MIS|TI™ PRESENTS

InfoSecWorld

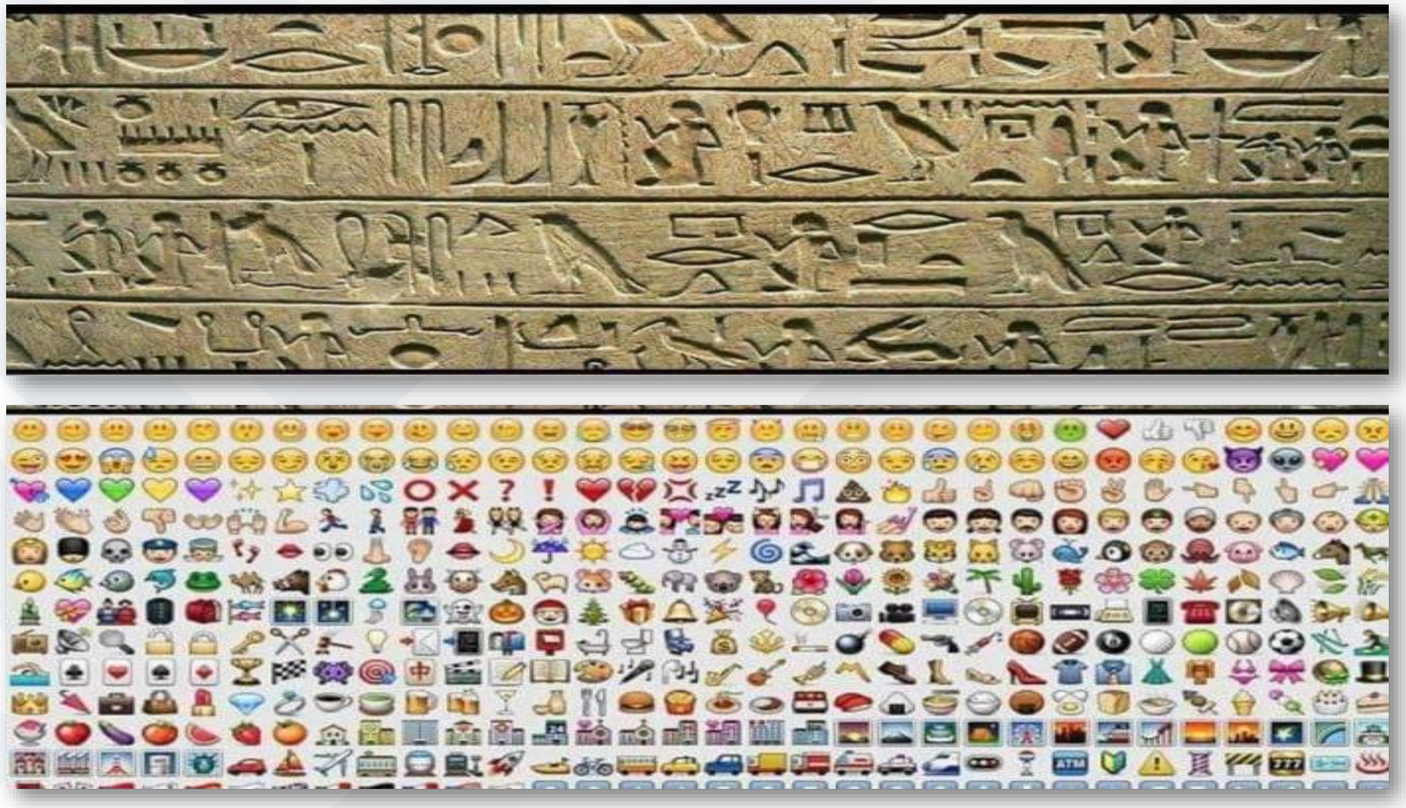
Conference & Expo 2018

SECURITY STRATEGY FOR DIGITAL TRANSFORMATION

JONATHAN NGUYEN-DUY
VICE PRESIDENT, STRATEGY & ANALYTICS
JNGUYENDUY@FORTINET.COM

AGENDA

- Digital Transformation
- Focus on DX Challenges
- Why Current Approaches Fail
- Segmentation & Virtualization
- Controls & Automation Requirements
- Applying New Security Approach

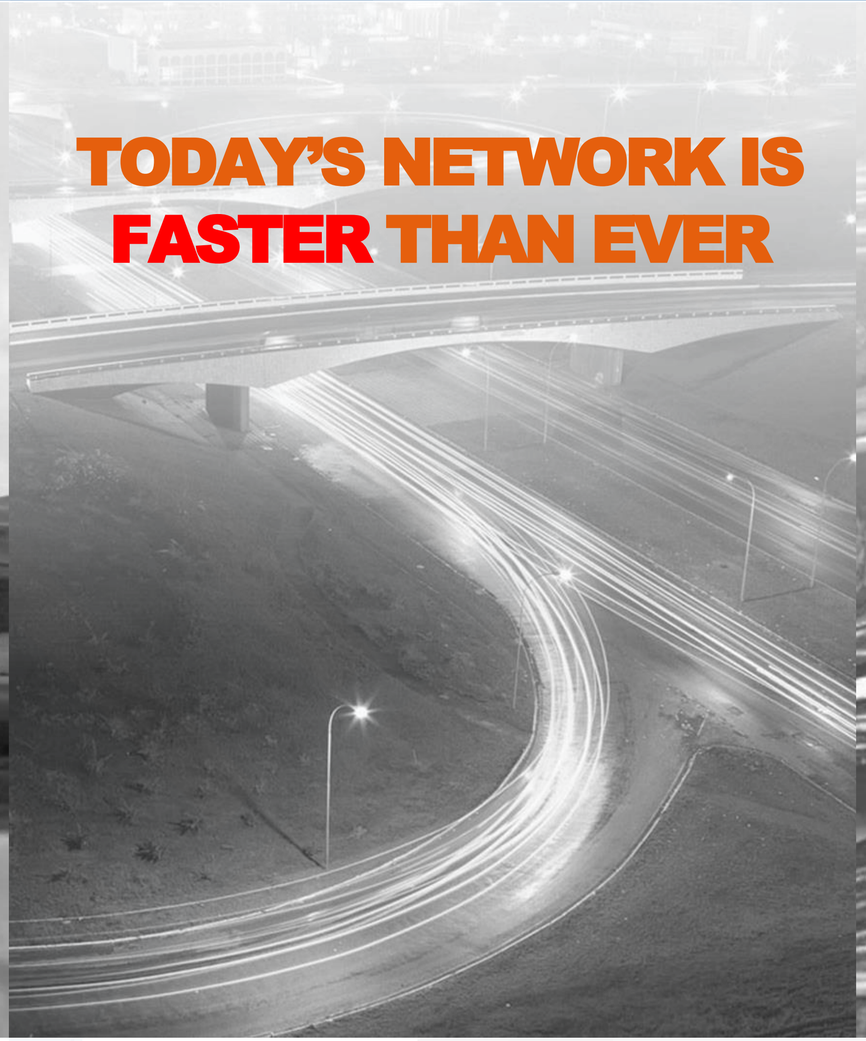


CYBER CHANGES SINCE 2007

	2007	2017
Threat Actors	<50	>1,000
Threat Types	<50	>1,000,000
Alerts/Day (Average Per Firm)	<1,000	>1,000,000
Security Vendors	<100	>2,300
VC Investments	<$500M	>$6B
Security Spending	<$3B	>$80B

Source: Optiv, 2017

POINT OF INFLECTION



[Digital Transformation]

integration of digital technology into all areas of a business, resulting in fundamental changes to how businesses operate and how they deliver value to customers

DIGITAL TRANSFORMATION

Digital Transformation

Omni Channel Customer Engagement

Empower Your Employees

Optimize Your Business

Transform from Products to CX

Digital Technology

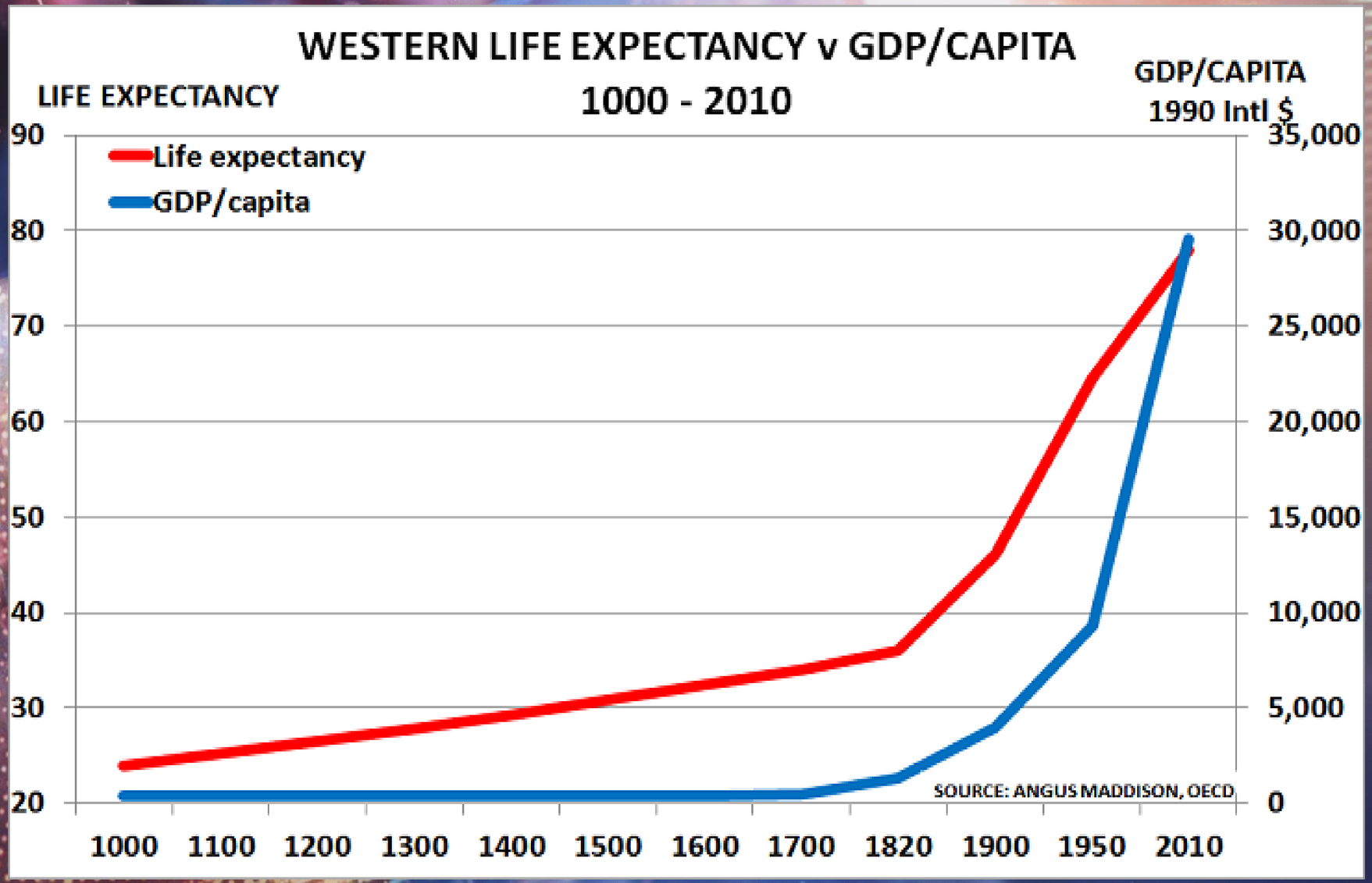
REAL LIFE DX – EMIRATES AIRLINE

Goal is to transform Emirates into the leading customer-centric, technology-enabled travel experience enterprise

- AI or robotics to reconstruct processes
- Efficiencies through task simplification so more tasks can be tackled
- Blockchain as revolution within a revolution

DIGITAL TRANSFORMATION IMPACT

Dramatic economic and quality of life improvements



Source: Paul Hodges, Economic Growth 2015

SECURING DATA AT SPEED & SCALE

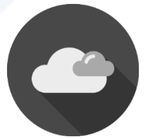
"…in the digital era, [security] focus needs to shift from securing network perimeters to safeguarding data spread across systems, devices, and the cloud."

MIT Technology Review, 2017

Mobile Devices

Augmented Reality/Wearables

IoT Platforms



Cloud Computing

Bid Data Analytics and Advanced Algorithms

Multi-level Customer Interaction and Customer Profiling

3D Printing

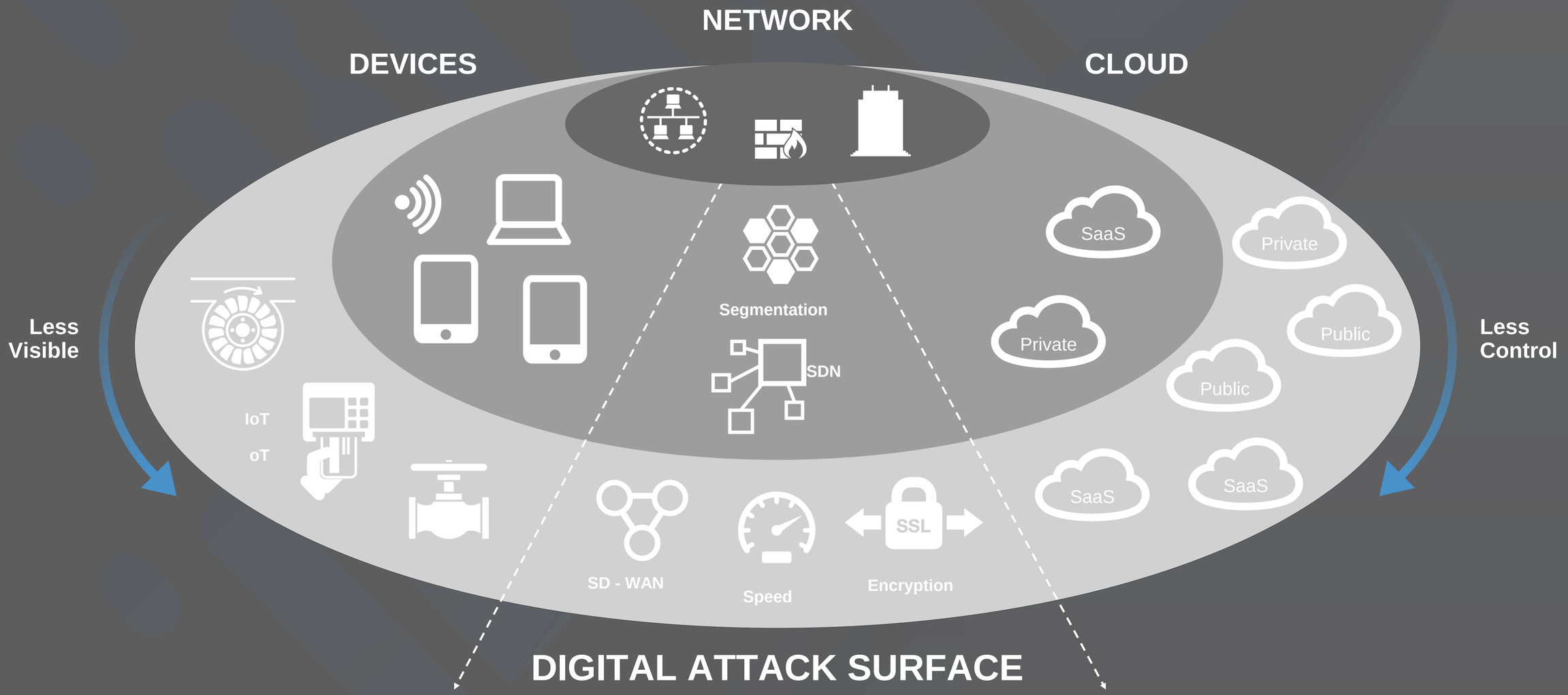
Location Detection Technologies

Smart Sensor

Advanced Human-machine Interfaces

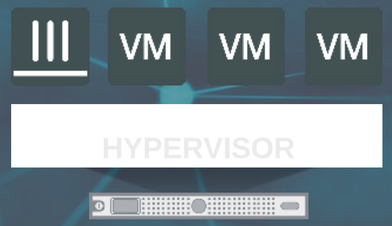
FOCUS 1: VIRTUALIZATION & CLOUD

DX CREATES A DIGITAL ATTACK SURFACE WHICH IS MUCH LARGER



The Multi-Cloud Experience…In Silos Due To Lack of Visibility & Control

VIRTUALIZATION



PRIVATE CLOUD

East-West

HYBRID

North-South

PUBLIC CLOUD

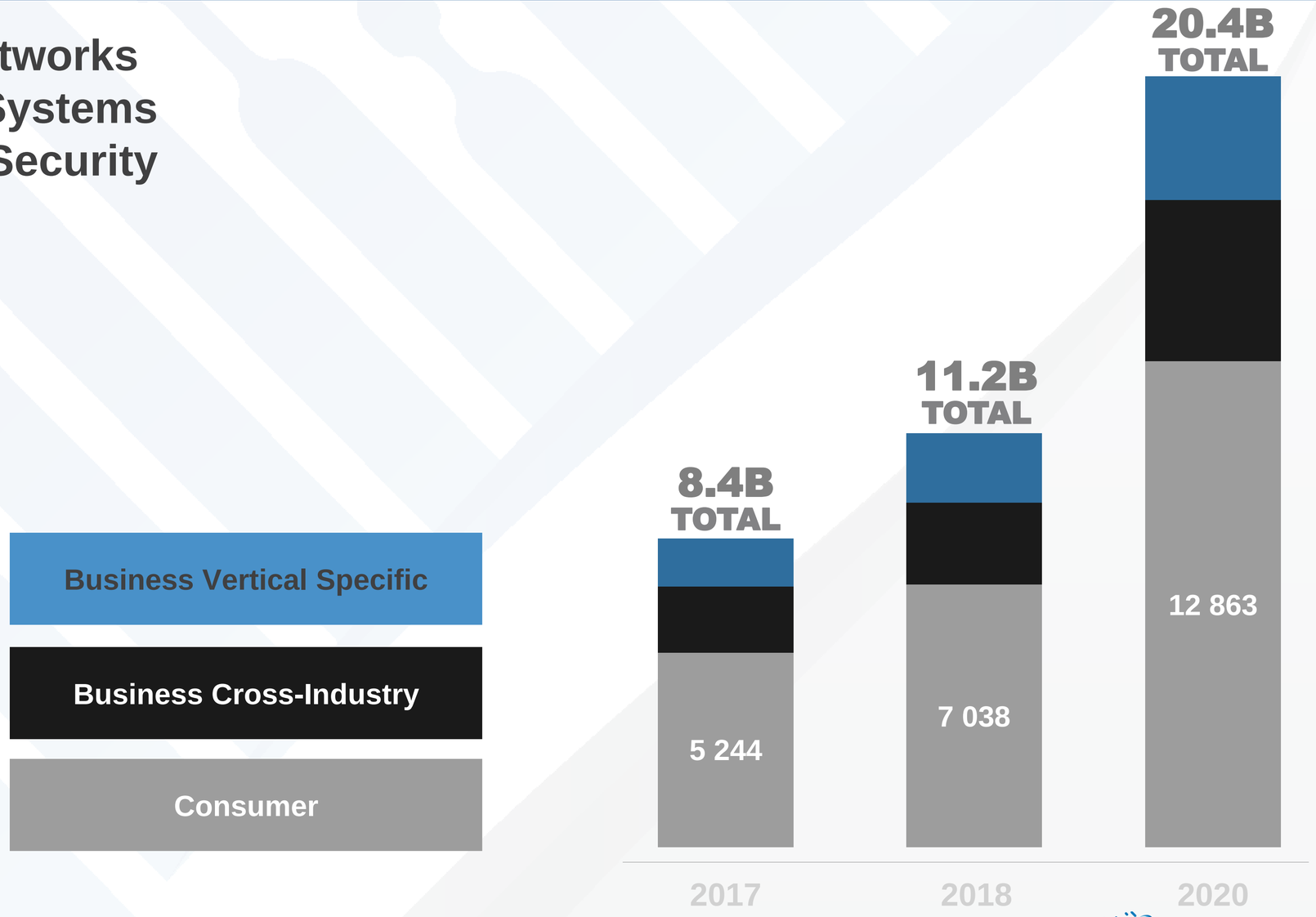
IaaS/PaaS

SaaS

FOCUS 2: INTERNET OF THINGS

EXPANDING EXPOSURE & COMPLEXITY

- Hyper-connected Networks
- Connected OT & IT Systems
- Functional & Cyber Security



Source: Gartner 2017

ADVANCED DETECTION AVAILABLE TO ALL FABRIC ELEMENTS

SECURING THE DIGITAL ECOSYSTEM

LEARN

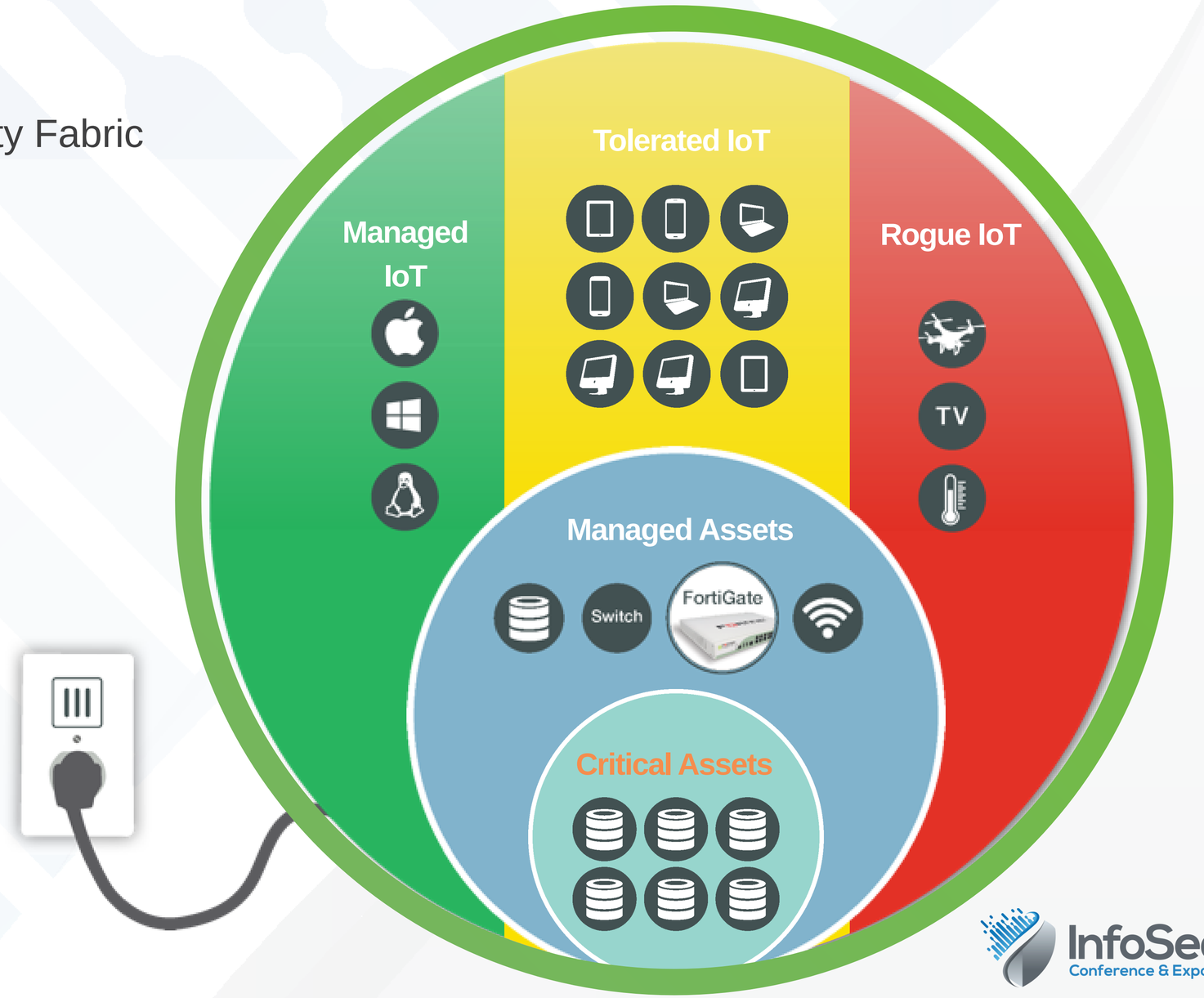
Identify devices within your Security Fabric

SEGMENT

Managed, Tolerated, Rogue

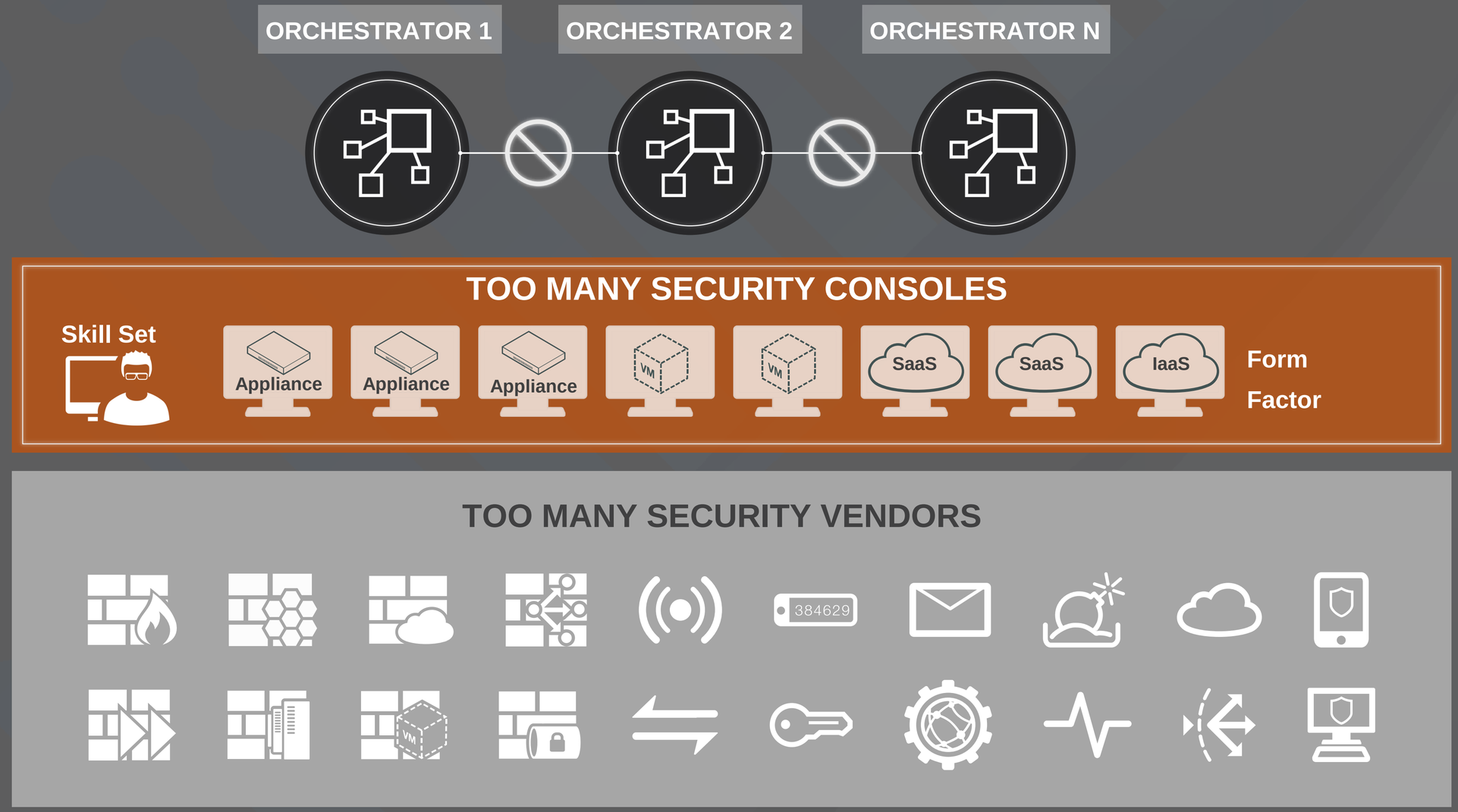
PROTECT

Security Fabric wide policies for visibility and control



FOCUS 3: THREATS & COMPLEXITY

CAN YOU KEEP ADDING MORE SECURITY VENDORS?



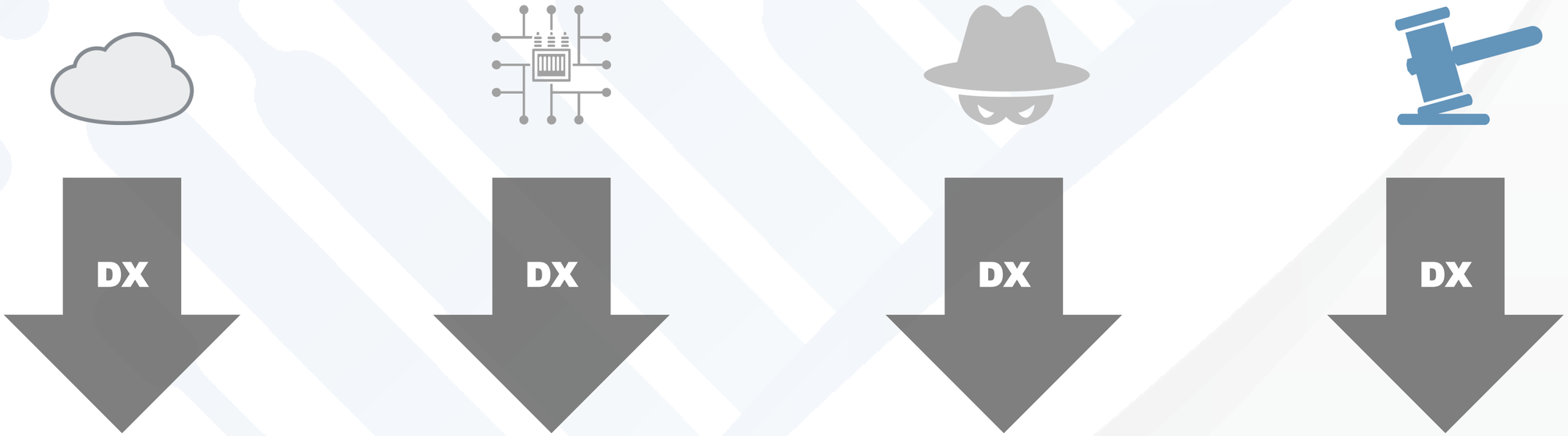
MISSING BASICS DUE TO COMPLEXITY

ELDERLY VULNERABILITIES ARE STILL DANGEROUS

90% OF ORGANIZATIONS
saw exploits for vulnerabilities
that were at least **3 YEARS OLD**

60% saw ones that were
10 OR MORE YEARS OLD

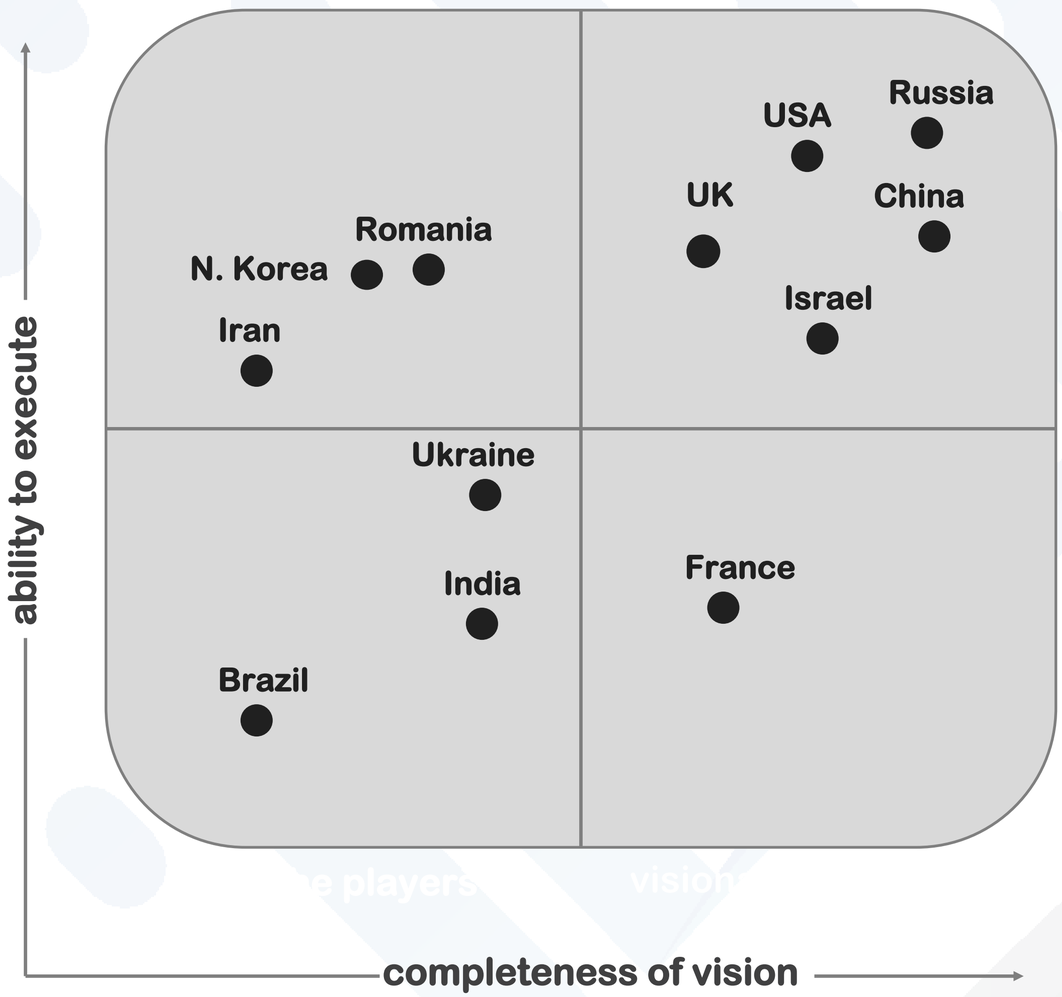
DX INCREASES COMPLEXITY



Existing Issues

BORDERLESS | **PERFORMANCE** | **COMPLEXITY**

THREAT ACTORS LEADERSHIP QUADRANT



1. USA, Russia, China, Israel, and the UK have ~ 100% success rates on offensive APT cyber operations

2. North Korea derives ~100% of its APT cyber operations capability via training and support from China

3. Romania, Iran, and Ukraine have large populations of technically trained, under-employed youth

4. Reconsideration of risk management and The disappearing perimeter

Source: Ed Amoroso

EXISTING APPROACHES ARE NOT WORKING…

- Missing basics due to complexity
- Cyber complexity is growing
- IT teams are overwhelmed
- Perimeters are disappearing
- Threat actors can break anything
- IT teams are missing security basics
- Less awareness and control
- Make complexity work for us

[Security Transformation]

is the integration of security into all areas of digital technology resulting in fundamental changes to how security is architected, deployed and operated.

SECURING THE DIGITAL ENTERPRISE

SECURITY PRINCIPLES:

01 **Holistic security plan based on simplicity and automation**

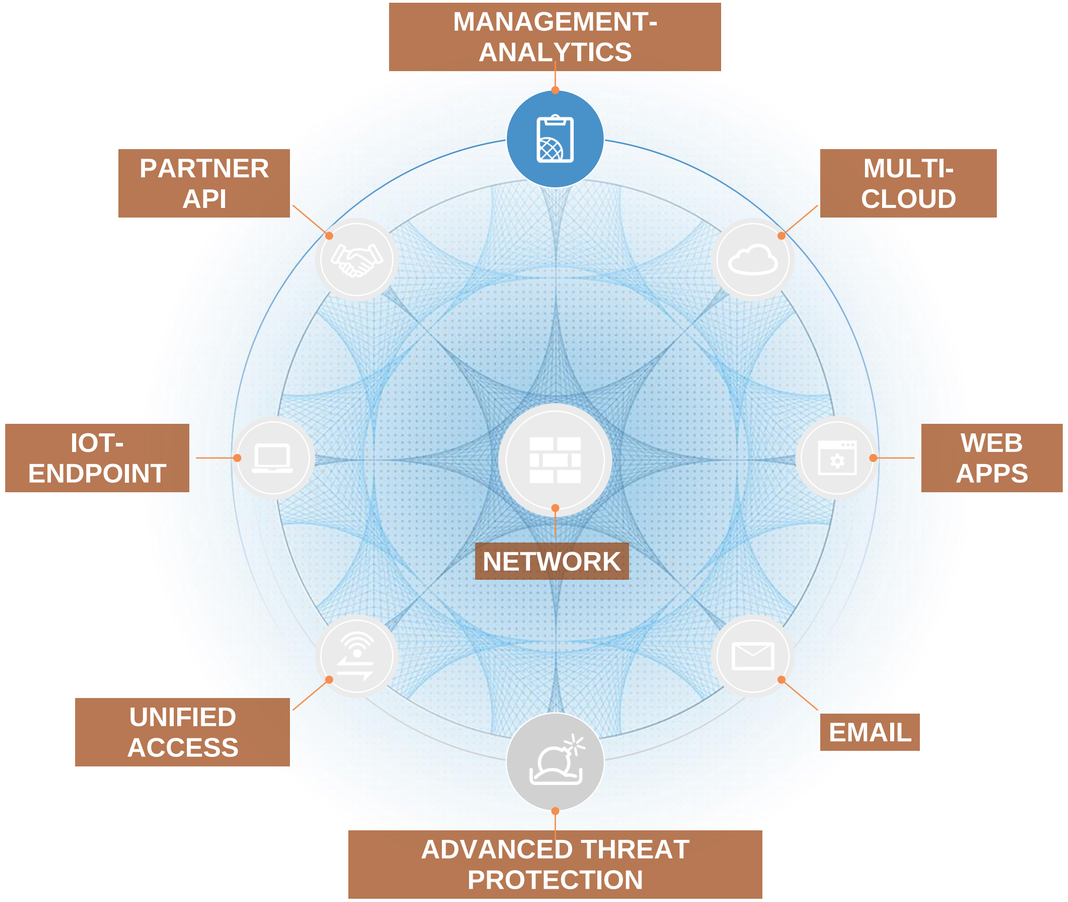
02 **Open standards so everything can connect**

03 **Single panel of glass – deep centralized visbility and control**

04 **Orchestration at Speed and Scale**

05 **Analytics & Artificial Intelligence for behavioral analysis**

APPLYING SEGMENTATION & VIRTUALIZATION



A Security Architecture that is:

BROAD

Provides Visibility and Protection Across the Entire Digital Attack Surface

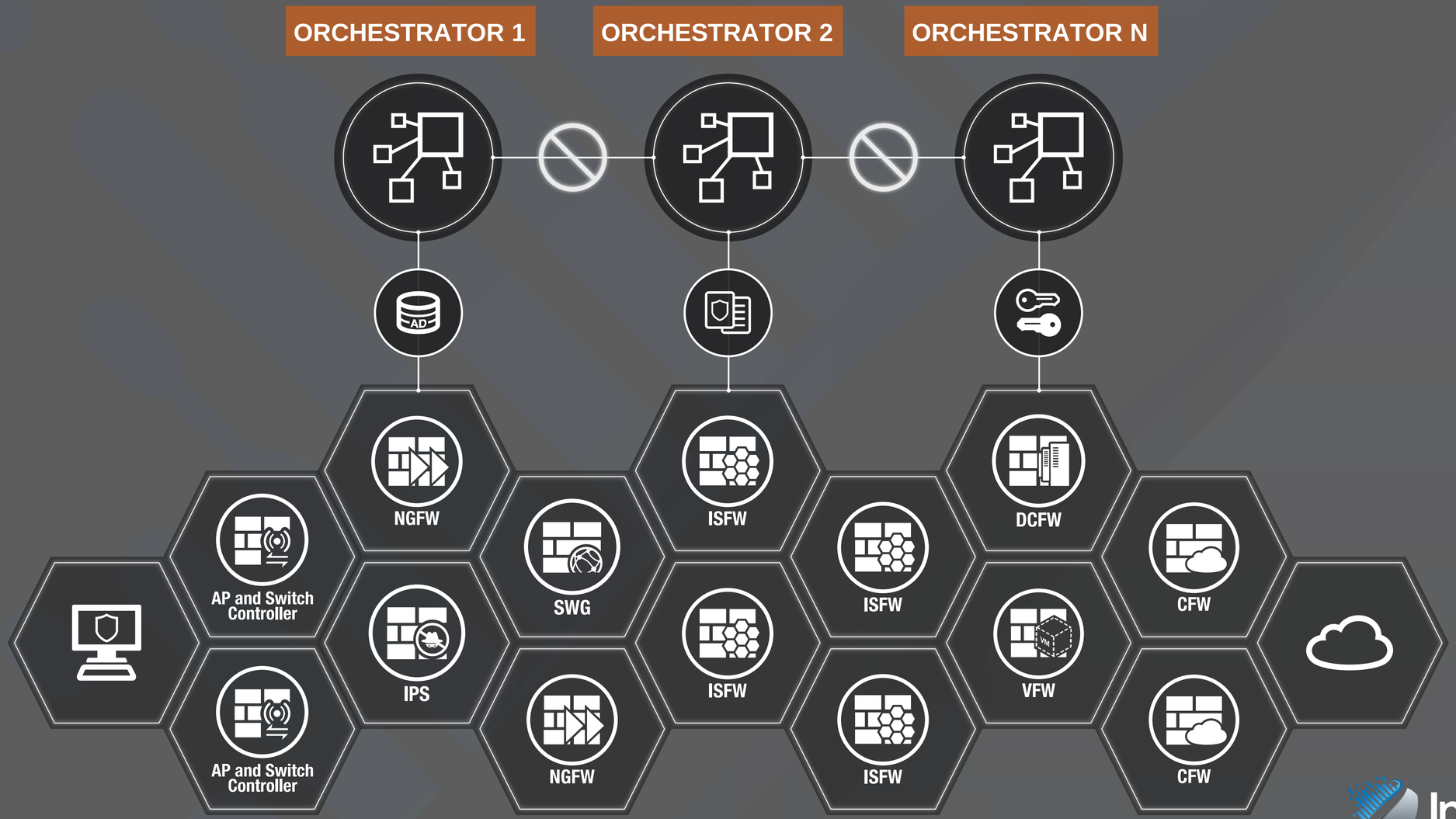
INTEGRATED

Multiple Technologies Working Together for the Detection of Advanced Threats

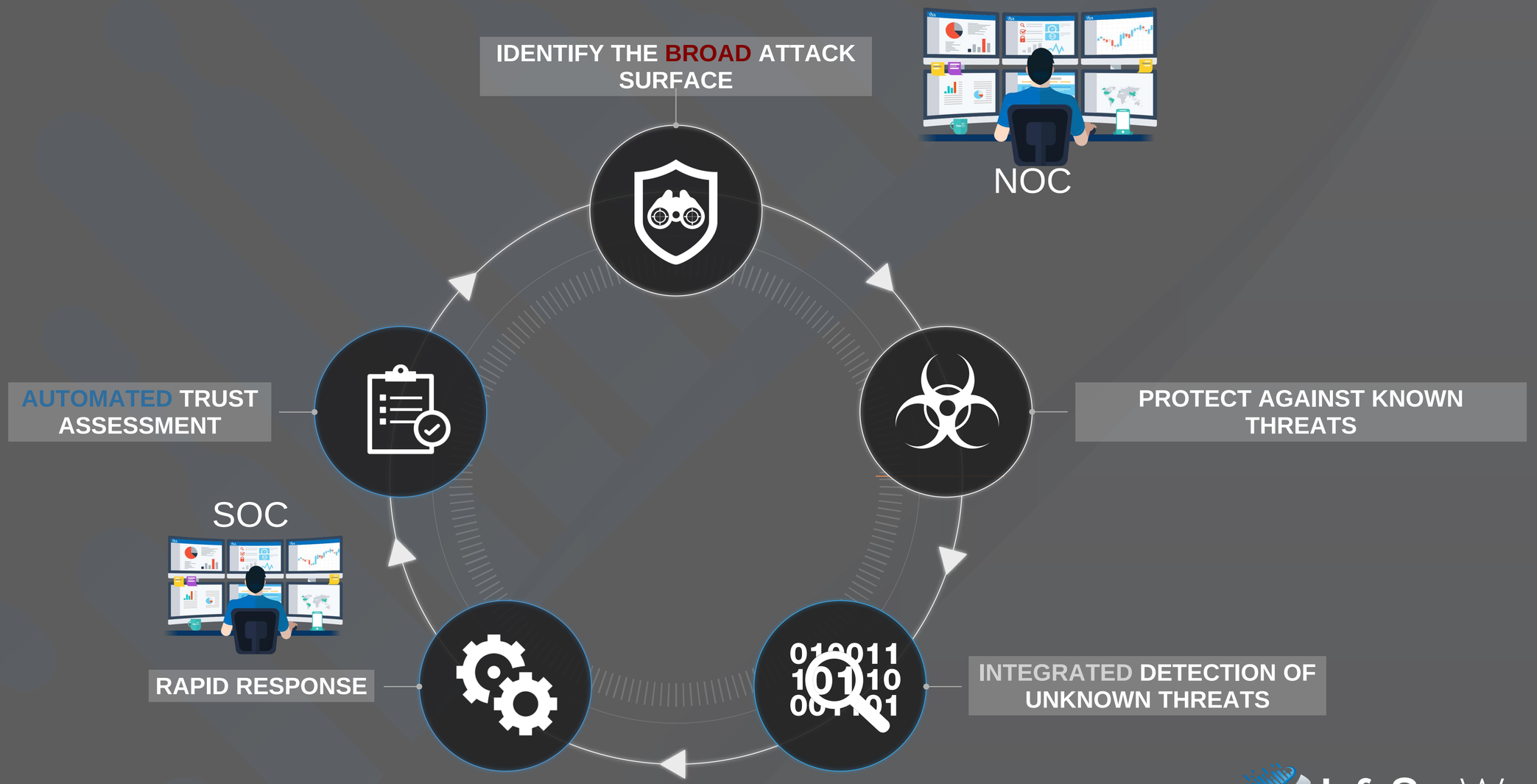
AUTOMATED

Embedded Intelligence for Automatic Response & Continuous Trust Assessment

ORCHESTRATED END-TO-END SEGMENTATION REQUIREMENTS

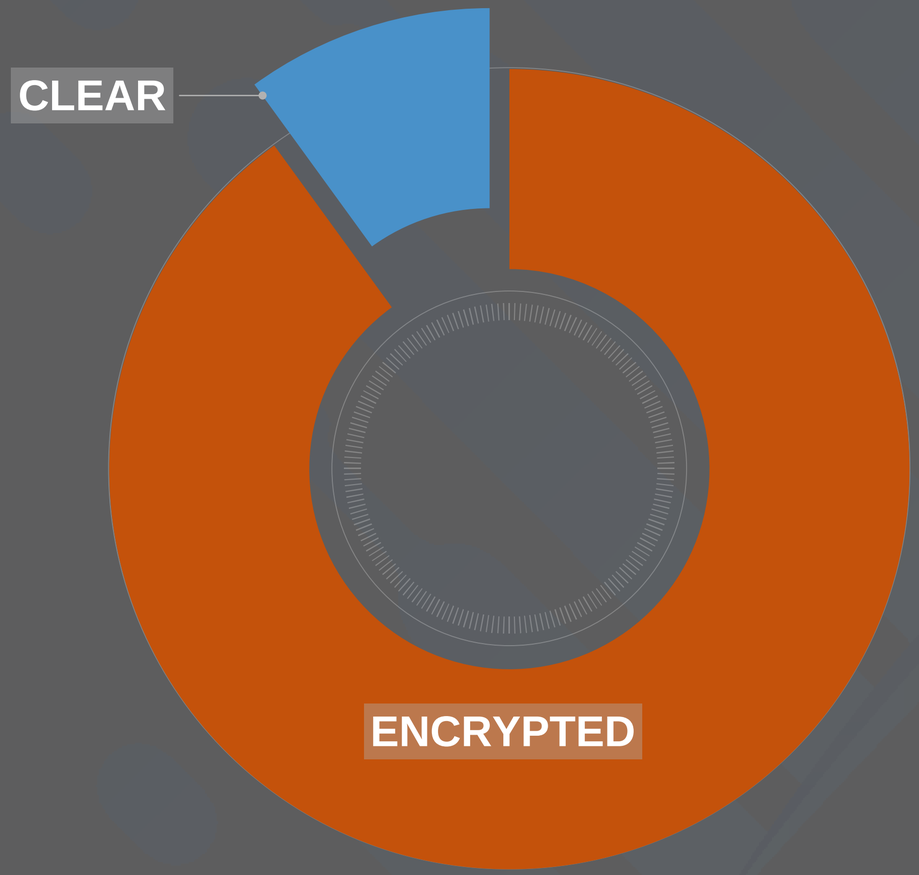


DIGITAL ATTACK SURFACE REQUIRES AN ADAPTIVE SECURITY FRAMEWORK

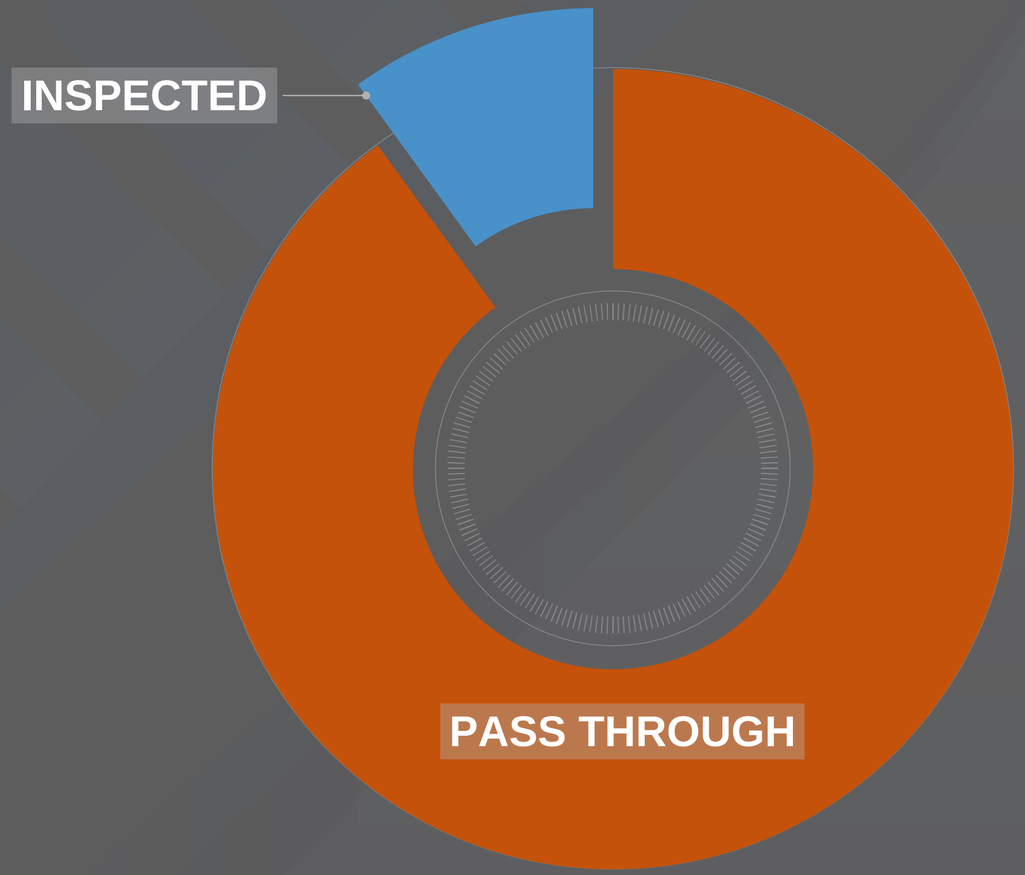


ENCRYPTION REQUIREMENTS

A Giant Hole in Enterprise Security



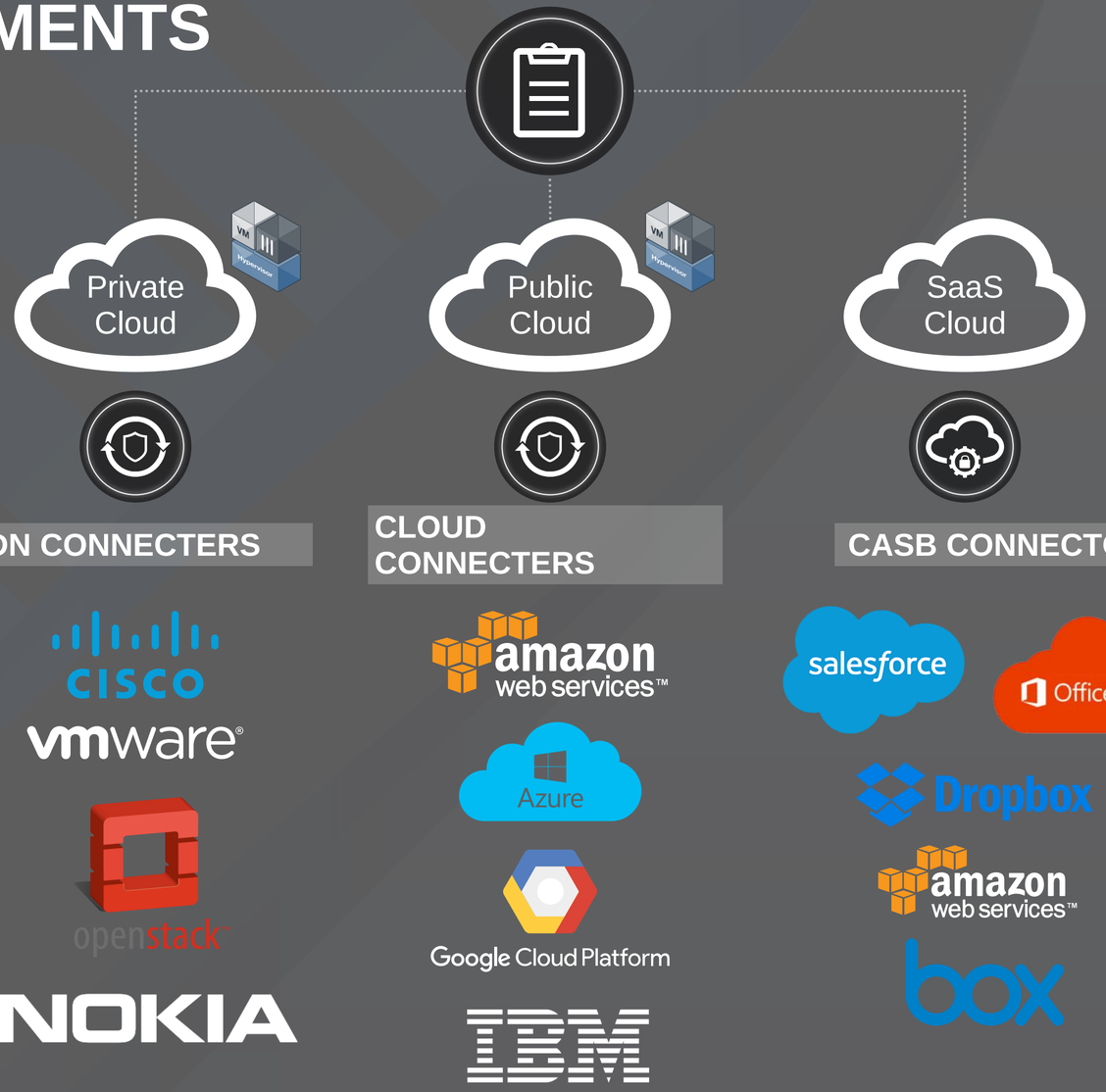
Source: Encrypted Traffic Across Google Report



Source: Gartner 2017 Enterprise Firewall Magic Quadrant : Adam Hills

MULTI-CLOUD SECURITY REQUIREMENTS

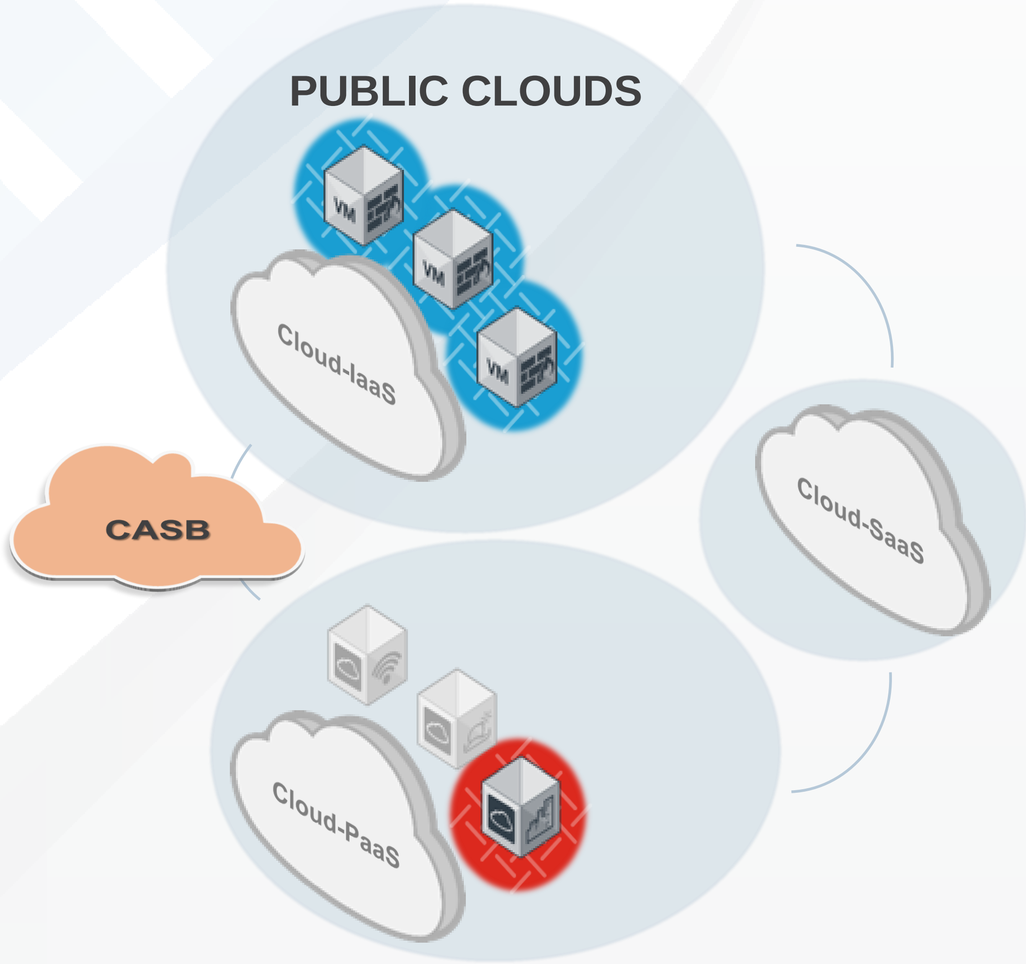
Private	Public	SaaS
Virtual Security	Cloud Security	API
Applications	Applications	Applications
Data	Data	Data
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Networking	Networking	Networking



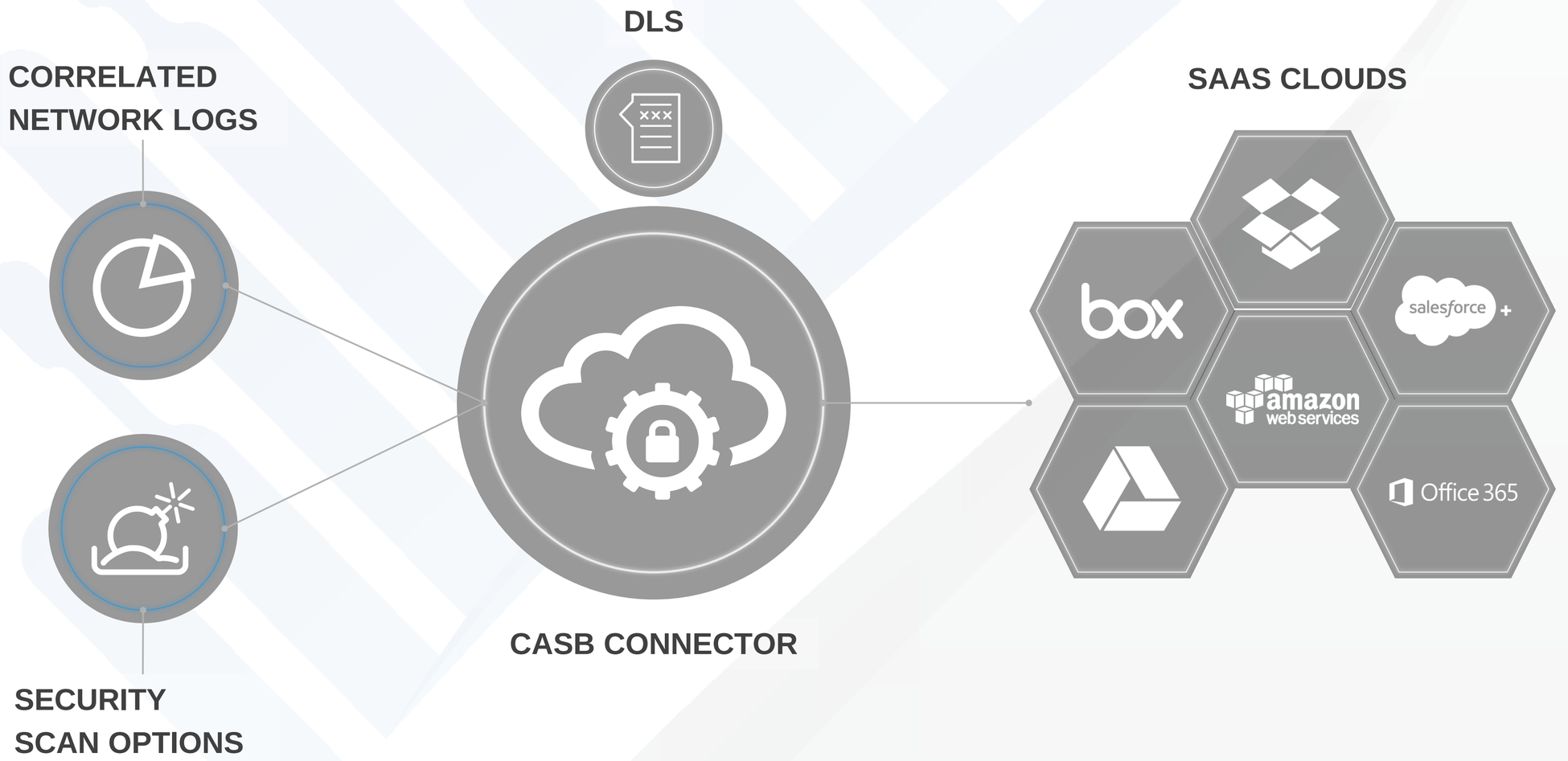
CLOUD SECURITY REQUIREMENTS

Unified Security Framework: 5 key requirements

- Auditing or pen testing
- Application security readiness
- Scalable security
- Integrated intelligence
- Automated segmentation



CASB REQUIREMENTS



SECURITY CONTROLS FOR DX

ASD Relative Security Effectiveness Rating	Mitigation Strategy	ASD Potential User Resistance	Fortinet Upfront & Ongoing Cost	Fortinet Solution
Mitigation Strategies to Prevent Malware Delivery and Execution				
Essential	Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Medium	Low	FortiGate Application Control FortiGuard
Essential	Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	Low	Low	FortiGate IPS FortiSandbox FortiGuard
Essential	Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Medium	Low	FortiGate Application Control FortiGuard
Essential	User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	Medium	Low	FortiGate Application Control FortiGuard
Excellent	Automated dynamic analysis of email and web content run in a sandbox, blocked if suspicious behaviour is identified e.g. network traffic, new or modified files, or other system configuration changes.	Low	Low	FortiSandbox
Excellent	Email content filtering. Whitelist allowed attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.	Medium	Low	FortiMail FortiSandbox FortiGuard
Excellent	Web content filtering. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.	Medium	Low	FortiGate Web Filtering & AV FortiCache Web Filtering & AV FortiSandbox FortiGuard
Excellent	Deny corporate computers direct Internet connectivity. Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.	Medium	Low	FortiGate FortiGate Web Filtering & AV
Excellent	Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Low	N/A	N/A
Very good	Server application hardening especially Internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive or high-availability) data.	Low	Low	FortiDB FortiWeb FortiGuard

Essential Controls

- Segmentation
- Multi-factor Authentication
- App Vulnerability Management
- Security Awareness Training

Benchmarking Against Compliance Standards

- ASD Mitigation Strategies
- PCI DSS
- ISO2700
- HIPAA
- NIST CSF
- SSAE16
- HIPAA / HITECH
- NY 23 NYCRR 500 State Fin Serv Law Part 500 of Title 23

YESTERDAY'S PRIMARY STRATEGY: DISTRIBUTED SEGMENTATION & VIRTUALIZATION

STATE OF THE ART STRATEGY: DISTRIBUTED SEGMENTATION & VIRTUALIZATION

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

JONATHAN NGUYEN-DUY
VICE PRESIDENT, STRATEGY & ANALYTICS
JNGUYENDUY@FORTINET.COM