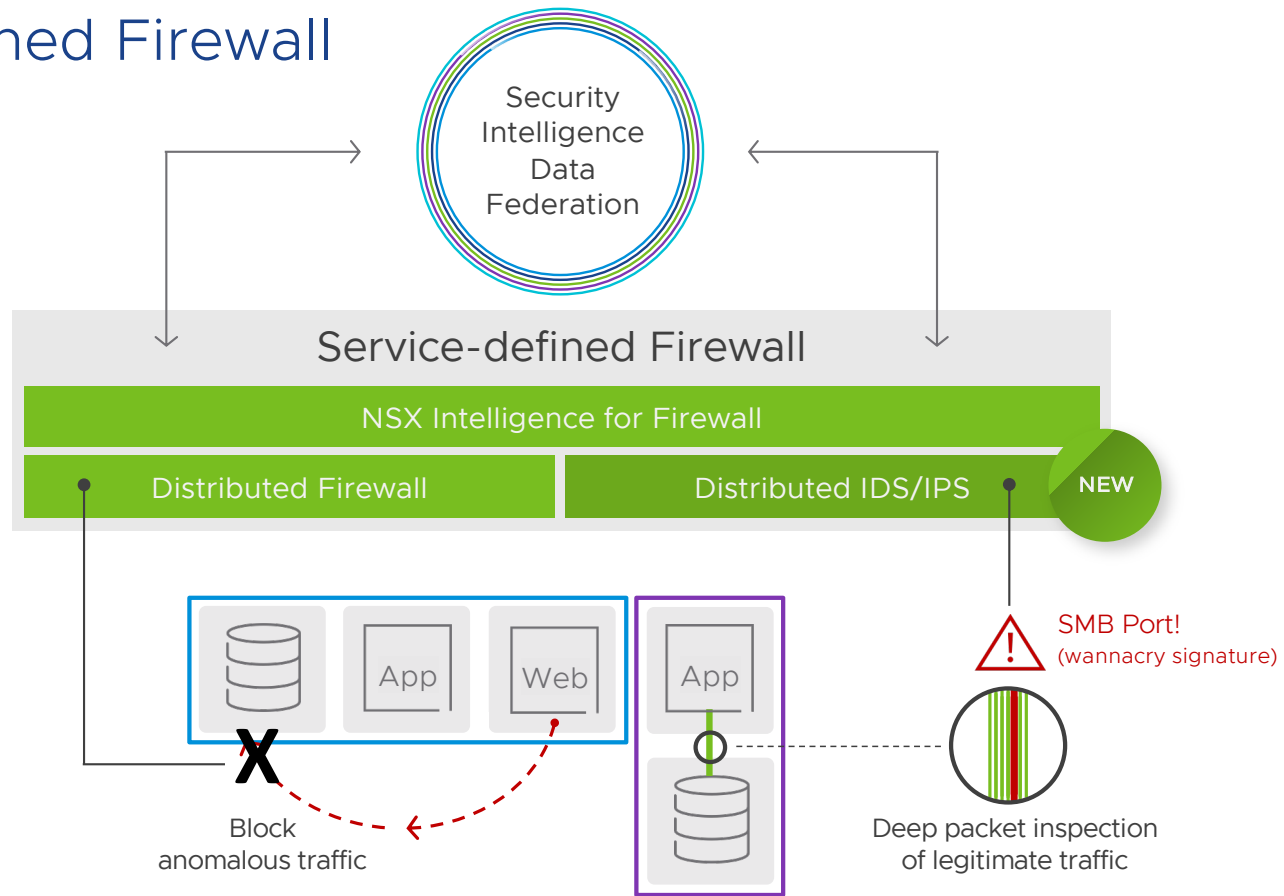
VMs and Containers Are Both First Class Citizens



= First Class Citizen

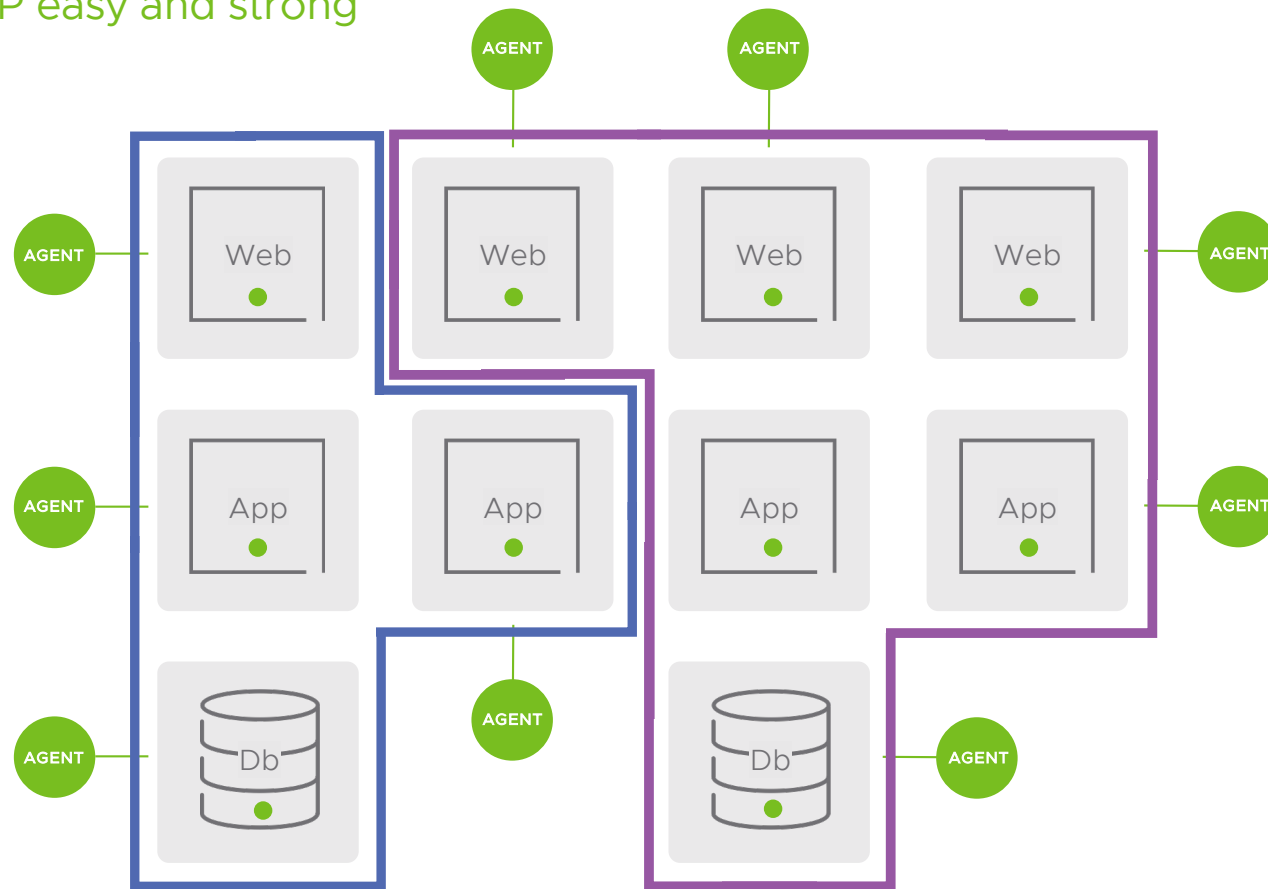
Service-defined Firewall

VMware NSX Service-defined Firewall



The Power of Micro Segmentation

Making server EPP easy and strong



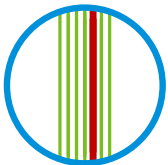
Port Blocking



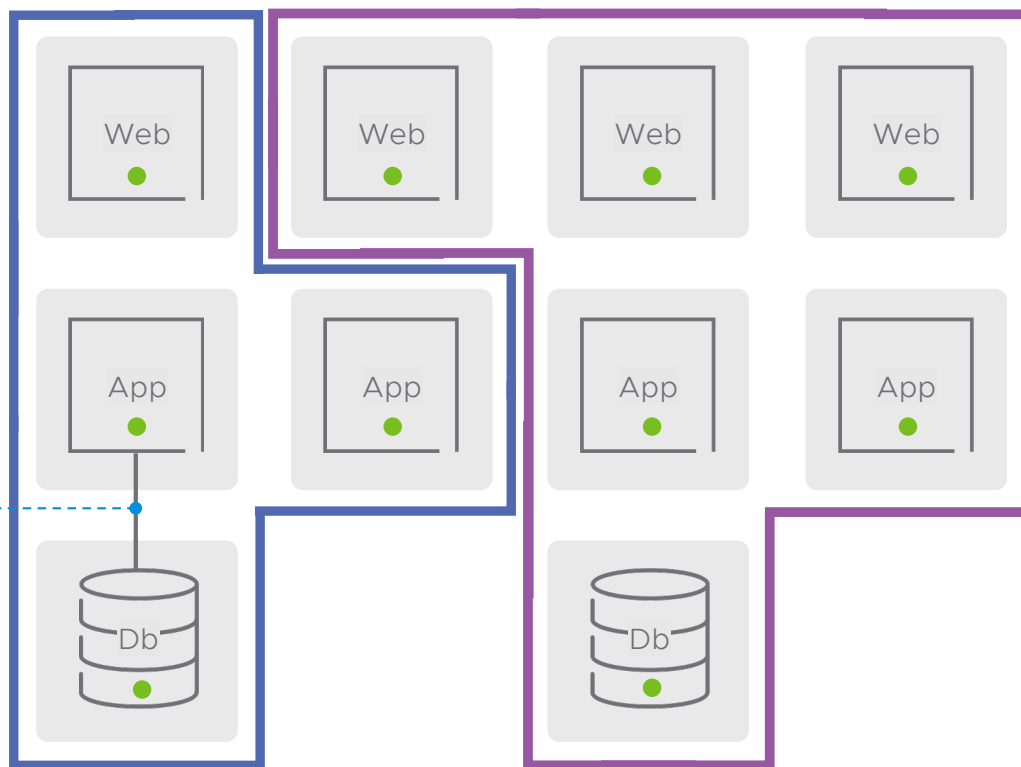
Port Blocking to Server to Server Inspection



!
SMB Port!
(wannacry sig)



Analyzing ALL traffic
looking for anomalies



NSX Intelligence for Firewall

Closing the Insight and Action Gap with Network and Host Informed Analytics

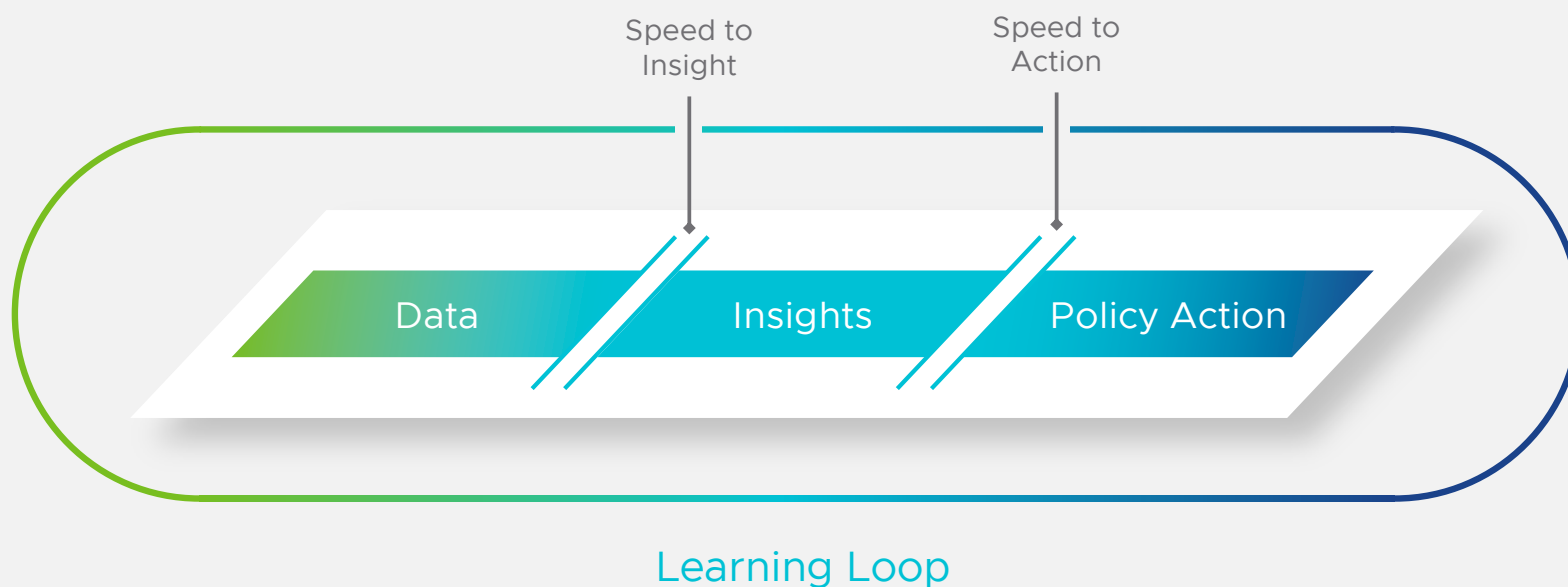


The Insight Gap
Data Overload & Alert Storms

The Action Gap
Limited Context for Action

NSX Intelligence for Firewall

Closing the Insight and Action Gap with Network and Host Informed Analytics



HOT OFF THE PRESS!!!

The image shows a browser window with two tabs. The active tab is titled "VMware Security- One Of The B...". The browser address bar shows a URL ending in "/sites/moorinsights/2020/05/20/". The VMware website is visible, with the VMware logo and "Network Virtualization" text. The page content includes a "VISION" section with the headline "VMware Announces Intent to Acquire Lastline" and a sub-headline "Network Detection and Response Powered by AI". The article text discusses VMware's intent to acquire Lastline, a pioneer in anti-malware research and AI-powered network detection and response. The article mentions that VMware's vision of Intrinsic Security will be amplified by Lastline's capabilities. The article also mentions that VMware will bring a world class team of network-focused anti-malware researchers and developers, and go-to-market security experts, into the NSX team. The article concludes by stating that VMware will continue to foster their deep understanding not just of the threat, but of the motivation and tactics behind the threat.

vmware® Network Virtualization

Getting Started Vision Solutions Technical

// VISION

VMware Announces Intent to Acquire Lastline

Tom Gillis Posted 4 days ago 0 Comments

By Tom Gillis, SVP and GM, Networking and Security Business Unit, VMware

Today we announced our intent to acquire Lastline, a pioneer in anti-malware research and AI-powered network detection and response. This is an important step forward for VMware's vision of Intrinsic Security, as it will allow us to further take advantage of the intrinsic attributes of our virtualization platform to yield innovative security capabilities. Our aim is not to replicate that which exists today, but rather to build security solutions that we can uniquely deliver, spanning from the heart of the data center to users in a branch office and all the way to mobile users at home or on the road.

In the security industry, the nature of threats changes so rapidly that security technology is constantly being re-invented. In this context, it is not the algorithms per se that matter; it is the people that make the algorithms. Great people build great products, and great products build great companies. And that's why we are so excited about the combination of Lastline and VMware. Upon close of the deal, we will bring a world class team of network-focused anti-malware researchers and developers, and go-to-market security experts, into the NSX team. Lastline boasts several of the top 10 most published security threat researchers globally, and the Lastline team has been credited with bringing structure and rigor to the world of malware research. This is reflected in the fact that the Lastline team has 15 PhDs and academics on staff. At VMware, we will amplify the academic focus of the Lastline team, and by joining forces with the Carbon Black Threat Analysis Unit (TAU), continue to foster their deep understanding not just of the threat, but of the motivation and tactics behind the threat.

of COVID-19. Unprecedented strain has been put on networks.

The image shows a banner for Lastline, a network detection and response (NDR) solution. The banner features the Lastline logo and the text "Network Detection and Response Powered by AI". Below this, it says "Automate Response" and "Everywhere your data goes." There are two buttons: "See How We Do It" and "Schedule Demo Today". The background of the banner is a dark blue and green abstract design.

lastline

PLATFORM USE CASES WHY LASTLINE RESOURCES PARTNERSHIPS LABS COMPANY

Network Detection and Response

Powered by AI

Automate Response

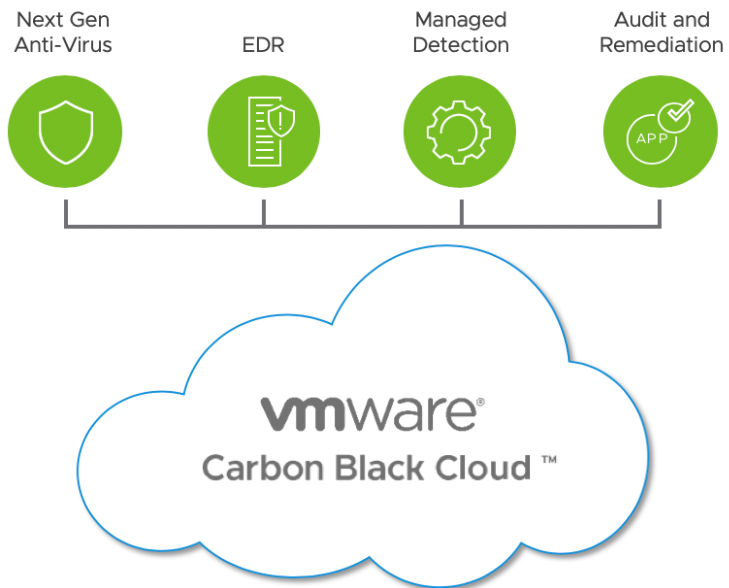
Everywhere your data goes.

See How We Do It Schedule Demo Today

vmware® lastline®

LASTLINE TO BE ACQUIRED BY VMWARE.

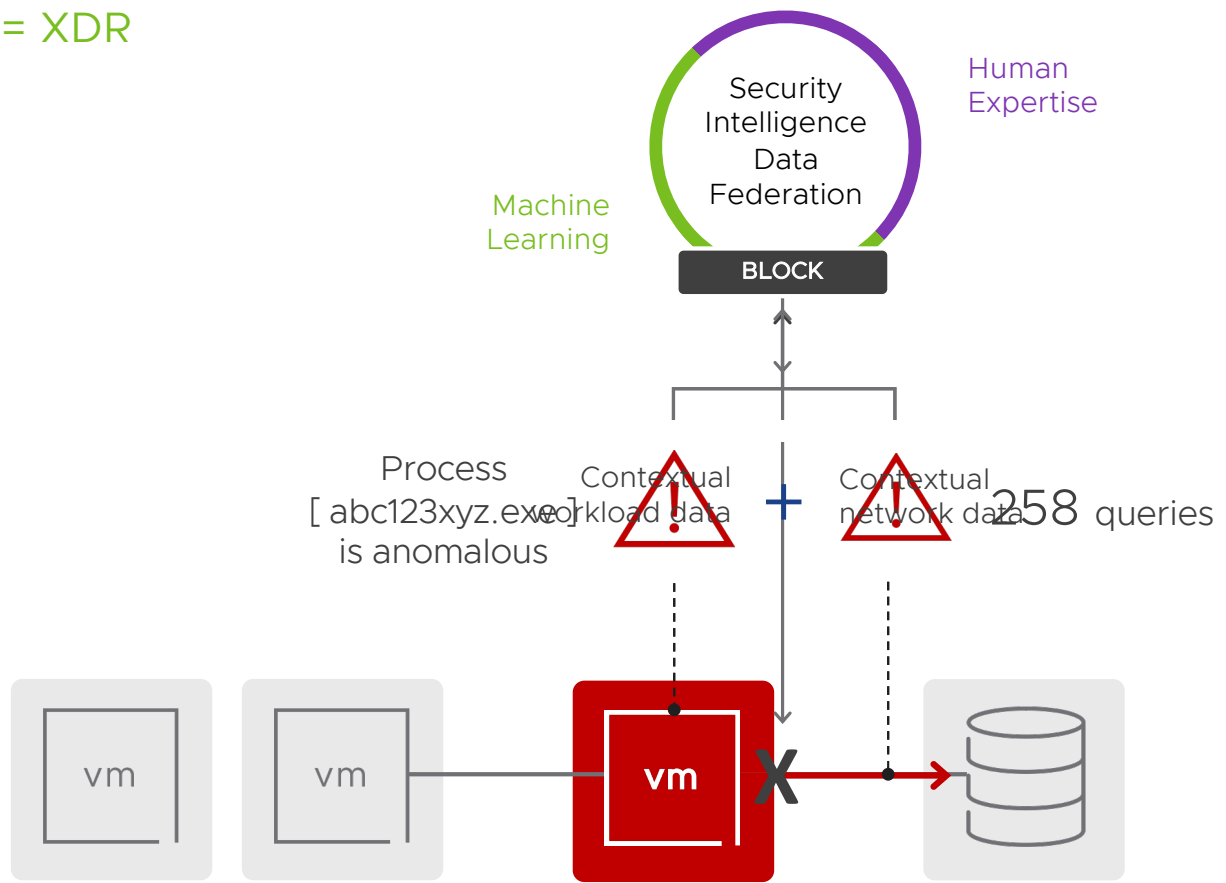
VMware Carbon Black Cloud Enterprise EDR/NGAV



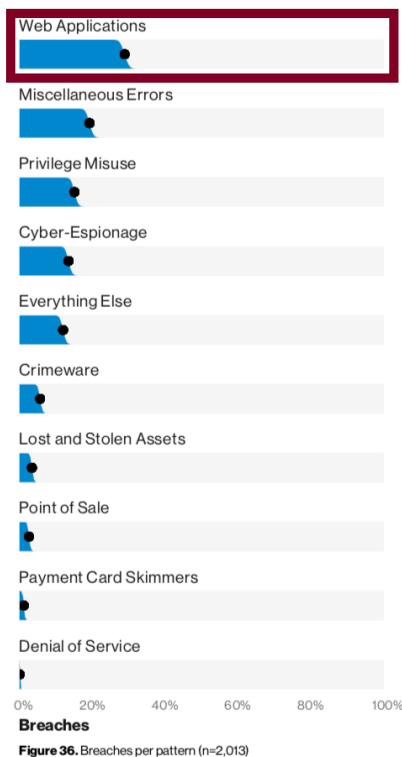
- Consolidate the endpoint stack across your entire organization
- Hunt for threats at enterprise scale
- Access comprehensive endpoint data in a central location
- Faster end-to-end response & remediation
- Clearer view of attack trends to help guide policy
- Bolster the value of your other security operations tools

The Power of Intrinsic

EDR + NDR = XDR



Web Application Breaches and Cost



Source:
Verizon Data Breach Investigations Report (DBIR) 2019

vmware®

BREAKING NEWS

Large corporation had a web application vulnerability, resulting in millions of \$\$\$ cost in data breach, damages, reputation and customer trust.

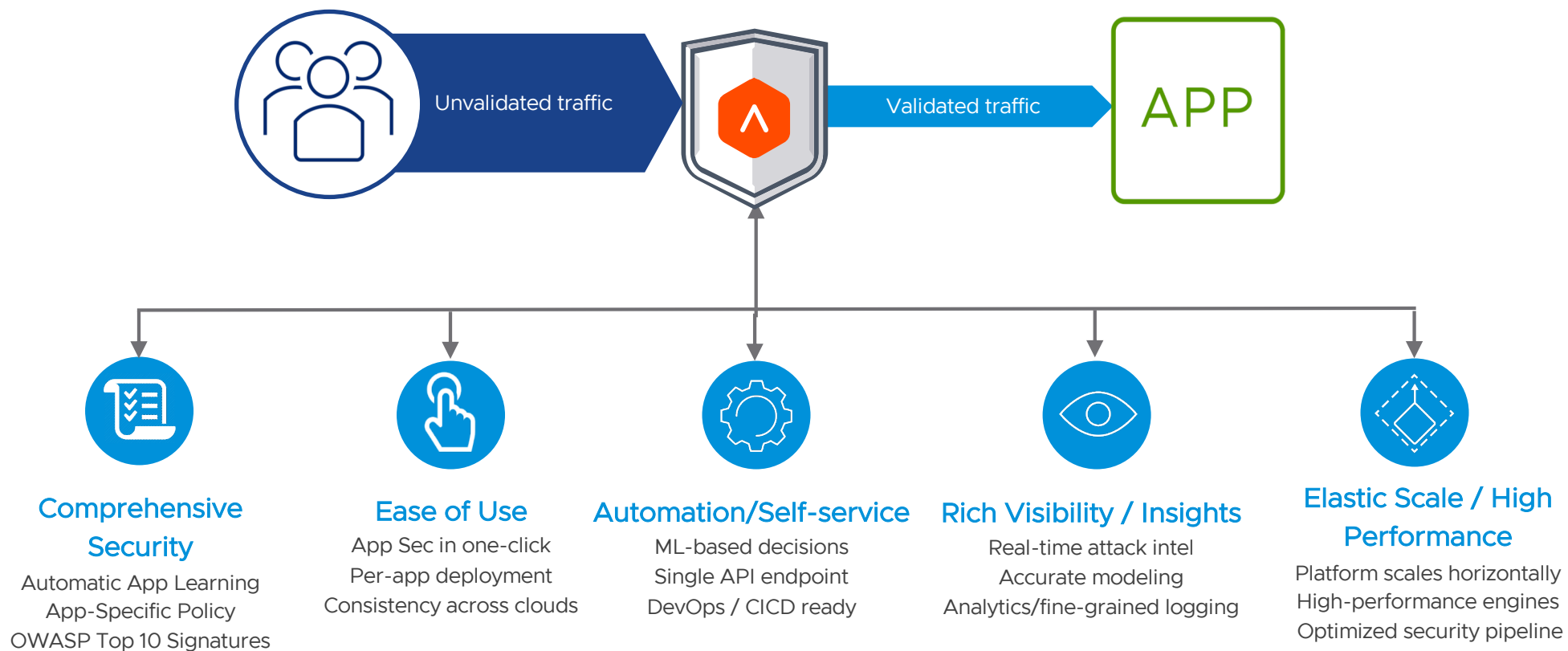
APP

Web application attacks have risen to #1 in terms of breaches.

WAF

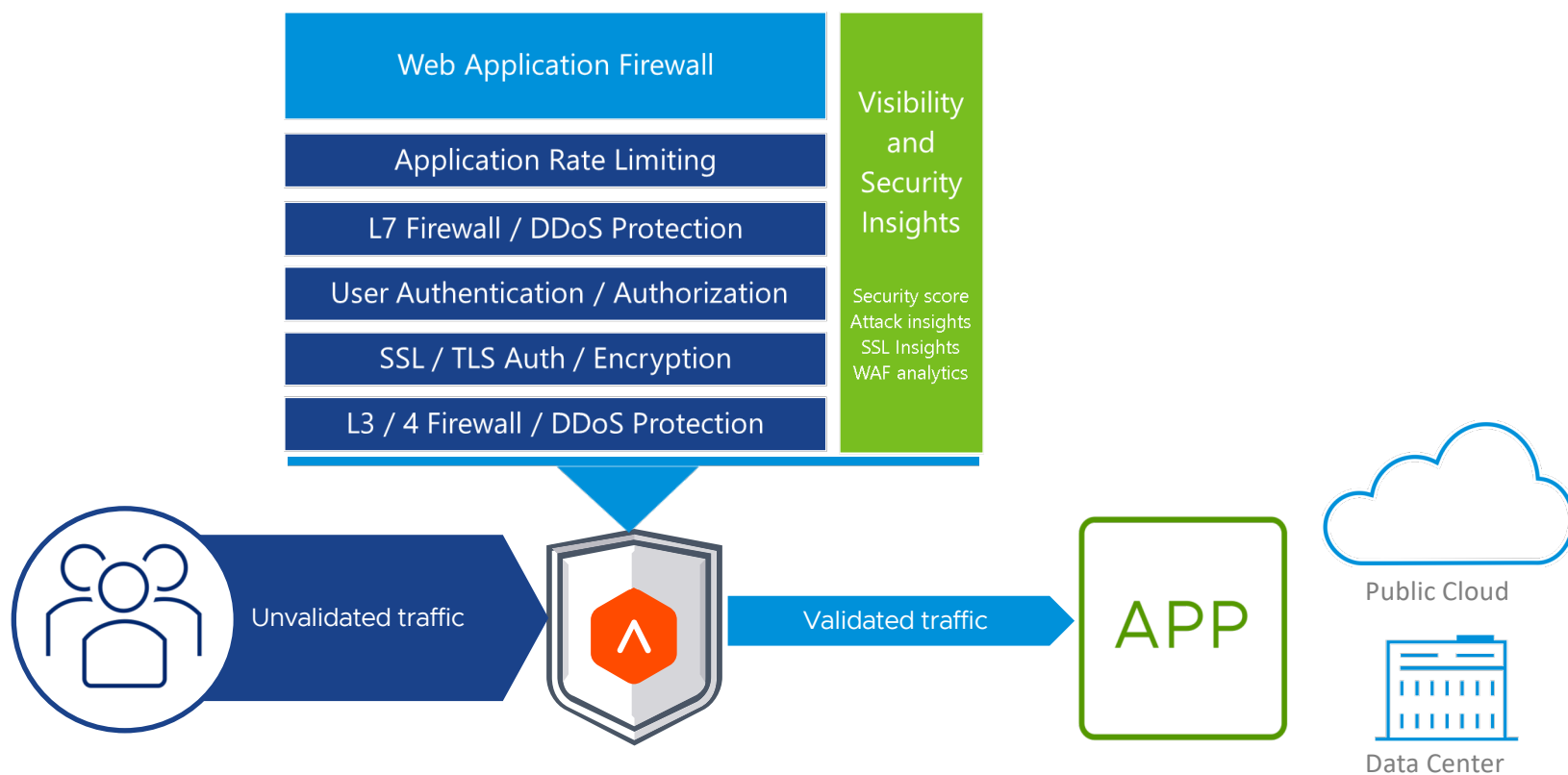
WAF is a critical part of security best-practices to defend against web application attacks.

NSX Application Security Vision

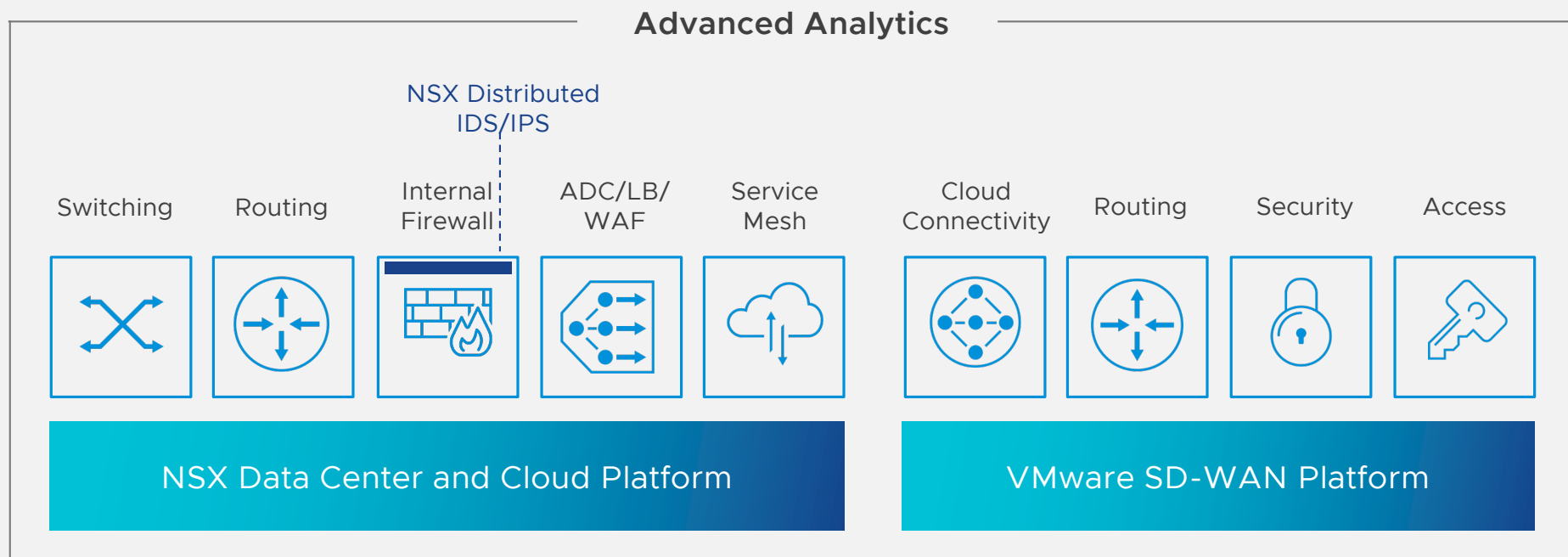


NSX - Application Security Vision

Deliver comprehensive app security and visibility in any data center or cloud



NSX: A Complete Solution



Virtual Cloud Network

vRealize Network Insight

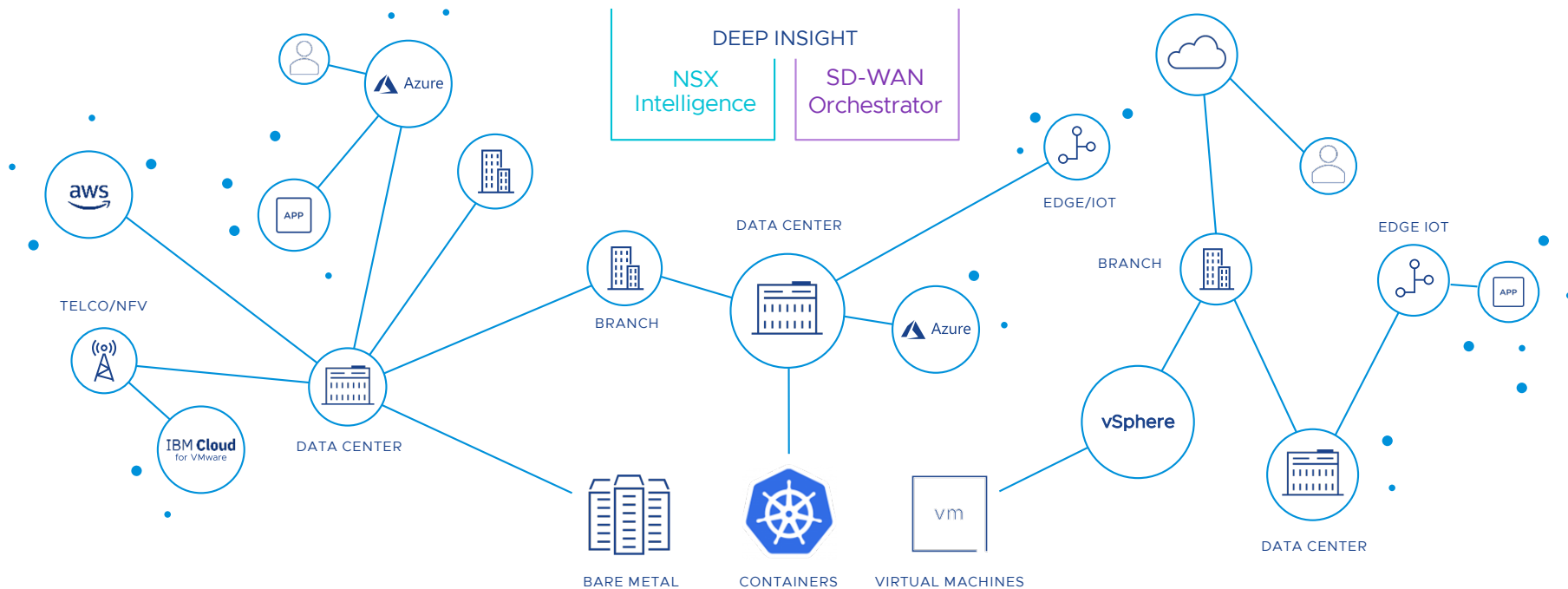
BROAD VISIBILITY

NSX + SD-WAN

DEEP INSIGHT

NSX Intelligence

SD-WAN Orchestrator





Thank You

<https://www.vmware.com/security.html>