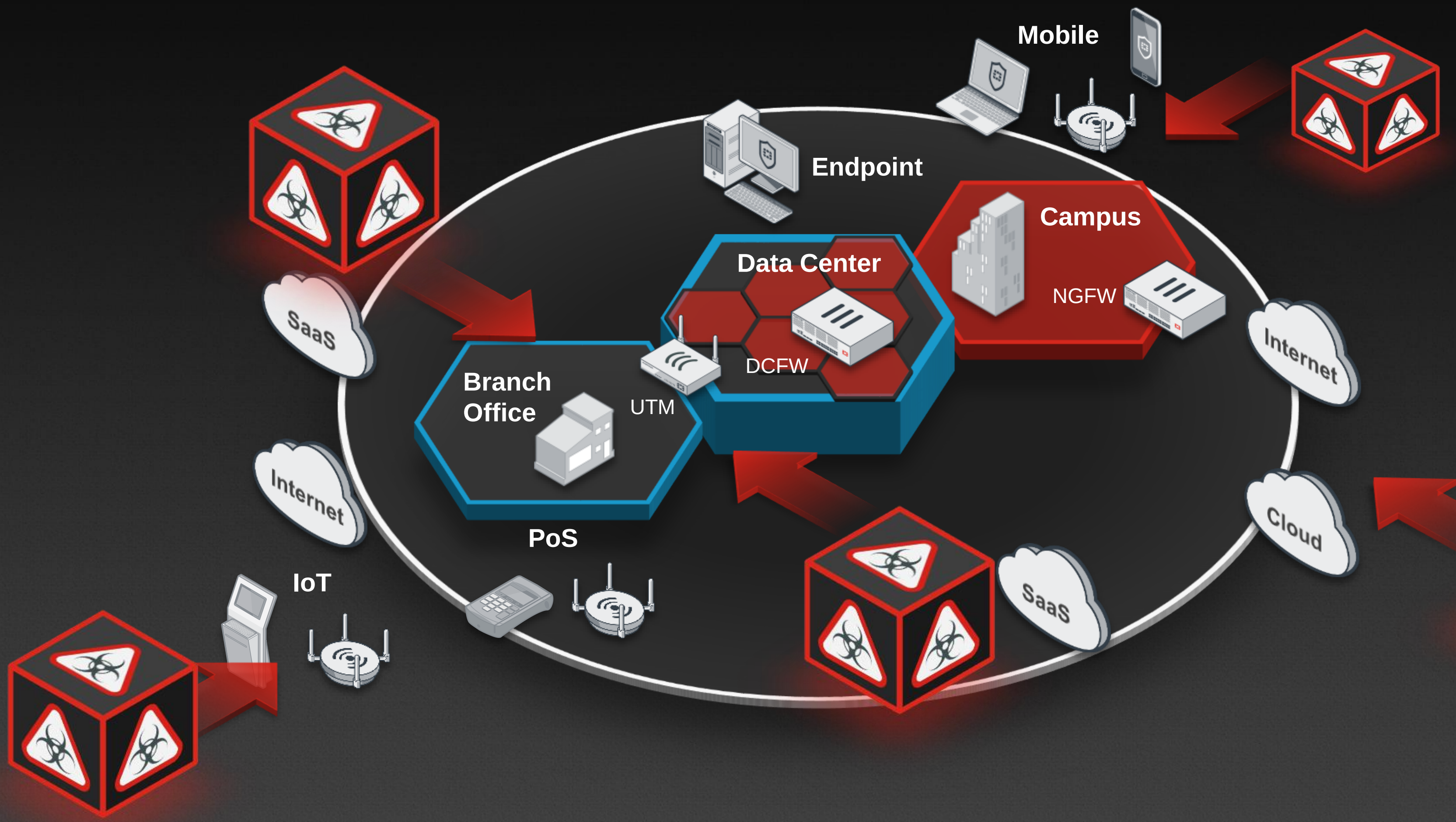
FortiSIEM,
nový komponent Fortinet Security Fabric

Zsolt Géczi, CEH

15.11.2016, ITAPA

The attack surface has increased dramatically, everywhere, inside and out.



🟥 Internal
⬡ External

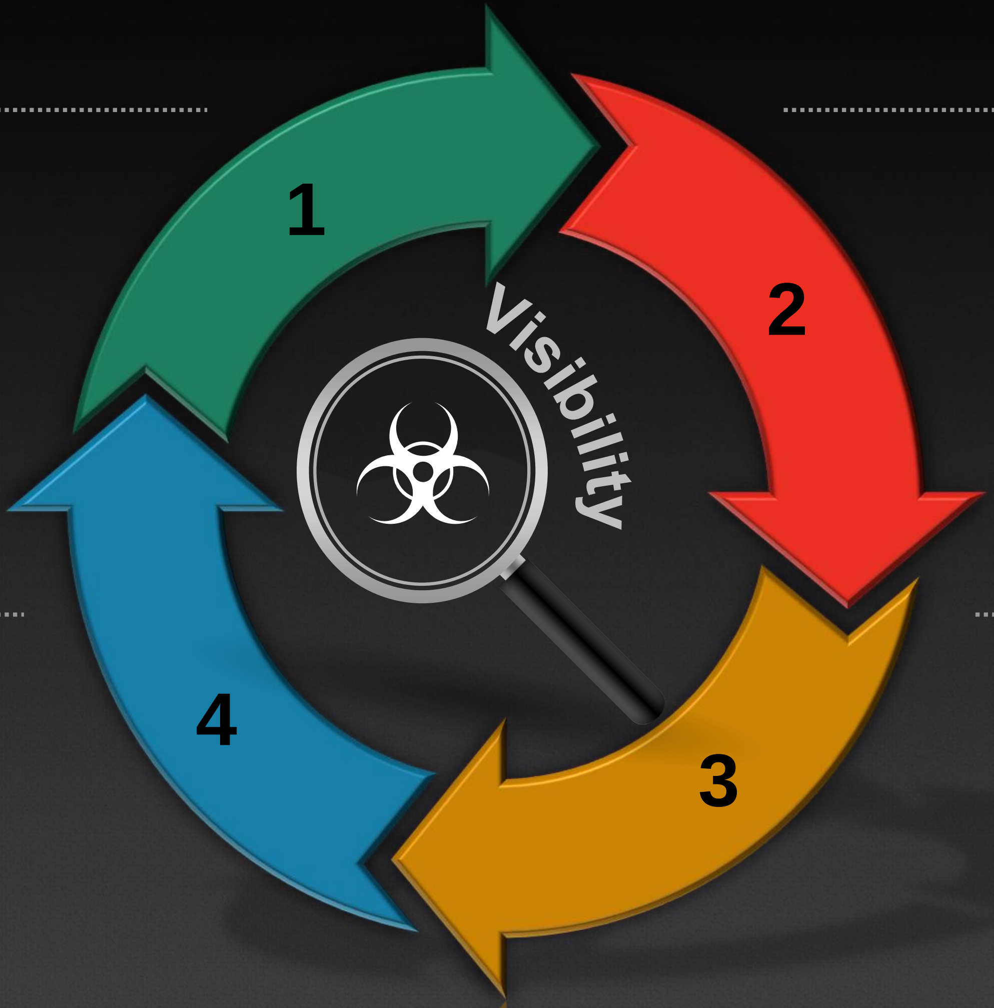
Continuous Monitoring and Analytics

Prepare

Segmentation
Processes
Training

Prevent

Harden
Isolate
Network
Application
Endpoint



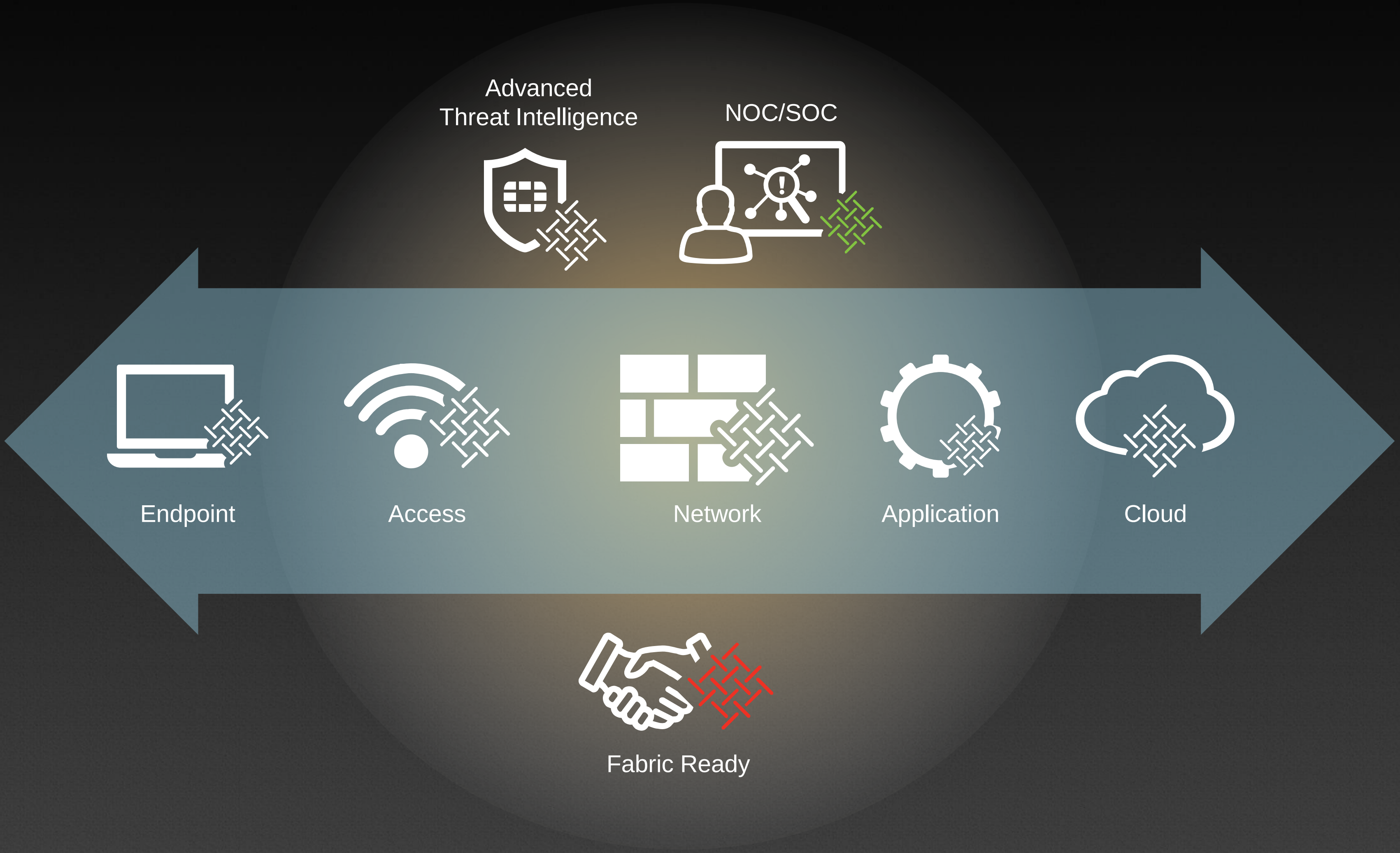
Respond

Contain
Remediate
Clean

Detect

ATP
>>> SIEM <<<
TIS

Fortinet Security Fabric



- **Scalable**
- **Aware**
- **Secure**
- **Actionable**
- **Open**

FortiSIEM

Typical NOC/SOC Environment

NOC

PRTG NETWORK MONITOR

Nagios

Kaseya

ScienceLogic

WIRESHARK

TICKETING SYSTEMS

servicenow

ConnectWise

Remedy Corporation

SOC

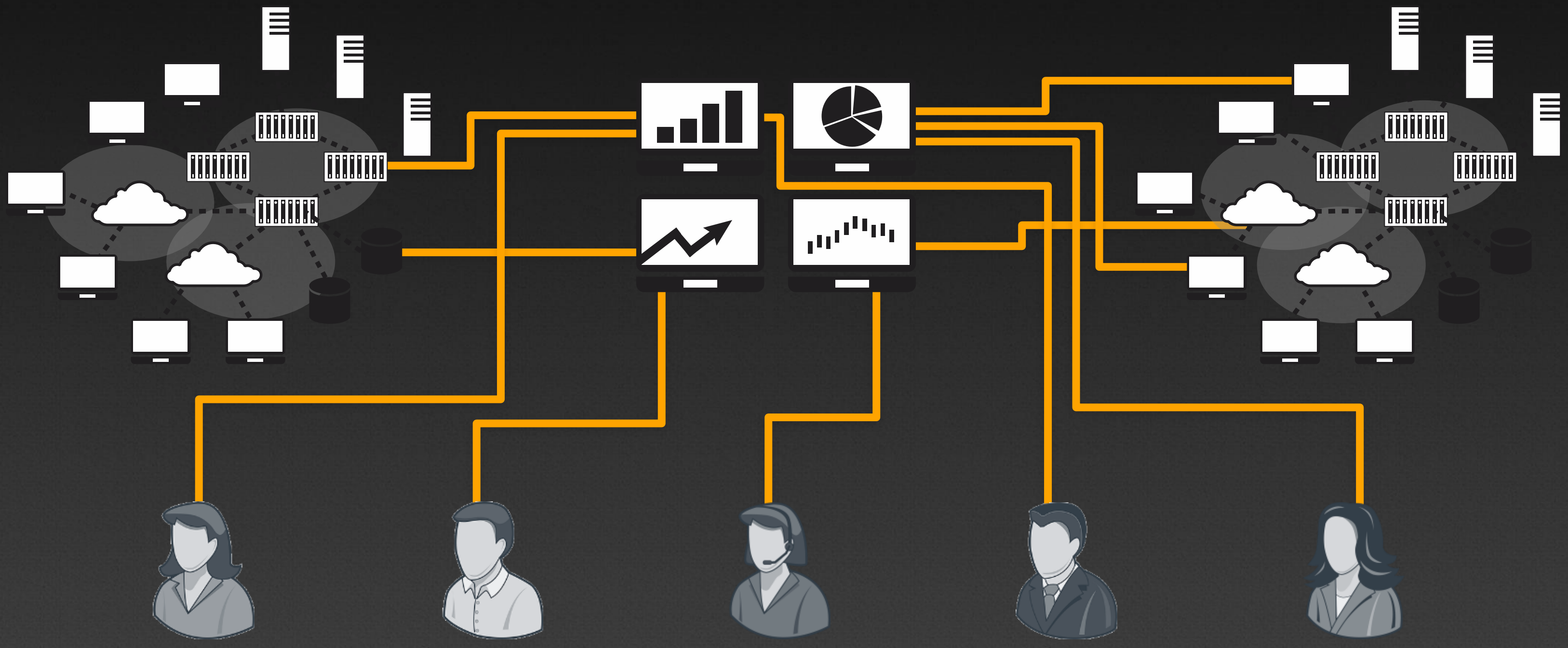
NetIQ

loggly

TIBCO

tripwire

sumologic



NOC Team

SOC Team

Help Desk

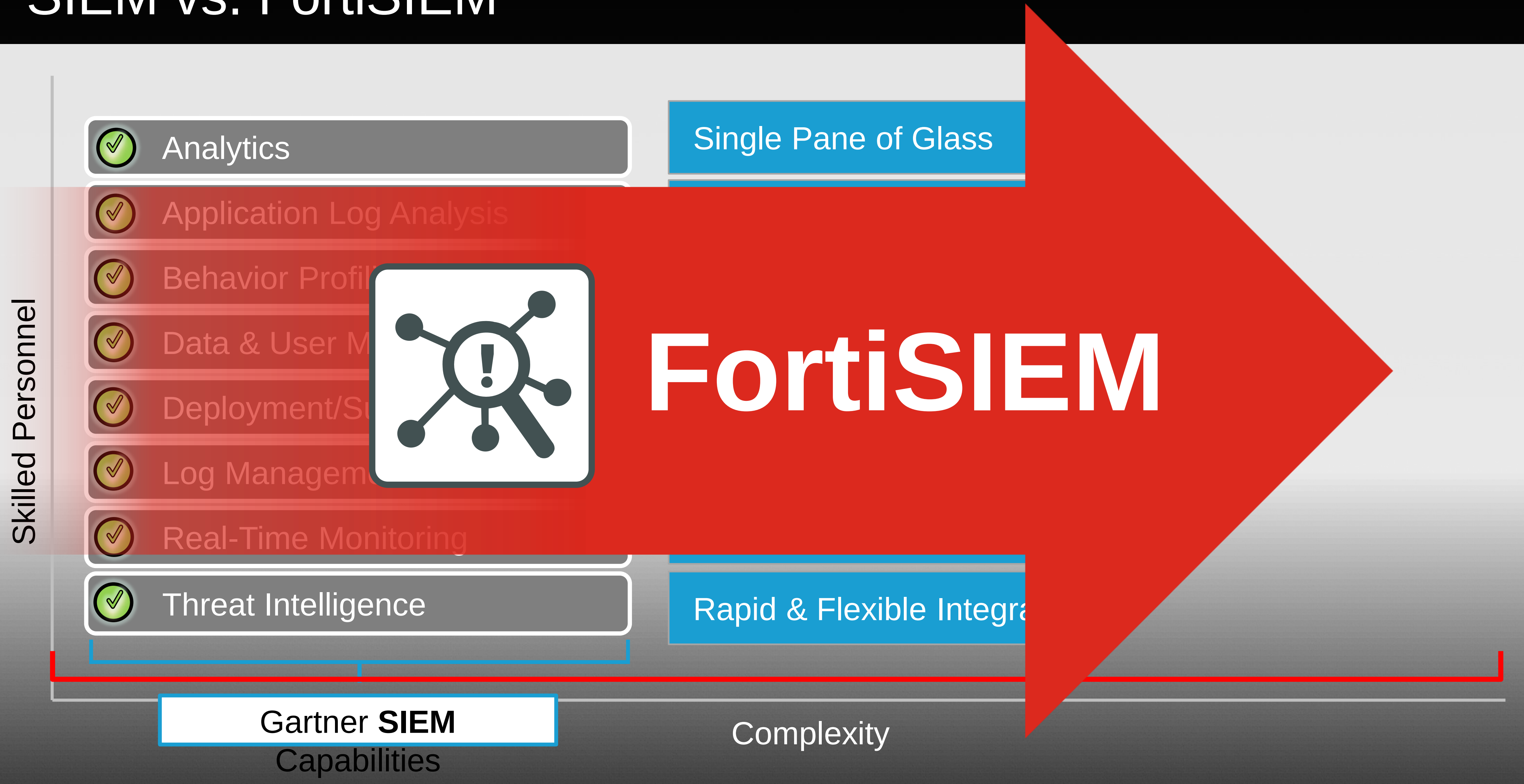
Datacenter Director

Systems, Admin

Visibility Needs

- Less Complexity
  - Consolidation/Integration of Tools
  - Deeper Analytics
  - More Context
- Real-Time Awareness of the Threat Landscape
  - Devices
  - Applications
  - Users
  - Networks
  - Virtual & Physical
  - Inter-relationships
  - Performance
  - Threat Data
- Faster Detection
- Scalability

SIEM vs. FortiSIEM



Skilled Personnel

✓ Analytics

✓ Application Log Analysis

✓ Behavior Profil

✓ Data & User M

✓ Deployment/Su

✓ Log Managem

✓ Real-Time Monitoring

✓ Threat Intelligence

Single Pane of Glass

Rapid & Flexible Integra

FortiSIEM

Gartner **SIEM** Capabilities

Complexity

Rapid Flexible Integrations

Context from Hundreds of Sources

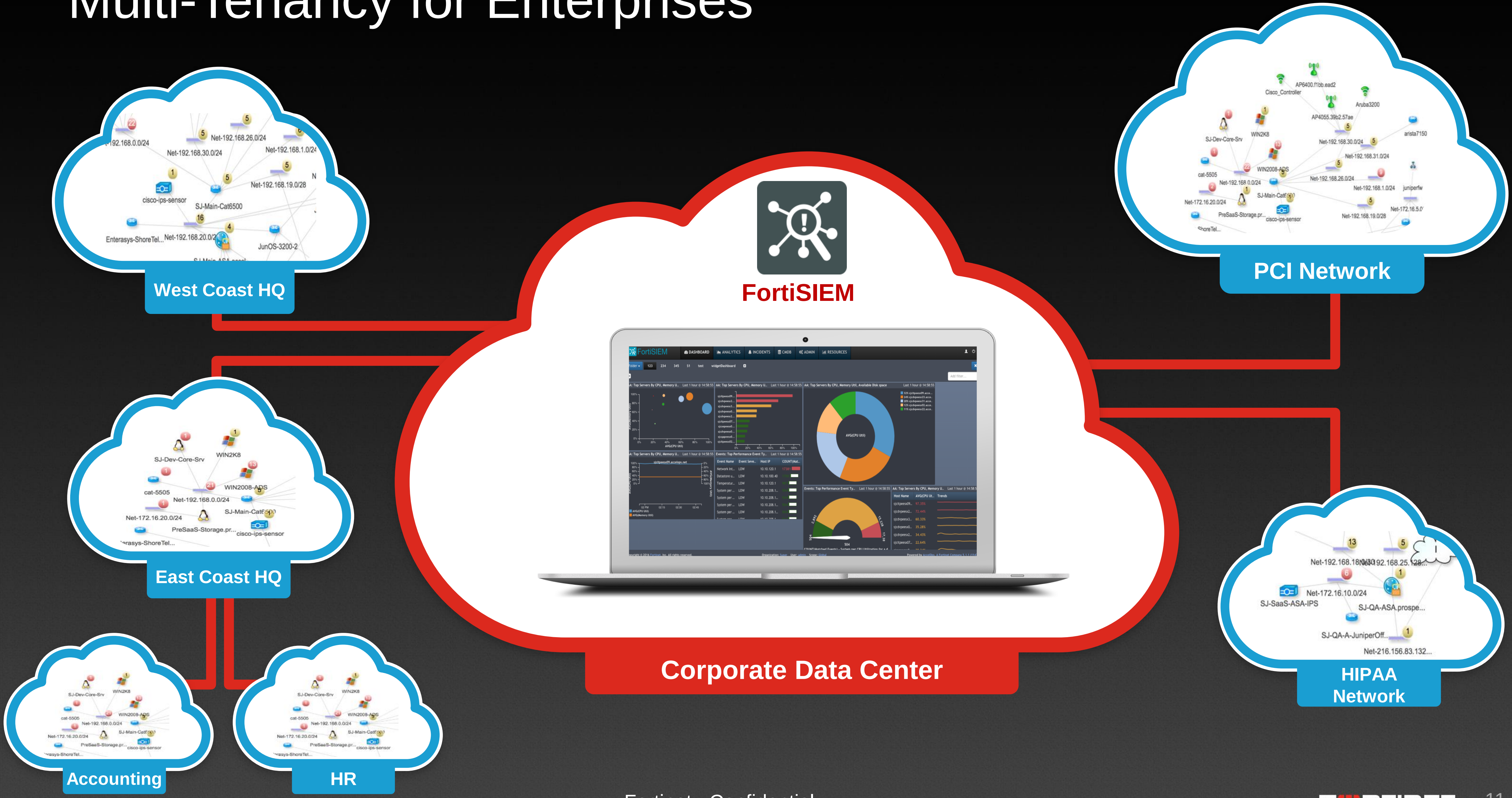
- Antivirus
- Cloud Services
- Databases
- Directories
- DNS/DHCP Servers
- Email
- Environmentals - HVAC
- External Monitoring
- File Monitoring
- **Firewalls**
- Hardware Monitoring
- Host OS
- Internet Security Gateways
- IPS/IDS
- Load Balancers
- Network Flow
- Remote Desktop
- **Routers/Switches**
- **Servers**
  - App Server
  - Authentication Servers
  - Blade Servers
  - Terminal Servers
  - VoIP Servers
  - Web Server
- Storage
- Synthetic Transaction Monitoring
- Unified Threat Management (UTM)
- Virtualization
- VPN Gateway
- Vulnerability Scanners
- WAN Accelerators
- Wireless

Only Cross Correlated SOC & NOC Analytics

SOC Analytics	NOC Analytics
Log Ingestion, Parsing and Storage	Real-Time Infrastructure Discovery CMDB
File Integrity Monitoring	Network and Interface Utilization
Patented Log Analytics	CPU, Memory, Disk Performance Monitoring
Incident Management, Ticketing and Response	Availability Monitoring
Reporting and Compliance – Built in/Custom	Storage Monitoring
External Threat Feed Intelligence Integration	Change monitoring – config., installed software
Pre-built Reports for Compliance and Security	Infrastructure and User Application Monitoring
Rule and Statistical Anomaly Based Reporting	Synthetic Transaction Monitoring

Cross Correlated in Real-Time

Multi-Tenancy for Enterprises



FortiSIEM

Corporate Data Center

West Coast HQ

East Coast HQ

Accounting

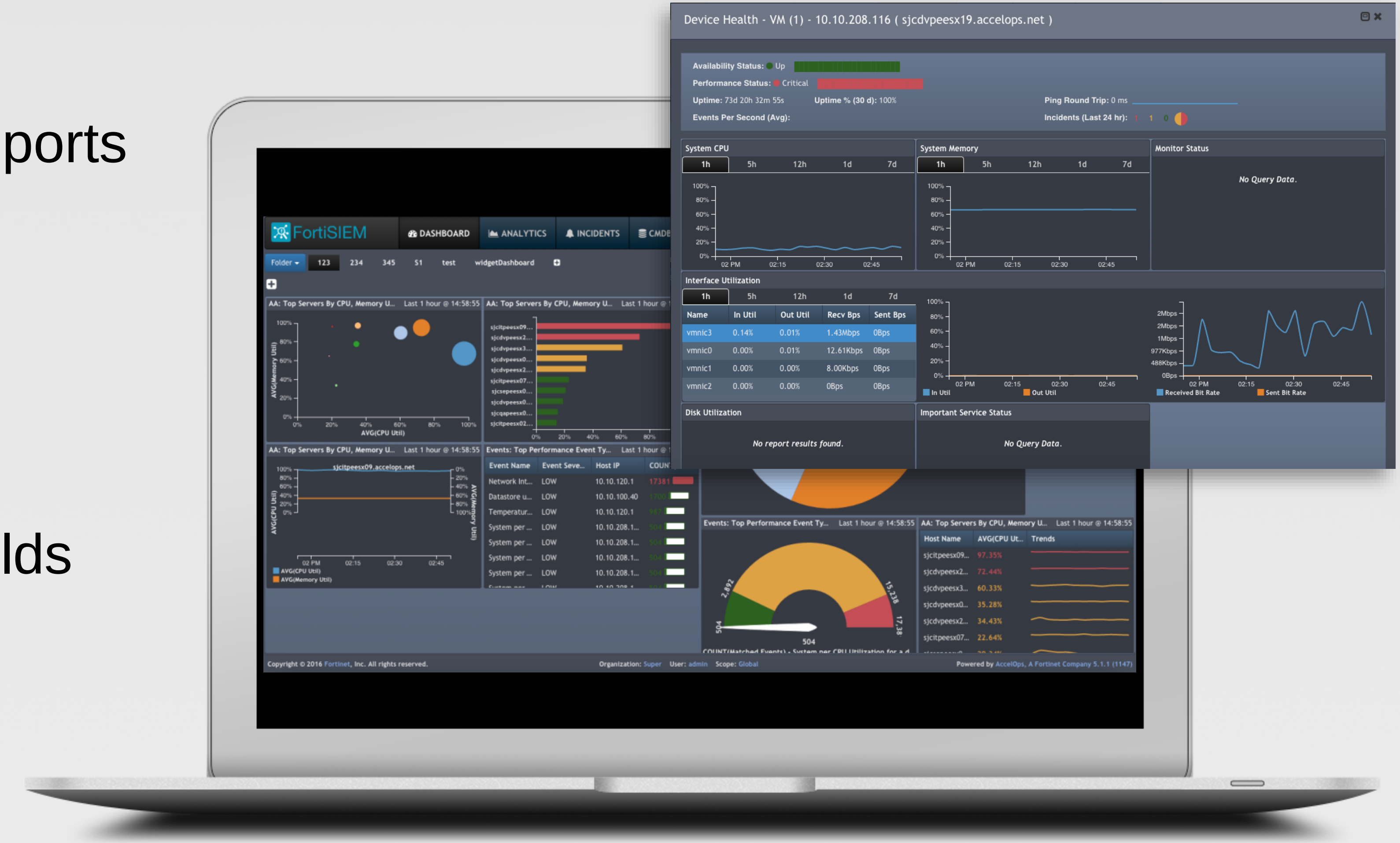
HR

PCI Network

HIPAA Network

Compliance Reporting Built-in

- Hundreds of Pre-Built Reports
- Compliance Reports
  - » **PCI – HIPAA – FERPA**
  - » SOX, NERC, COBIT, ITIL,
  - » ISO, GLBA, GPG13
  - » SANS Critical Controls
- 2,000+ Customizable Fields



Device Health - VM (1) - 10.10.208.116 (sjcdvpeesx19.accelops.net)

Availability Status: Up

Performance Status: Critical

Uptime: 73d 20h 32m 55s   Uptime % (30 d): 100%   Ping Round Trip: 0 ms

Events Per Second (Avg):   Incidents (Last 24 hr): 1 1 0

Monitor Status: *No Query Data.*

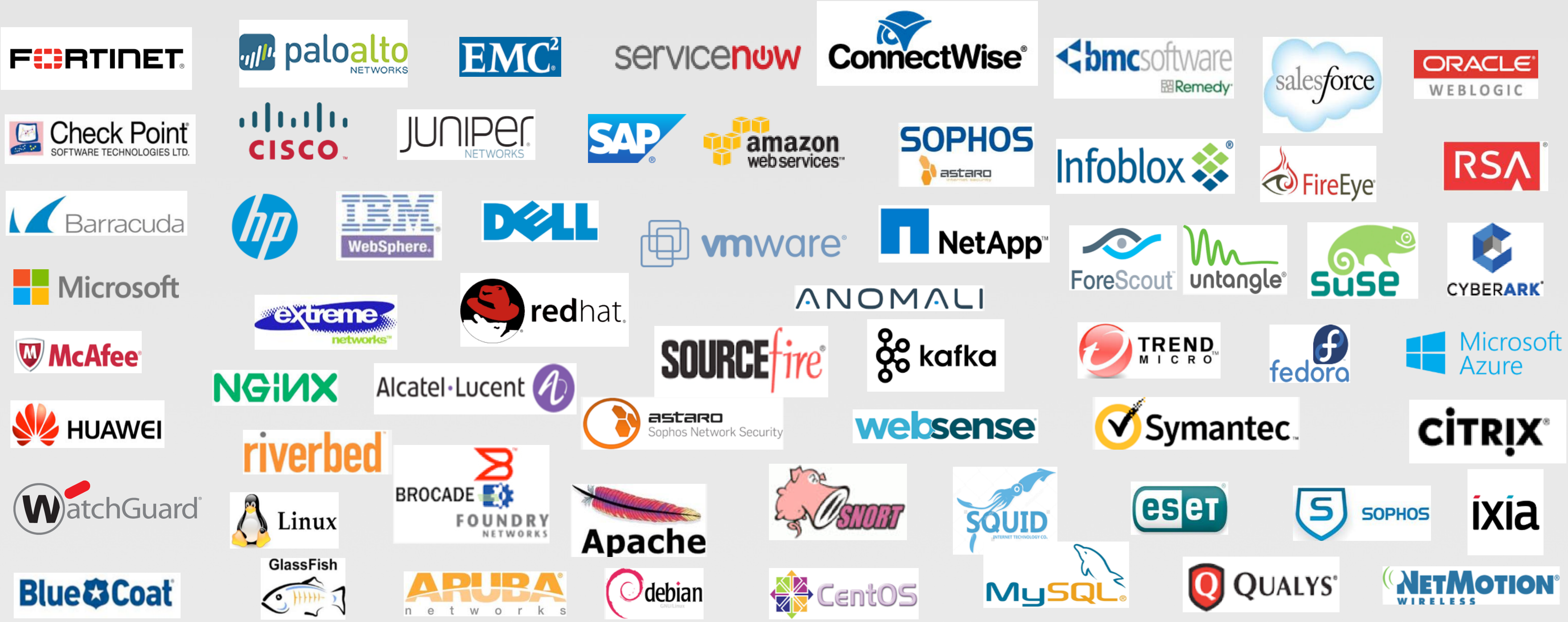
Interface Utilization

Name	In Util	Out Util	Recv Bps	Sent Bps
vmnic3	0.14%	0.01%	1.43Mbps	0Bps
vmnic0	0.00%	0.01%	12.61Kbps	0Bps
vmnic1	0.00%	0.00%	8.00Kbps	0Bps
vmnic2	0.00%	0.00%	0Bps	0Bps

Disk Utilization: *No report results found.*

Important Service Status: *No Query Data.*

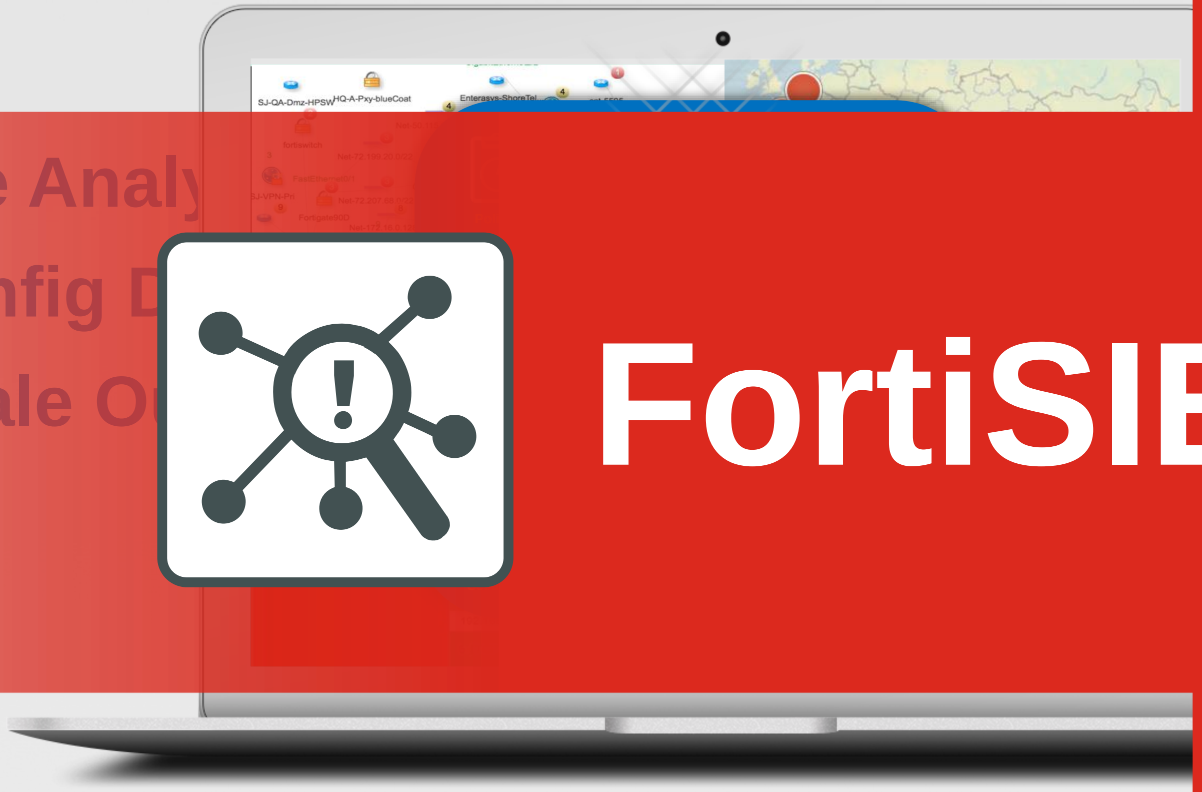
FortiSIEM Technology Integrations



Making Visibility & Control Easy – Today & Into the Future

1. **Real-Time Analy**
2. **Asset/Config D**
3. **Rapid Scale Ou**

hitecture



FortiSIEM

7. **Single Pane of Glass**

Ďakujem!

FORTINET®