MENA Information Security Conference 2017

On the Verge :

Combating Cyber Threats leveraging Threat Intelligence, Faster Detection & Automated Response

Threat Intelligence, The Power of Sharing

Charbel Sarkis

FORTINET®

Dealing With Today's Issues

AREAS OF GREATEST CONCERN FOR SECURITY*

Cloud	1
Vulnerability in IT systems	2
Inside Threats	3
BYOD	4
IoT	5

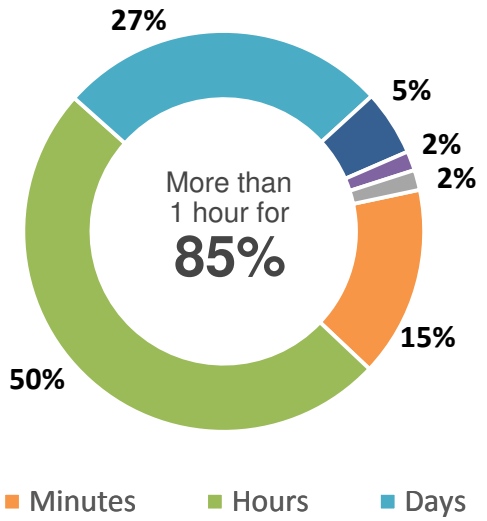
51%

OF EMEA ENTERPRISES BREACHED IN THE LAST 12 MONTHS*

3 BILLION

NEW DEVICES PER YEAR THROUGH 2020

TIME TO DETECT BREACH*



MENA INFORMATION SECURITY CONFERENCE 2017

FORTINET®

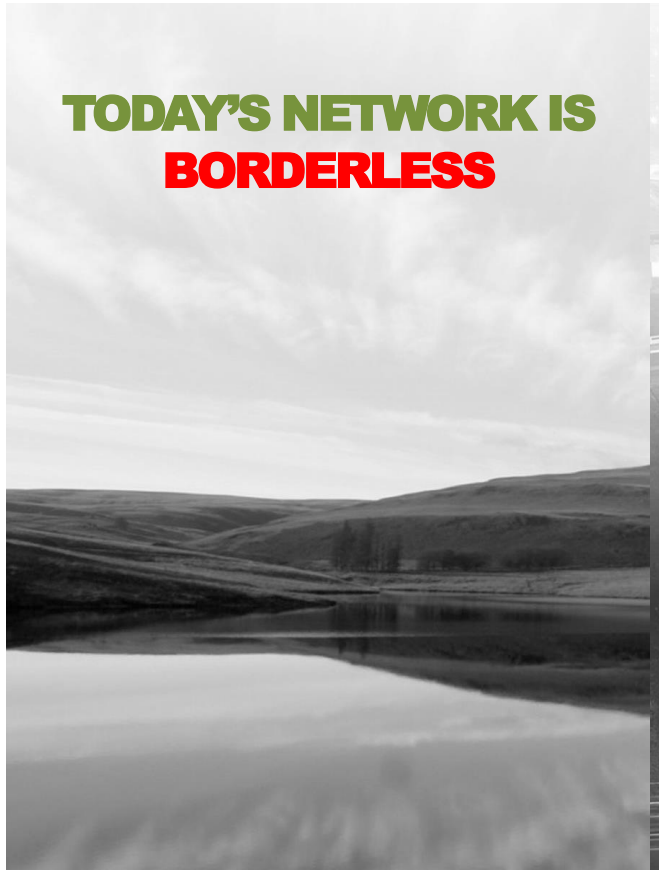
And Those of Tomorrow

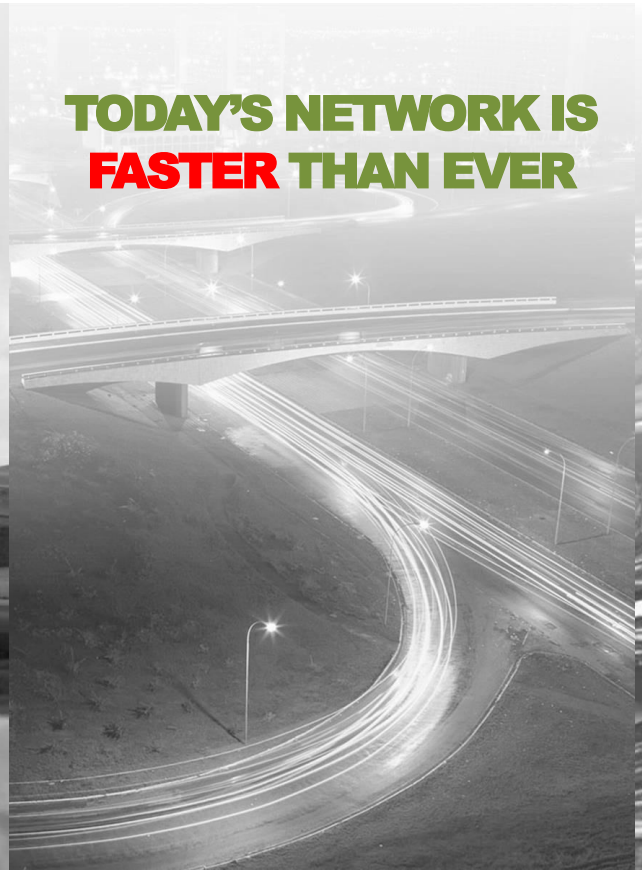
INFRASTRUCTURE EVOLUTION

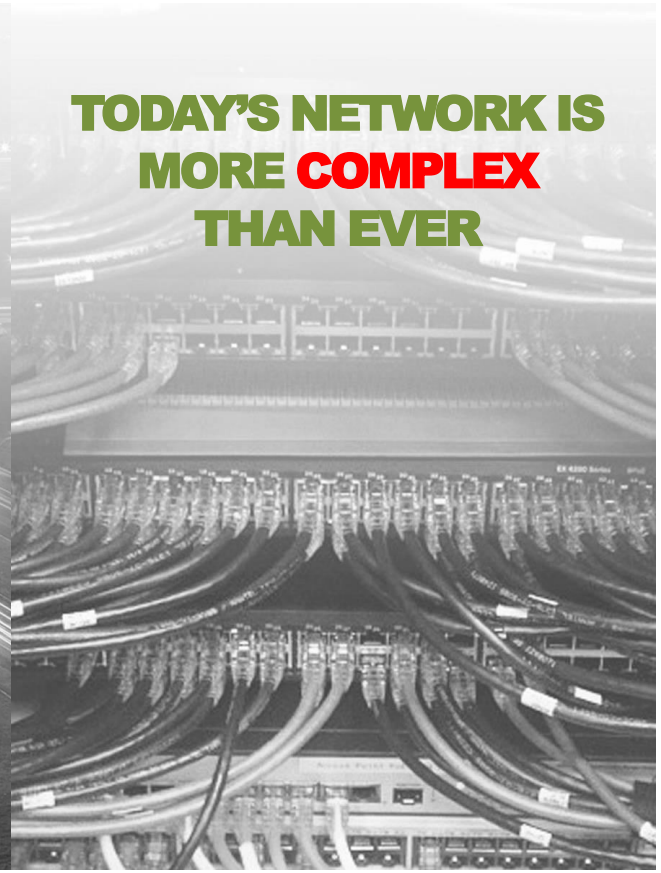
EVOLVING THREAT LANDSCAPE

REGULATION, COMPLIANCE AND CERTIFICATION

The State of the Enterprise Network

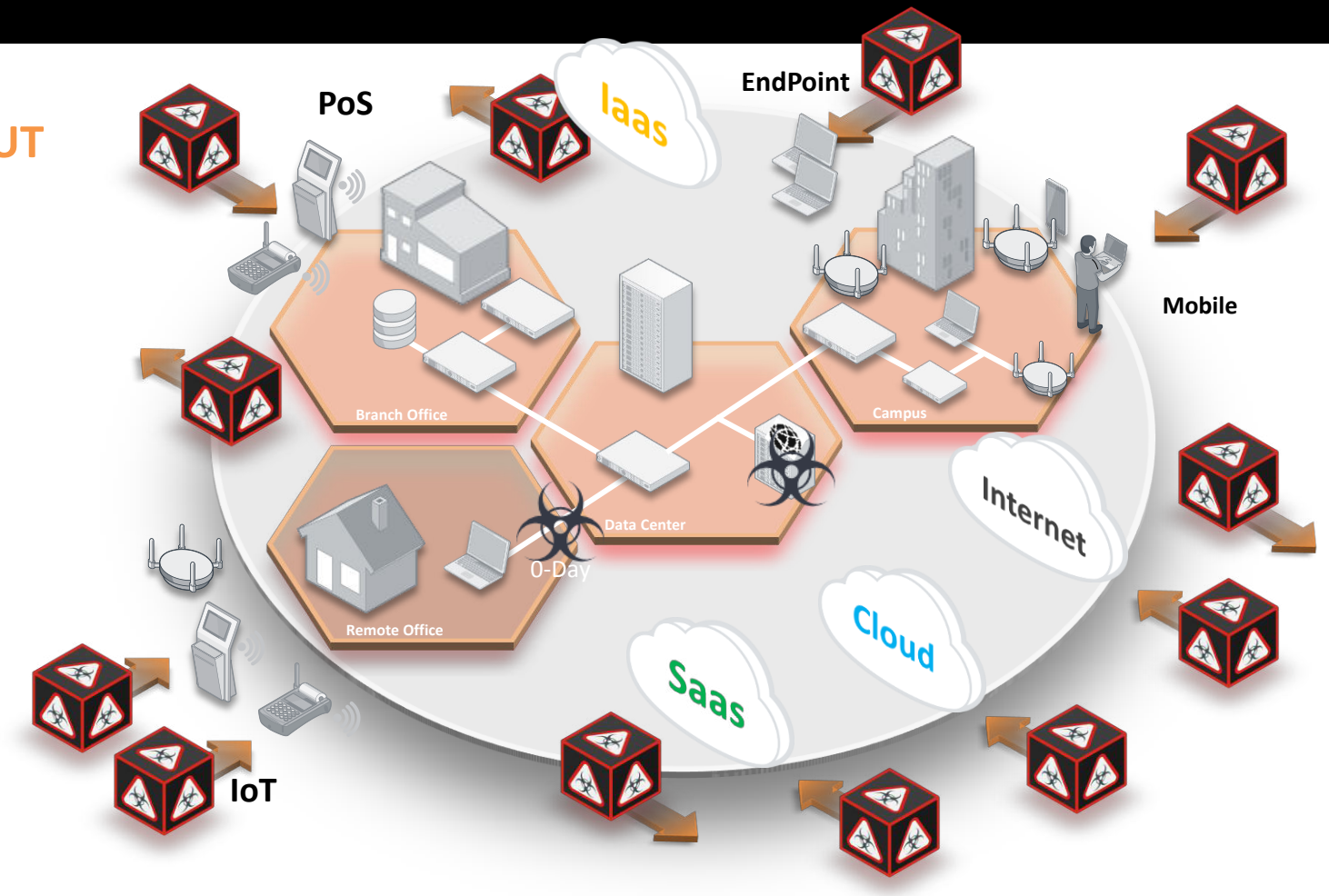






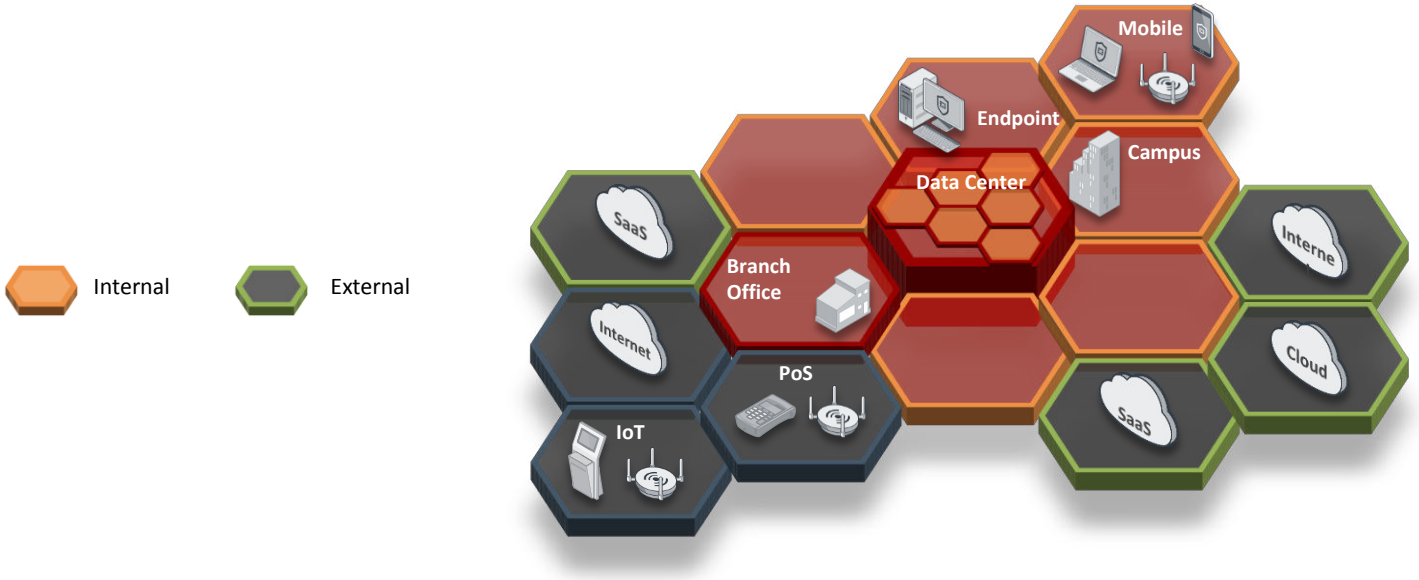
Borderless

More Ways IN
More Ways OUT



Containing the Borderless

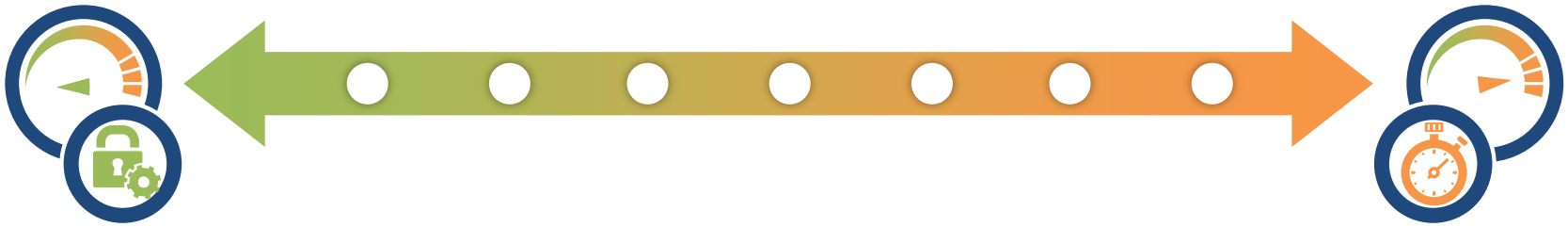
- Perimeter and internal security in equal doses
  - » Segmentation Strategies
- Security extending outward from the core to the access layer
- Integration between the elements of the broader network security solution



FASTER

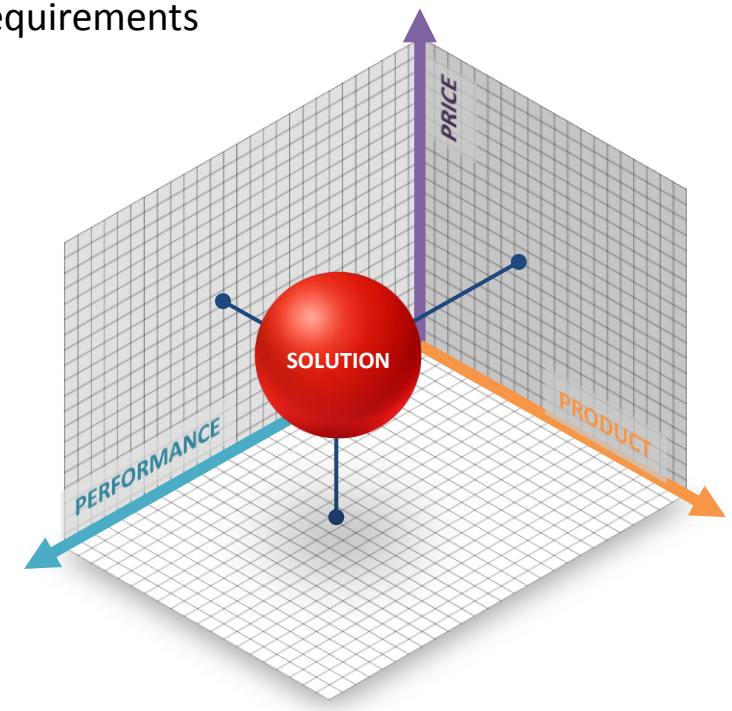
Which Compromise Do You Make?

BUSINESS SECURITY **INFRASTRUCTURE SPEED**



Powering the Solution

- Integration into the underlying network, not resting on top
- Scalability
  - » In terms of size and function
  - » Current and projected performance requirements
  - » Of the security model – the 3 P's



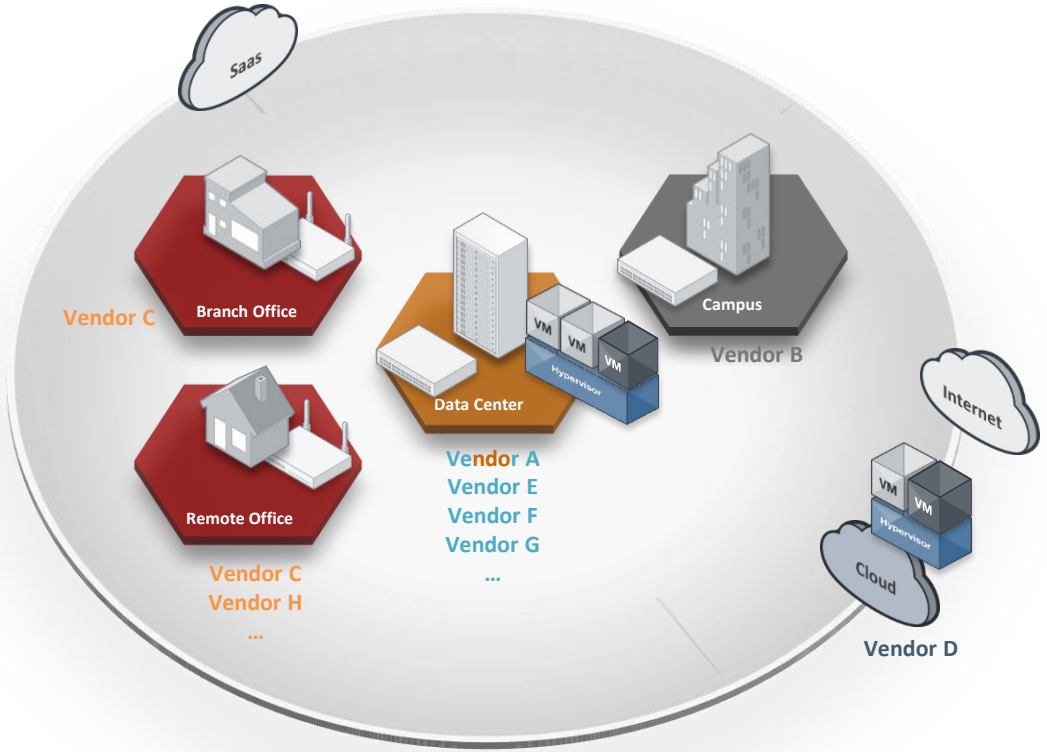
COMPLEX

Complexity Decreases Security Effectiveness

Each product is **“Silo’d”**

No interaction

No integration



Eliminating Complexity

- Individual elements that work together, automatically
- Pervasive threat intelligence
- Single pane of glass management

Addressing Today's Security Challenges

Broad – A Fabric Gives You Complete Visibility, Coverage and Flexibility Across The Entire Dynamic Attack Surface

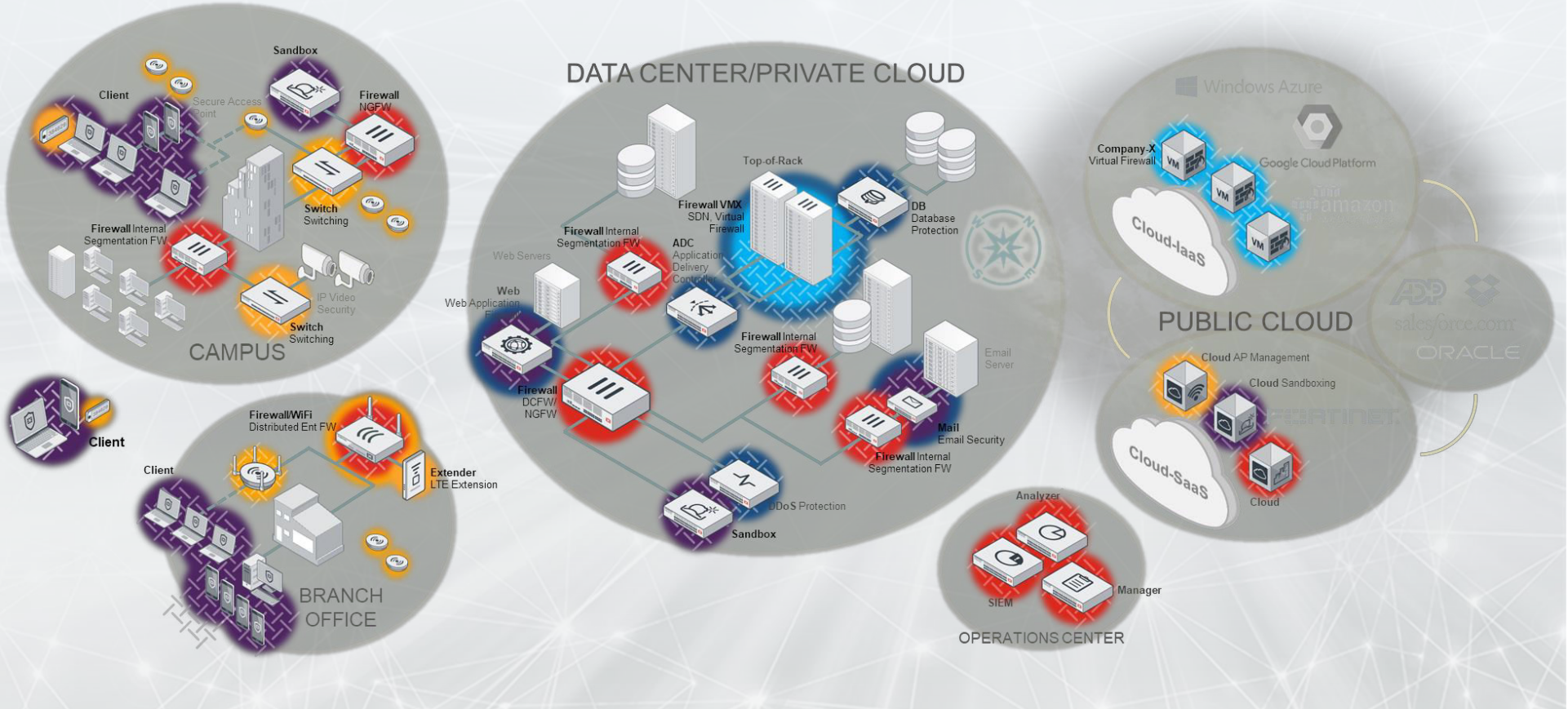
Visibility

Coverage

- Cloud Security
- Application Security
- Network Security
- Access Security
- Client/IoT Security

Flexible/Open

Broad – A Fabric Allows Flexible, Open Integration of Multiple Security Technologies

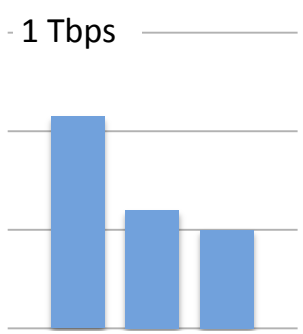


Powerful – Increasing Performance Reduces The Burden on Infrastructure

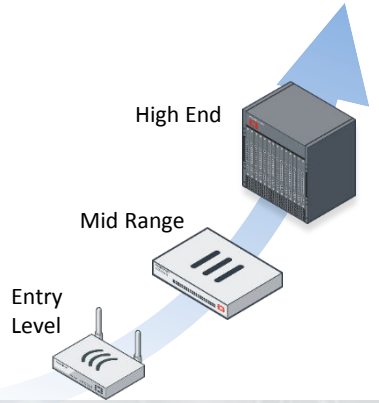
Security Processors (SPU's)

- NP6 — Accelerates Network Traffic
- CP9 — Accelerates Content Inspection
- SoC3 — Optimized Performance for Entry Level

Parallel Path Processing



Comprehensive Range



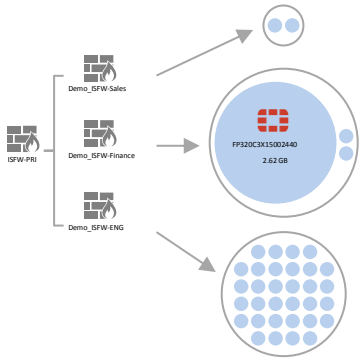
Automated to Provide a Fast, Coordinated Response to Threats

Global & Local

Known Threats
FortiGuard

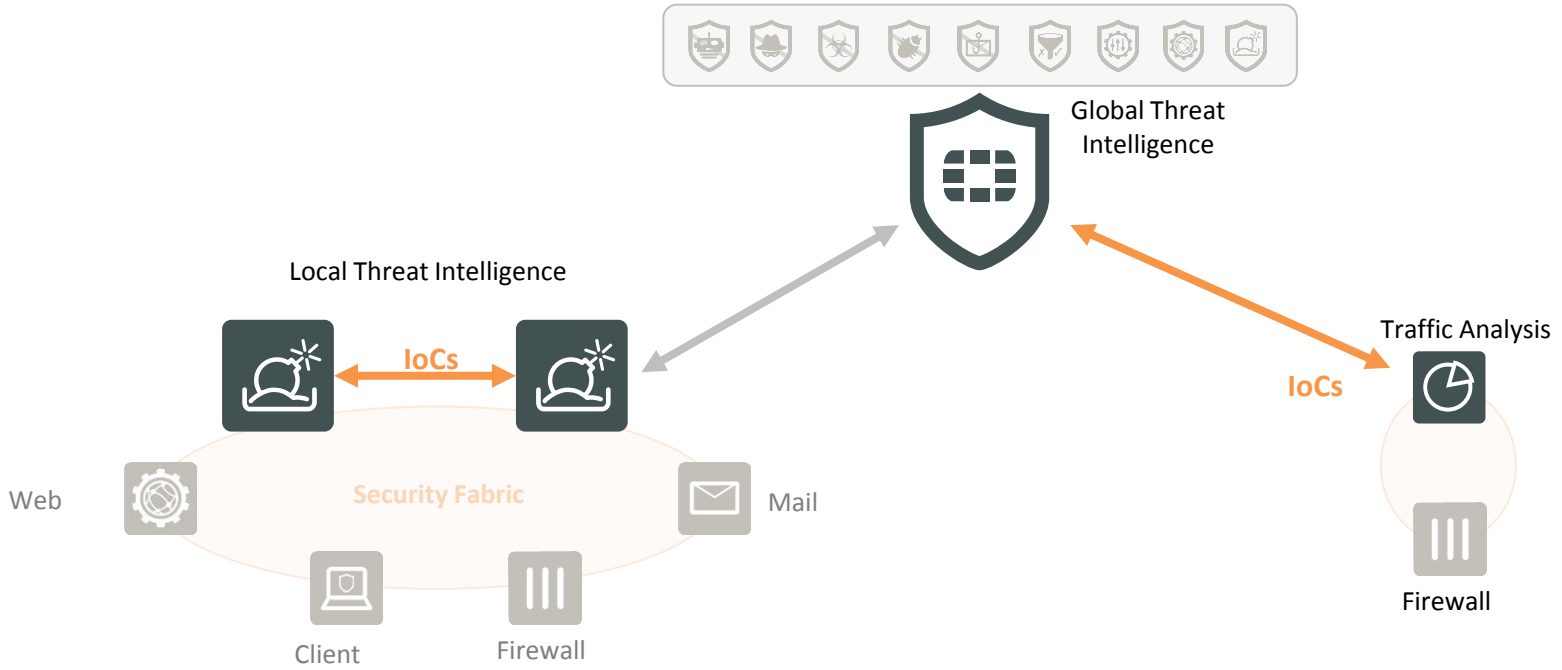
Unknown Threats
FortiSandbox

Audit & Recommend



Coordinated

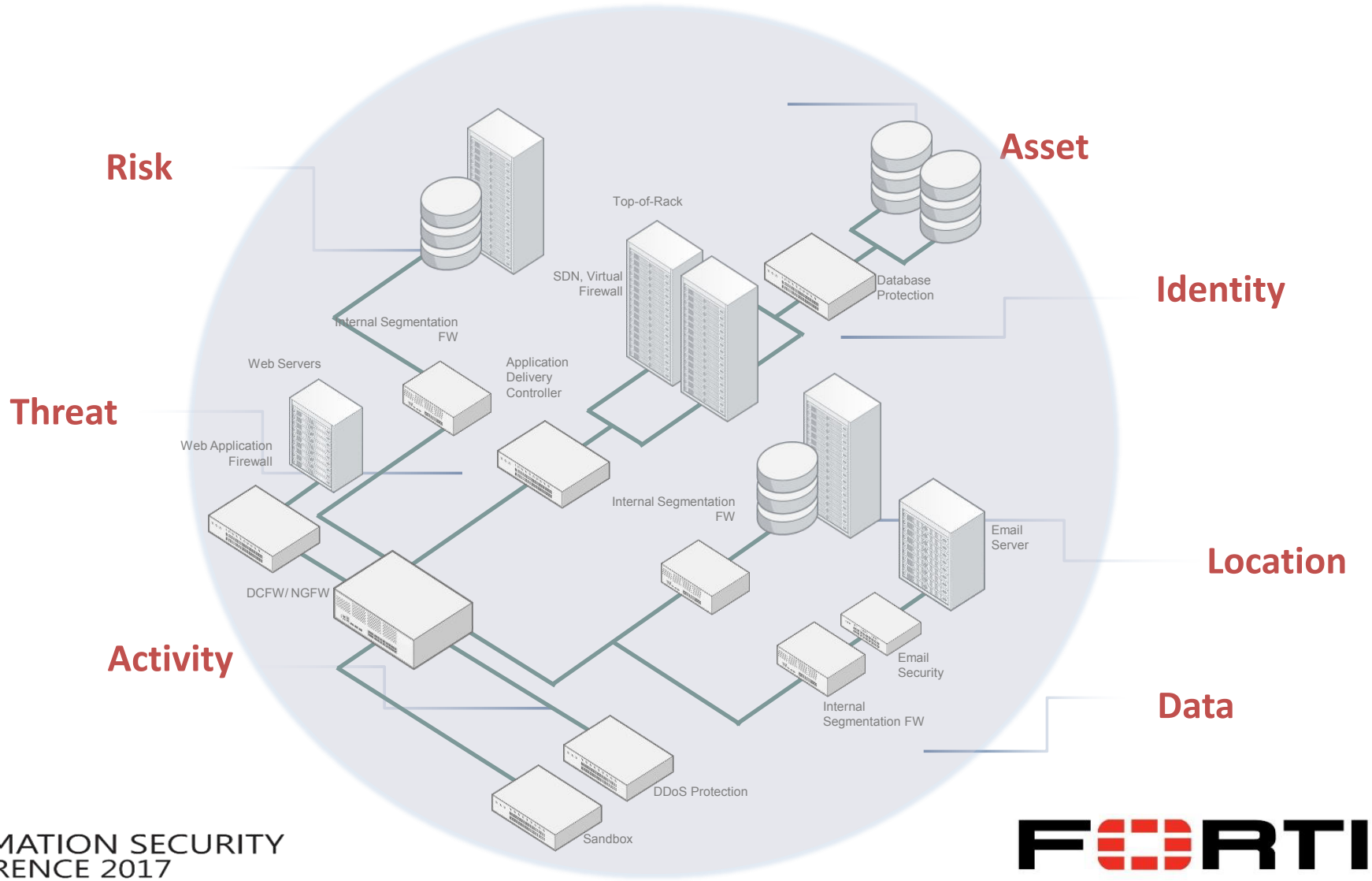
Rapid Sharing of Global and Local Threat Intelligence



Clustered Local Intelligence distributed throughout the Security Fabric speeds mitigation

Correlation of Global IoCs and networking logs pinpoints new threats

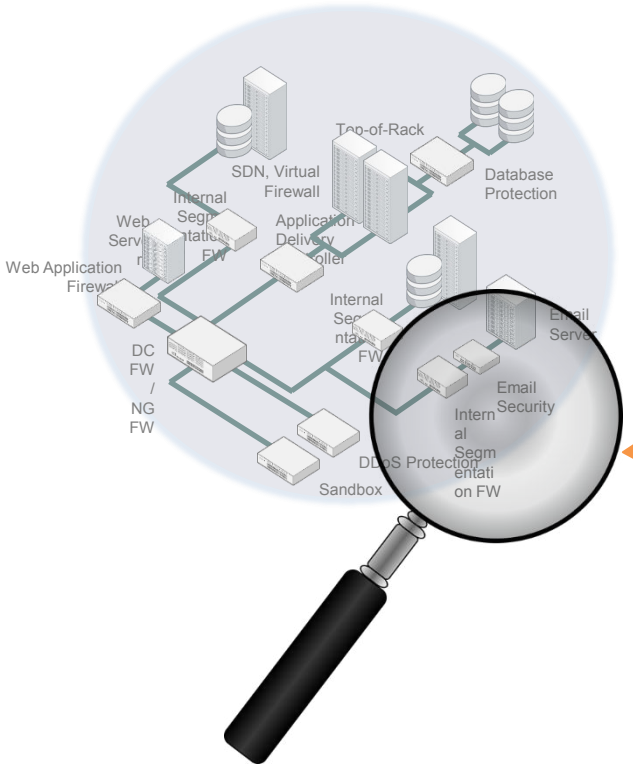
Threat Intelligence Sharing and IOCs



MENA INFORMATION SECURITY CONFERENCE 2017

FORTINET®

Threat Intelligence Sharing and IOCs



- Attack telemetry from clients
- Malware samples
- Public & private information sources
- Website monitoring
- Attack signatures
- Domain names
- Host names
- IP addresses
- File names
- Registry data
- Vulnerabilities
- Catalogued malware

Takeout Menu

Broad	Powerful	Automated
Deeper **visibility and control** throughout a Security Fabric **to reduce the attack surface from IoT to cloud**	**Accelerated** cloud-scale and security processor-based appliances with coordinated logging **to enable maximum threat protection without affecting performance**	**More efficient operations** with a Security Fabric audit/recommendations, intelligence sharing, and NOC views Multivendor integration for maximum ROI

THANK YOU