Total Visibility.
Focused Protection.

Mauro Cicognini | Comitato Direttivo Clusit
mcicognini@clusit.it

Davide Rivolta | Technical Director, Italy
davide.rivolta@skyboxsecurity.com

SKYBOX™ SECURITY

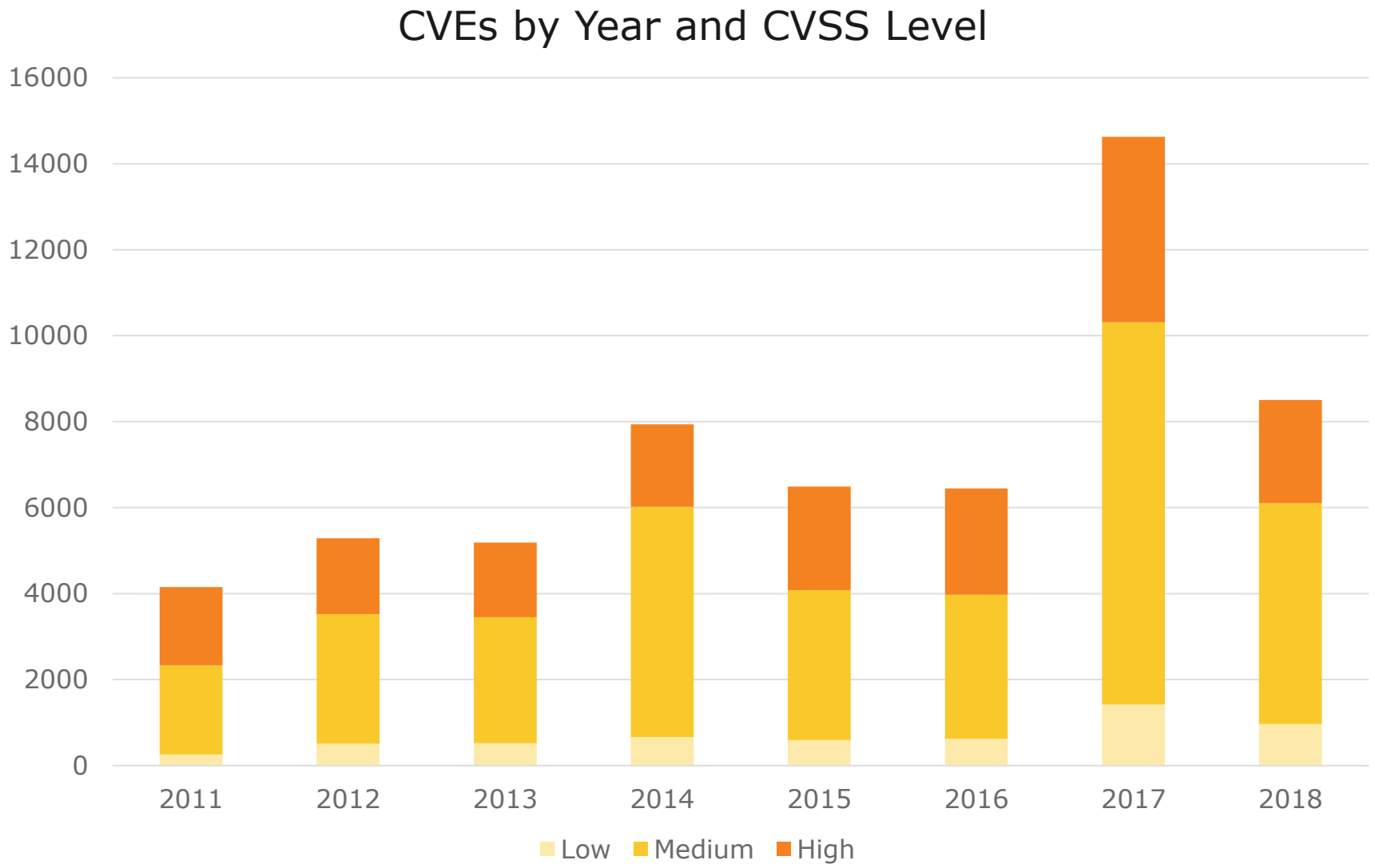
Vulnerability and Threat Trends

2018 Mid-Year Update

Skybox Security Research Lab

THE Great Flood

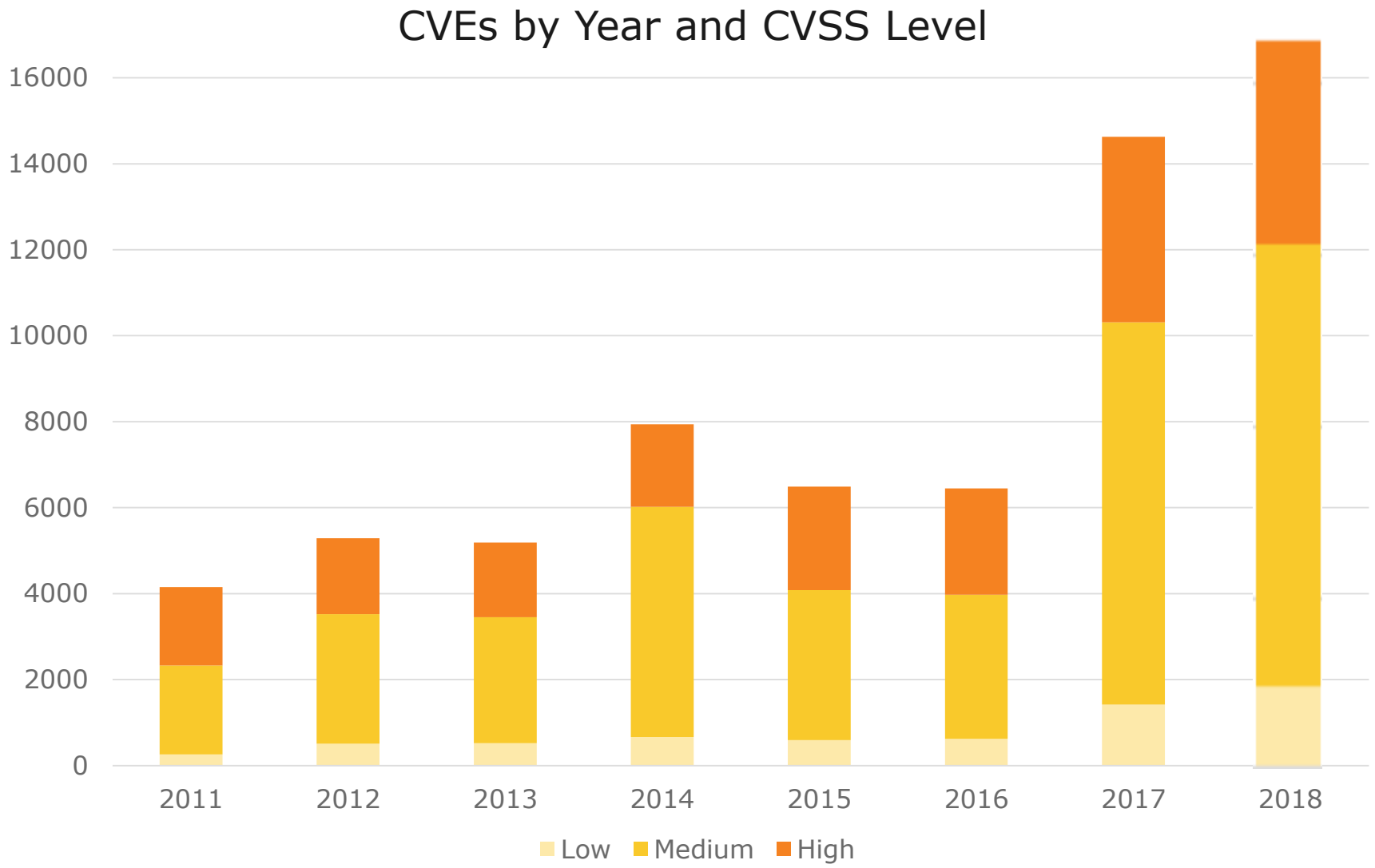
>8,500 new CVEs



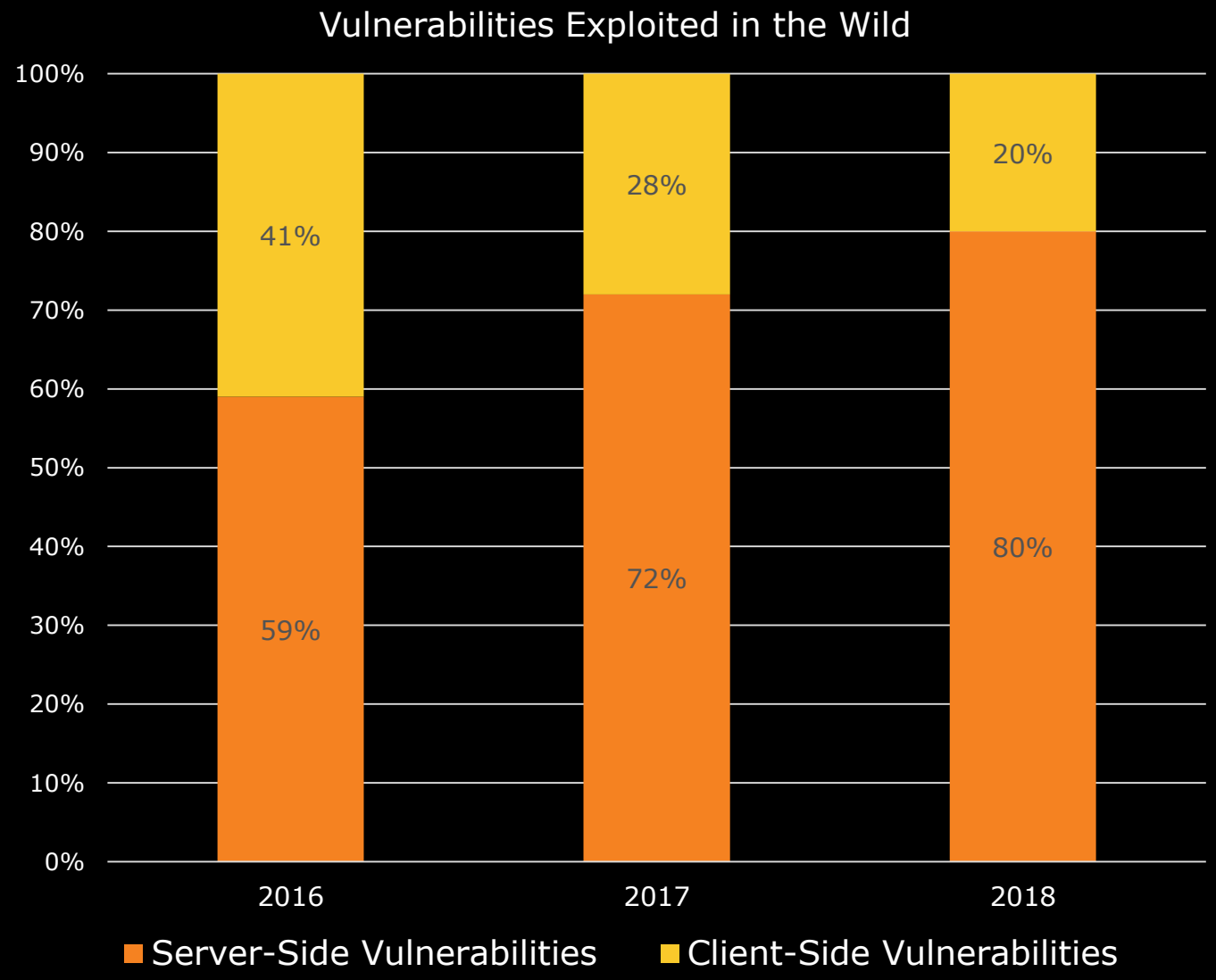
Source: https://nvd.nist.gov/vuln-metrics/ visualizations/cvss-severity-distribution-over-time

THE Great Flood

>8,500 new CVEs



Source: https://nvd.nist.gov/vuln-metrics/ visualizations/cvss-severity-distribution-over-time

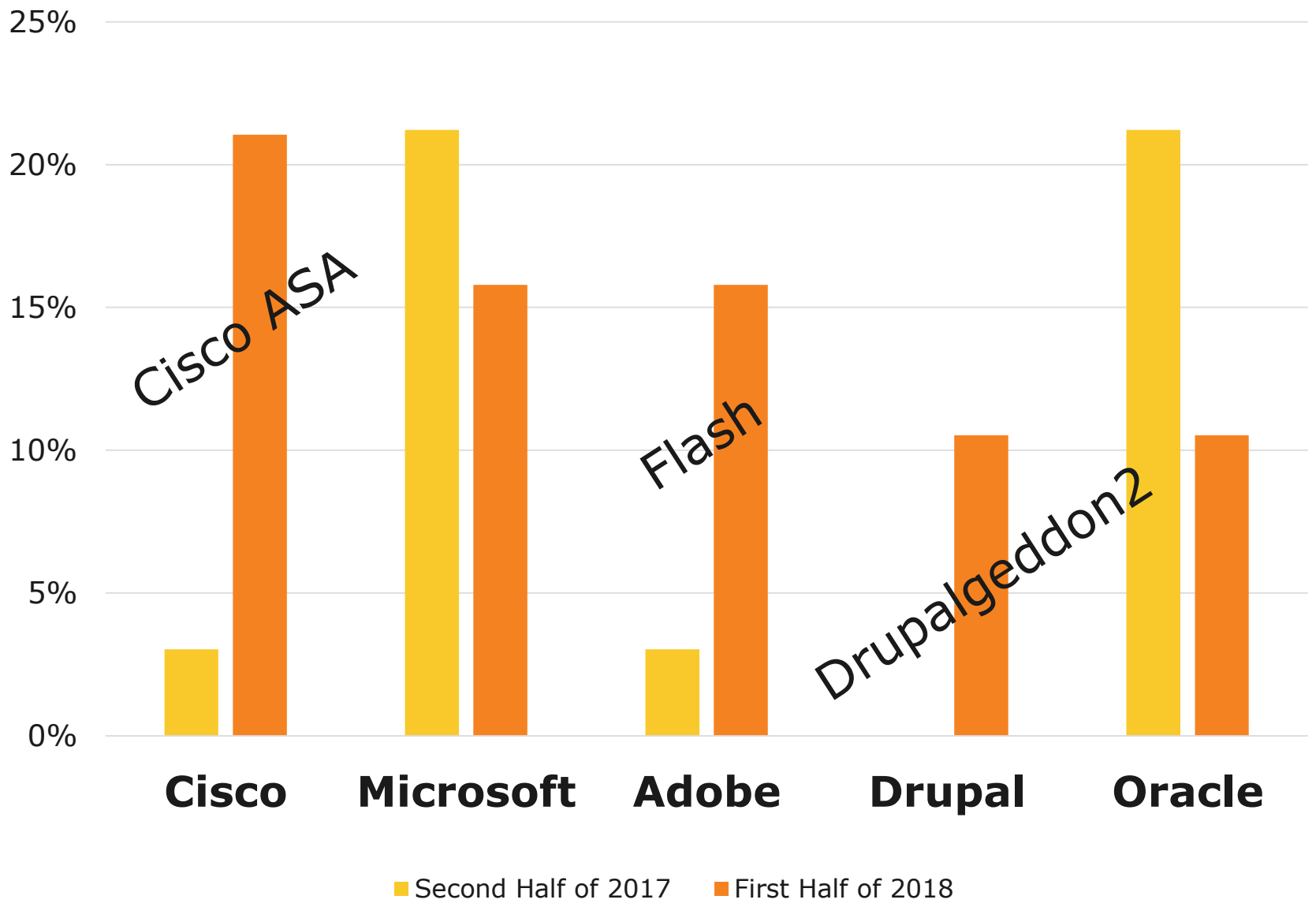


Source: Skybox Research Lab

MOST

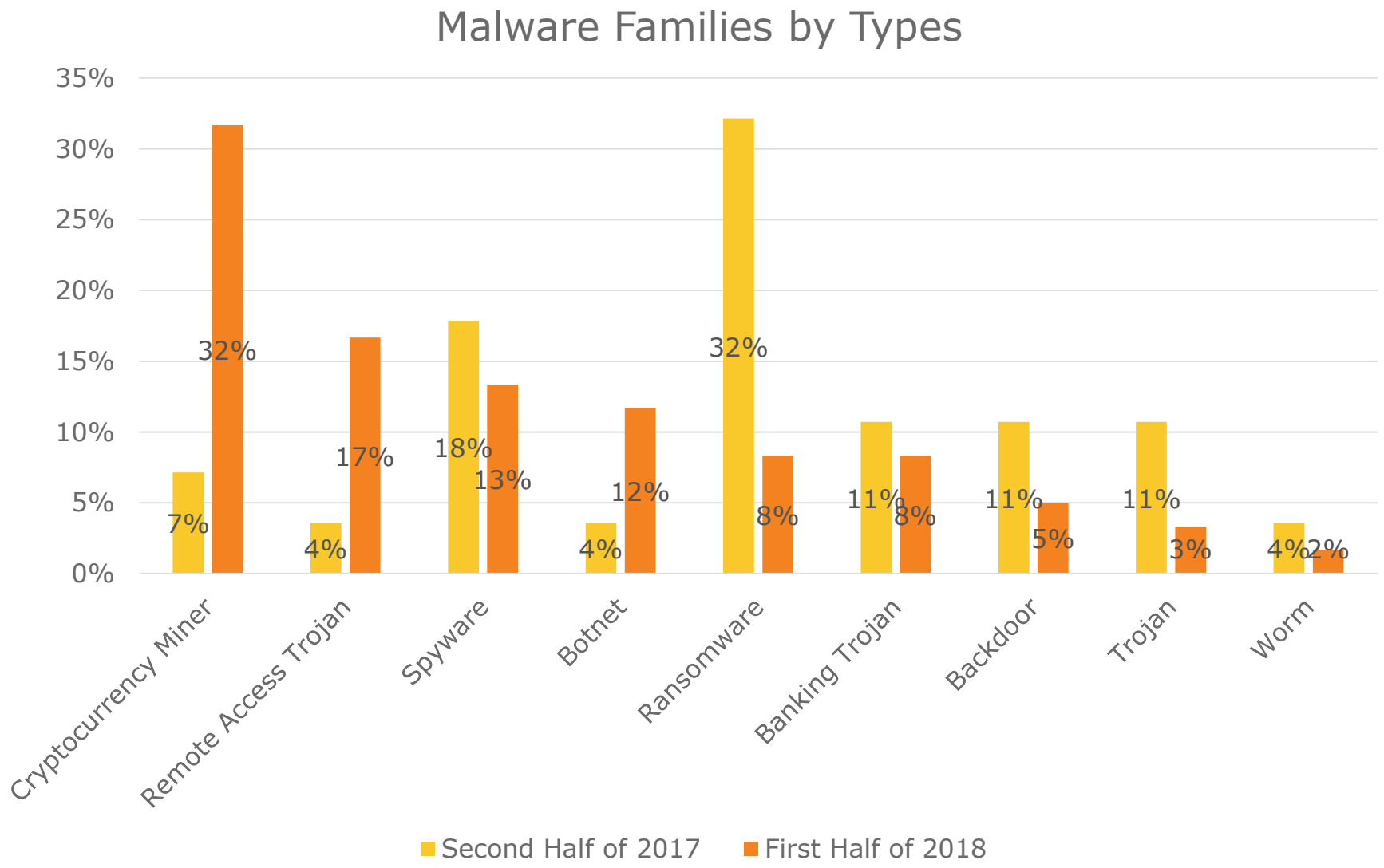
Exploited

Vendors



THE YEAR OF CRYPTO MINING

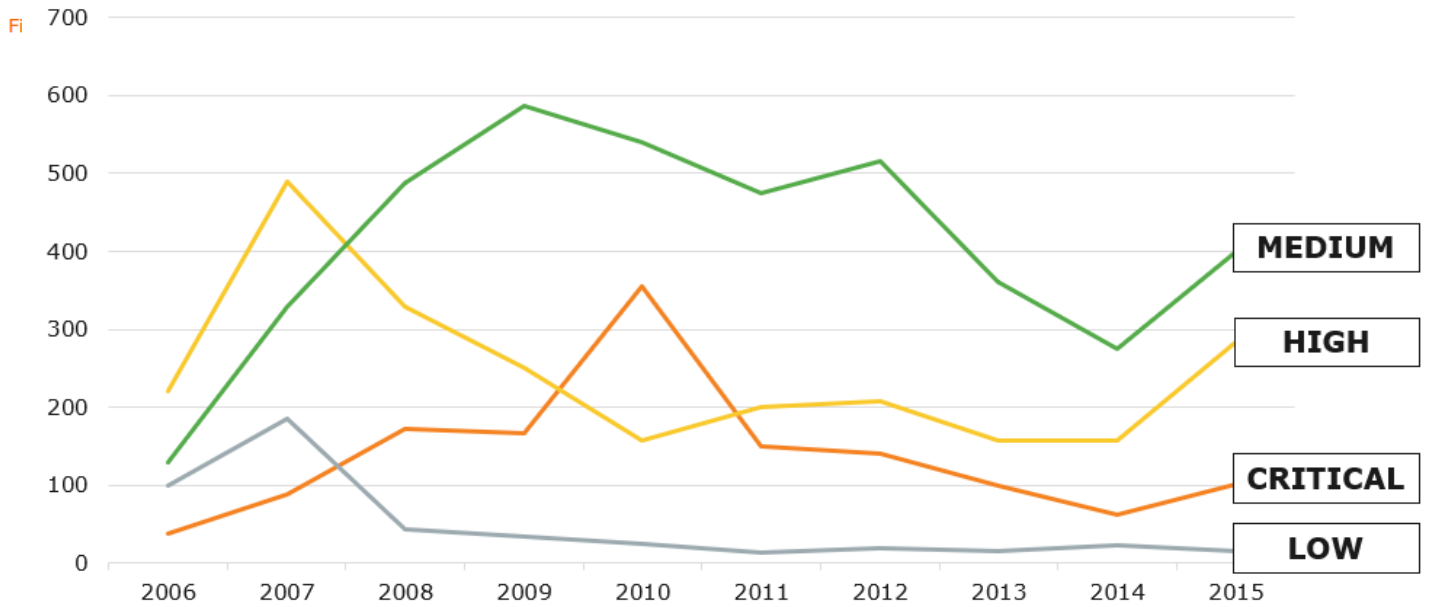
Cryptomining instead of ransomware



Vulnerability Exploited In The Wild

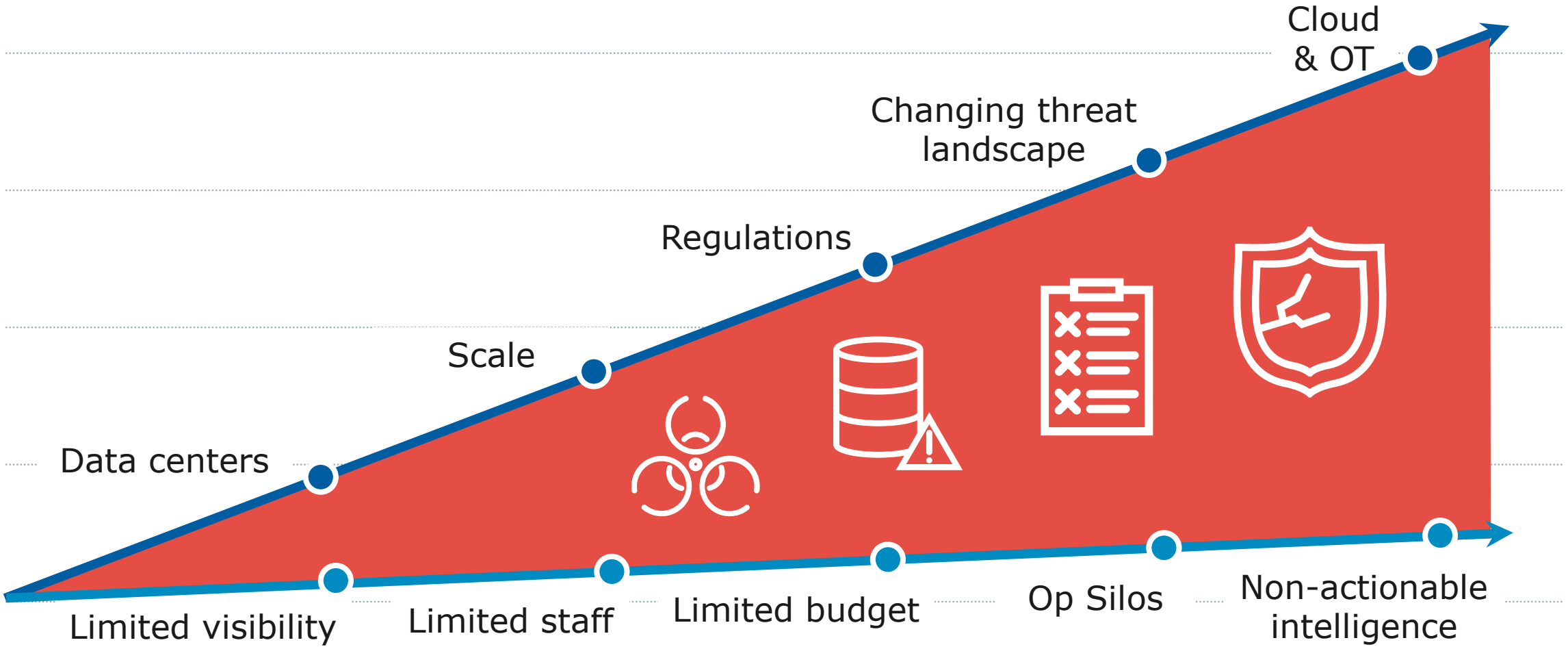
- When we look at all the vulnerabilities exploited in the wild (not only via EKs), we see similar patterns:
  - A few vulnerabilities that are very popular, are accountable for a big portion of the damage
  - Many of these vulnerabilities are old and a patch is available for years
  - Many of these vulnerabilities have a relatively-low CVSS score

85% of exploited vulnerabilities were **more than 2 years old**



– IBM X-Force/Analysis by Gartner, September 2016

Security Management Gap



Improving Vulnerability Management

"To truly manage vulnerabilities and not play Whac-AMole with scan findings, you need to trust your asset management, understand how your vulnerabilities fit into the context of your organization, and be able to analyze the paths attackers might take in that context."

– Verizon Data Breach Incident Report 2018

SKYBOX™ SECURITY

Vulnerability Management in 2018

Who We Are

Silicon Valley HQ

Offices around the globe

Fastest–growing company in our space

$270M funding since February 2016

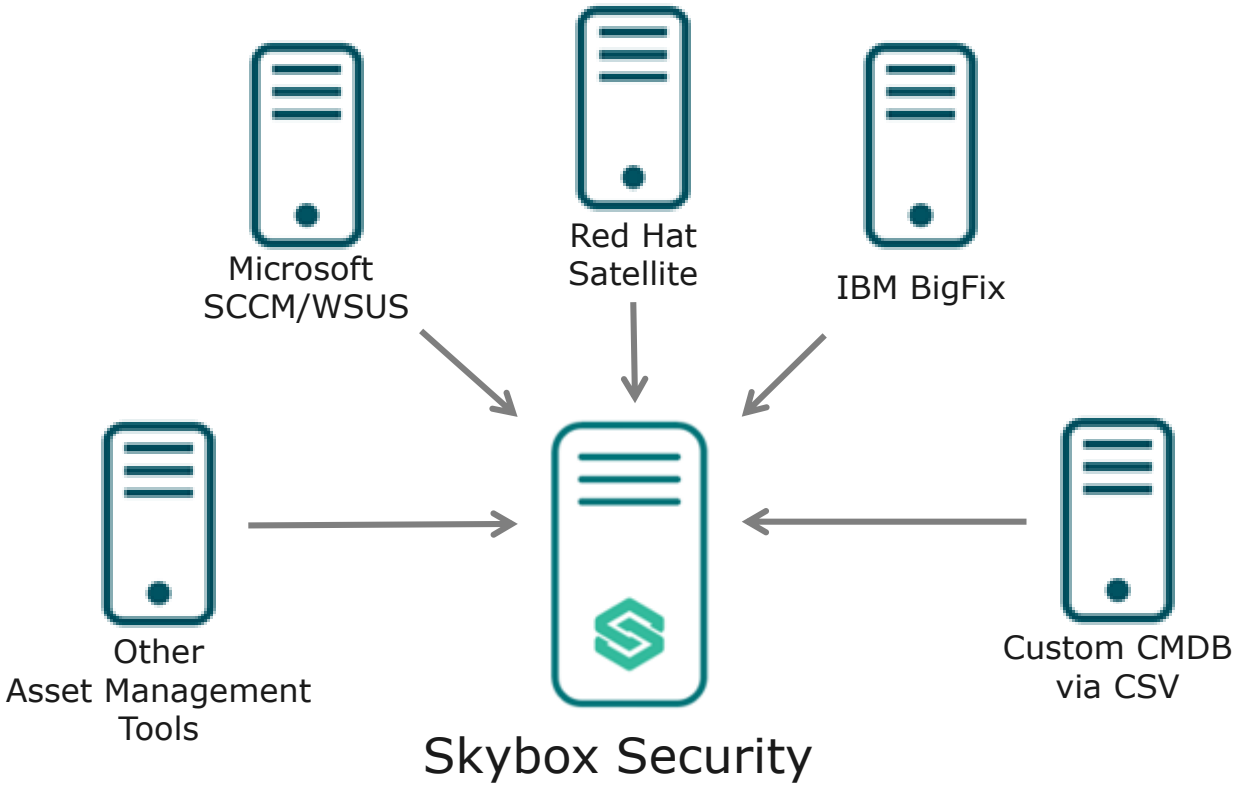
5–star reviews

Vulnerability/Threat Management
Risk/Policy Management

700+ active customers

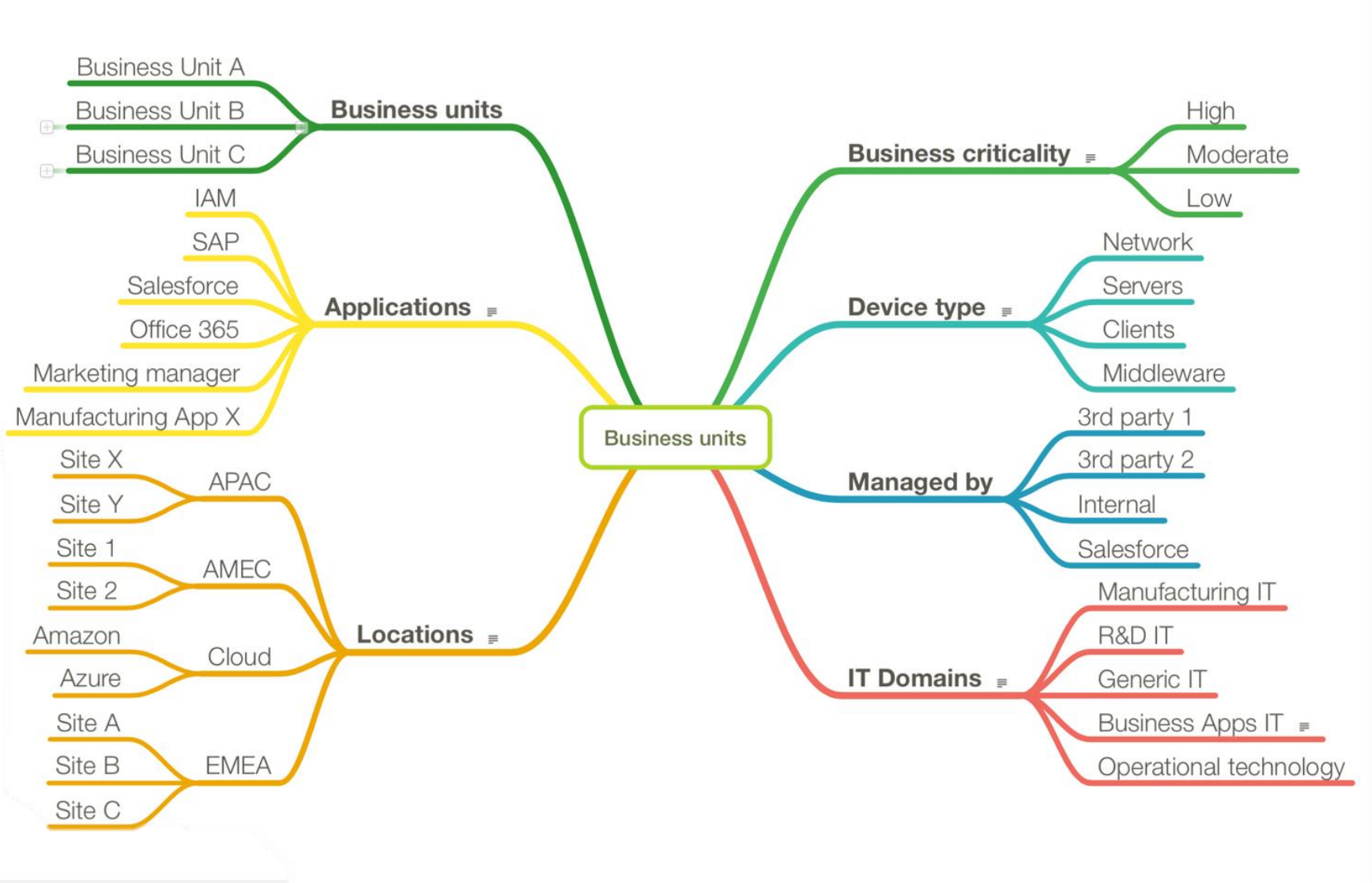
50 countries, all verticals

Asset Management

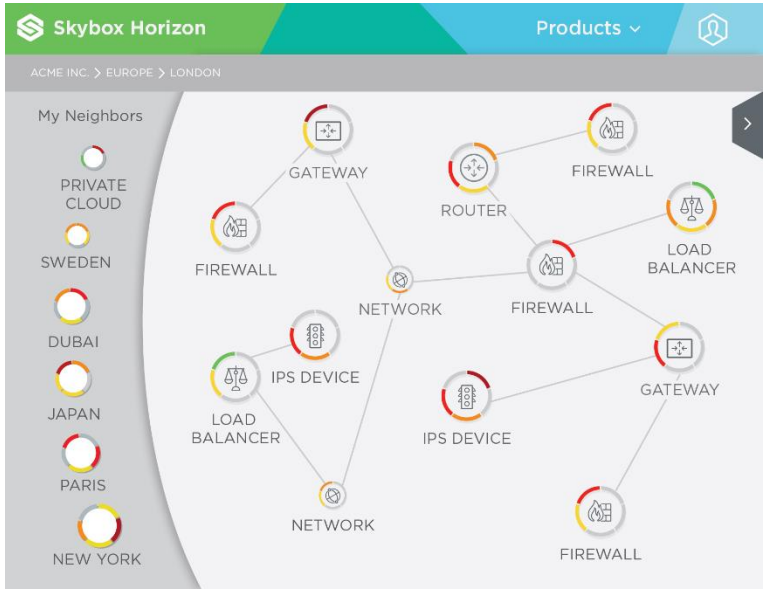


Central repository with unprecedented visibility of all assets, their location and their business function

Asset Management

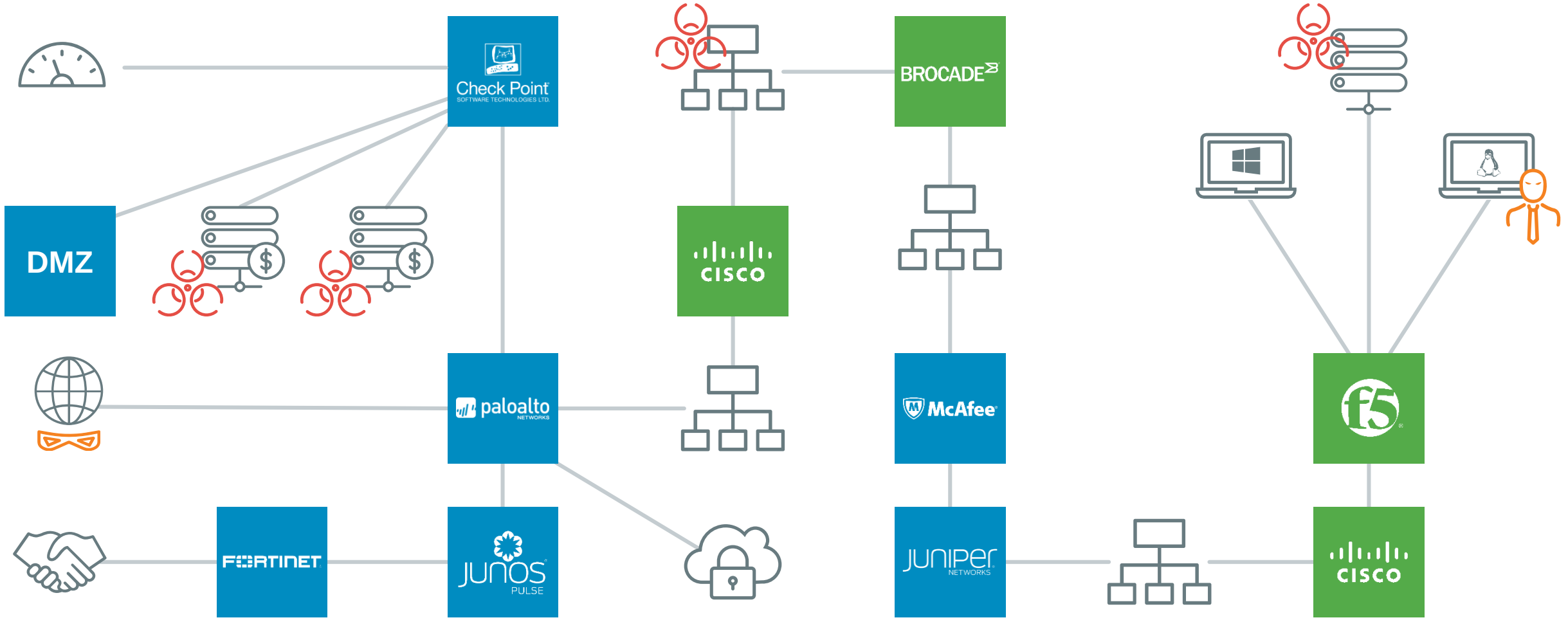


Asset Management



- Visualize your entire attack surface from multiple perspectives
- Display data in formats useful to security and business-oriented stakeholders

It all starts with modeling the Attack Surface



Security Controls | Network Topology | Assets | Vulnerabilities | Threats

Firewall/Network Security & Infrastructure

Barracuda, Hewlett Packard Enterprise, ARUBA networks, AVAYA, JUNIPER NETWORKS, solarwinds, FORTINET, BLUE COAT, bmc, NOKIA, CISCO, TREND MICRO, Check Point SOFTWARE TECHNOLOGIES LTD., BROCADE, ARISTA, Symantec, paloalto NETWORKS, DELL, f5

Vulnerability Management, SIEM

Hewlett Packard Enterprise / ArcSight, McAfee, RAPID7, splunk>, Symantec, QUALYS, IBM, tripwire, EMC², RSA SECURITY, tenable network security

Endpoint Security

intel Security, redhat LINUX, CISCO, Microsoft, Symantec, Barracuda, Linux

Cloud/ Virtual

amazon web services, vmware NSX, Microsoft Azure

OT Security

SECURITY MATTERS, CyberX

120+ technology integrations

Skybox Security Intelligence Feed

Skybox Research Lab

700,000+ sites
in the dark web

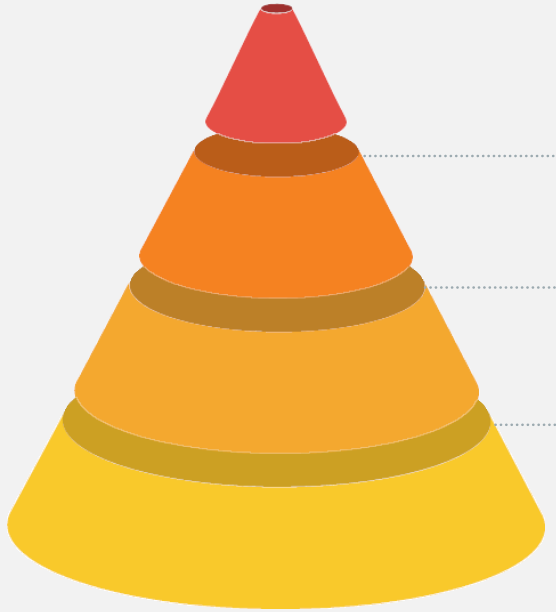
30+ security
data feeds

- Exploits in the wild
- Vulnerabilities used in ransomware, exploit kits, etc.
- Attack vector details

Threat-Centric Vulnerability Management

Imminent Threat
High-priority remediation/mitigation

Potential Threat
Gradual risk reduction



Exposed (≃ 0,1%)

Exploited In The Wild (0,6%)

Exploit Available (11,9%)

No Exploit (87,5%)

Source: Skybox Security Dictionary – September 2018

More Options in Remediation

PATCH

UPGRADES

Requires Asset Layer Insight

IPS SIGNATURE

FW/SECURITY TAGS

CONFIGURATION

Requires Network Layer Insight

Skybox Security Suite

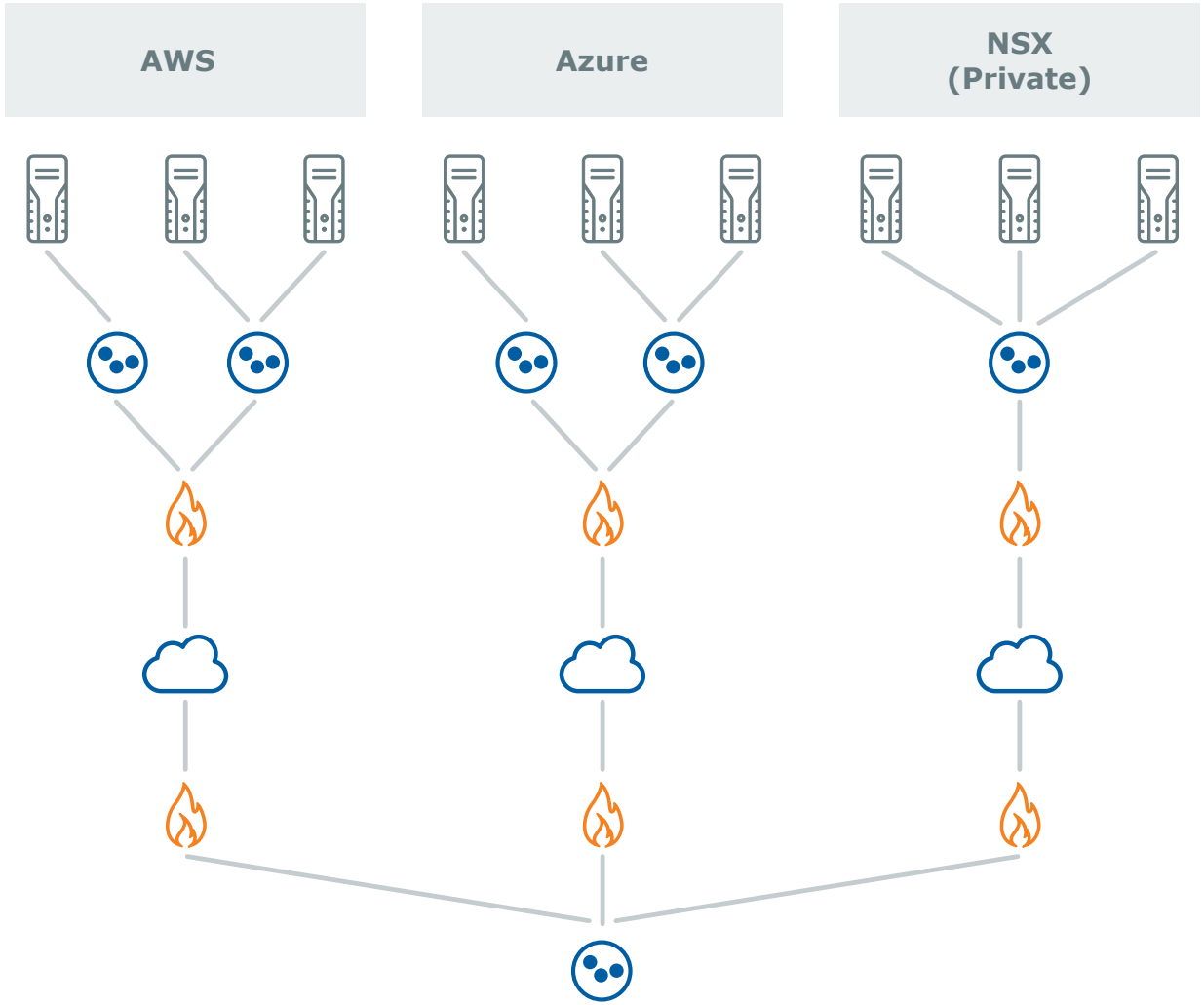
Integrated Security Management

- Total visibility of the attack surface
  - Traditional IT
  - Virtual and cloud
  - Operational technology
  - Vulnerabilities and threats
- Built for large, complex networks
- One platform, many solutions

SKYBOX™ SECURITY

Vulnerability Management in the next years

Security in Multi-Cloud Environments



Complete Visibility

End–to–end path analysis

Policy compliance across networks in a single dashboard view

Out–of–the–box regulatory compliance checks

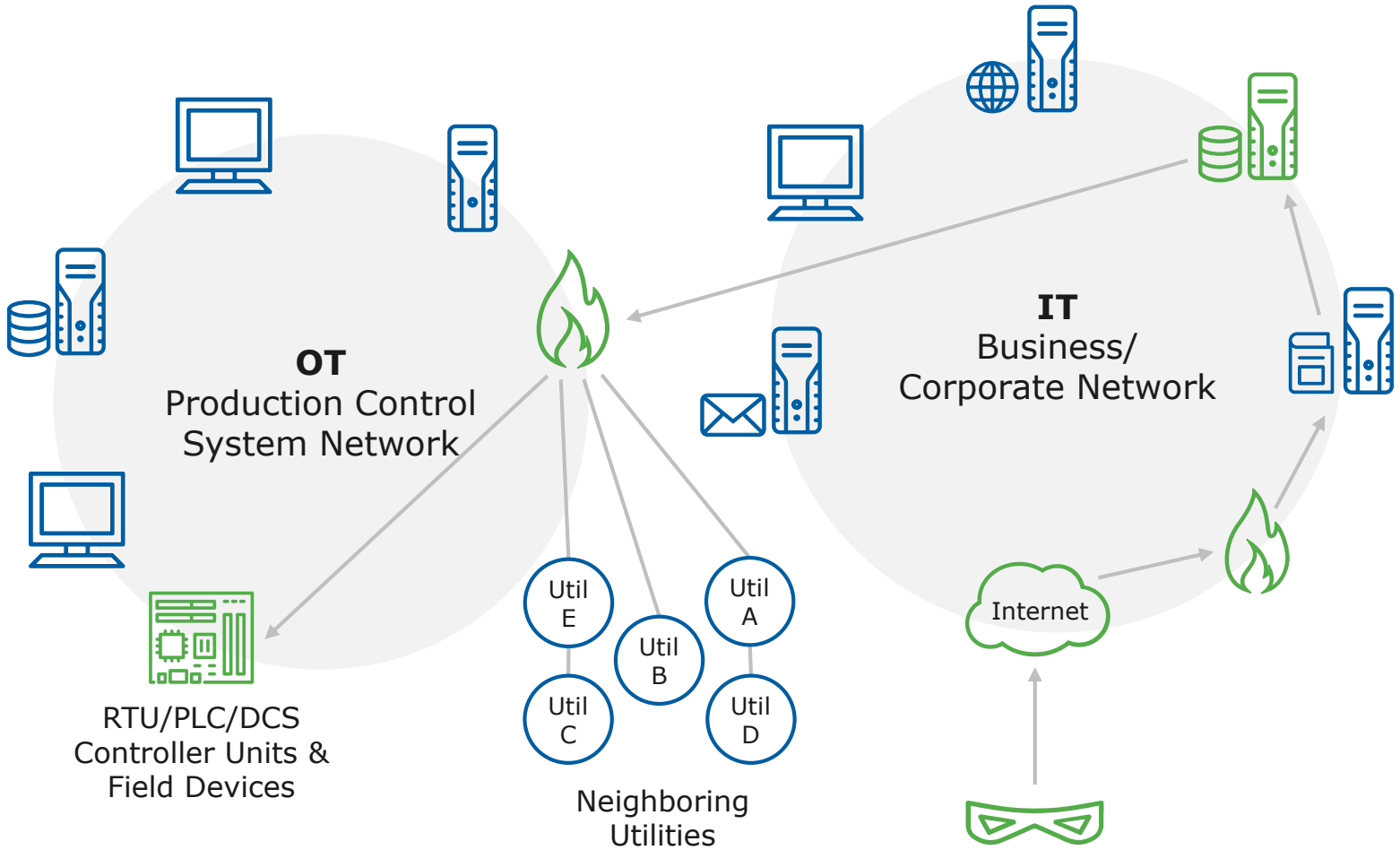
Threat–centric vulnerability management

Security in Industrial Networks

Visibility and path analysis for combined IT and OT networks

Risk analysis

Vulnerability detection



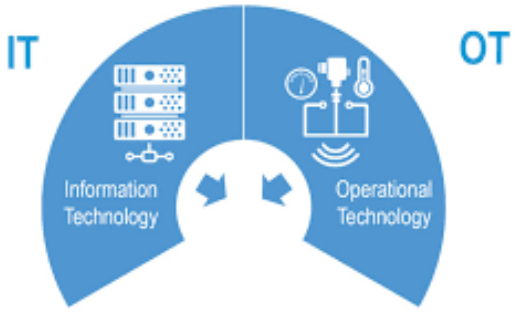
SKYBOX™ SECURITY

Managing Security Across IT and OT Networks

Operational Technology is everywhere

Financial Services	Oil & Gas	Energy	Transportation	Telecom	Health
					
Building Management Systems (BMS)	Drilling and Distribution Process	Power Generation and Distribution	Signaling, traffic control, Naval Ports, Airports	Cell Tower management system	PACS, Health Sensors, BMS

ICS/Scada Security Demand Drivers



OT and IT Convergence

Nation led Cyber Warfare & Geopolitical conflicts

Successful ICS Breaches

Regulatory Compliance

Key Challenges in Industrial Networks

Closed, proprietary technology	Many flaws, no security mechanisms, protocols are easily exploitable
Managed and installed on outdated IT systems	Lots of vulnerabilities at the software stack, no vendor support
IP connectivity transformation, derived by ICS vendors	Exposure to corporate IT threats, malicious insiders
Organizational challenges	OT and IT speak different languages

Key Security Requirements in Industrial Networks

Visibility	Ability to discover and show IT and OT assets as well as the Network connectivity & Access
Vulnerability Management	IT and OT Vulnerability Analysis, including Exposure and Exploited in the wild
Threat Detection	Anomaly detection of malwares/attacks in the network
Compliance Reporting	Automated reporting on compliance with best practices such as ISA99,NERC CIP, FISMA

Skybox OT Sensor

- Linux based (Virtual Appliance or Physical)
- Broadest ICS Protocol support
  - DNP3
  - IEC 104
  - IEC 61850 (MMS, GOOSE, SV)
  - ICCP
  - Synchrophasor
  - Modbus/TCP
  - EtherNet/IP (including Rockwell)
  - OPC-DA/AE
  - Profinet
  - BACnet
    - Proprietary protocols from ABB, Emerson, Honeywell, Siemens, Yokogawa
    - 30+ IT protocols, including SMB/CIFS and DCOM

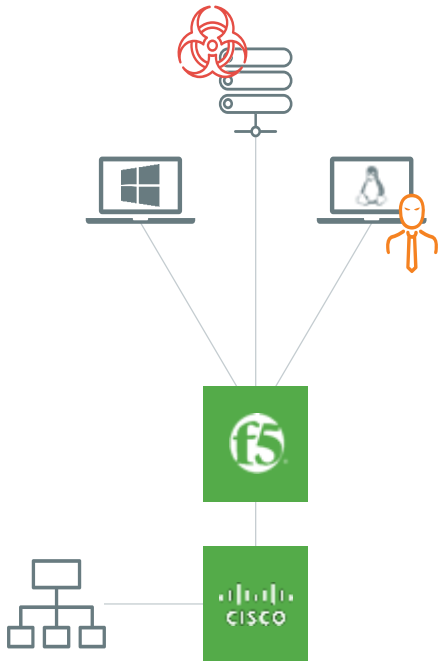
Passively collected information includes:

- IP/MAC address
- Vendor and model (depending on protocols)
- Device role
- Protocols/services, commands
- Number of links and data flows to other devices
- Sent/received bytes
- OS version and host name (depending on protocols)
- Network topology
- ISA99 Level (0-4)

Putting al the pieces together

IT Network

IT Assets



Level 5: Corporate Network

IT Assets

Level 4: Business Apps

Check Point

paloalto

CISCO

Level 3.5: Data DMZ

OT Network

IT Assets

JUNOS PULSE

McAfee

CISCO

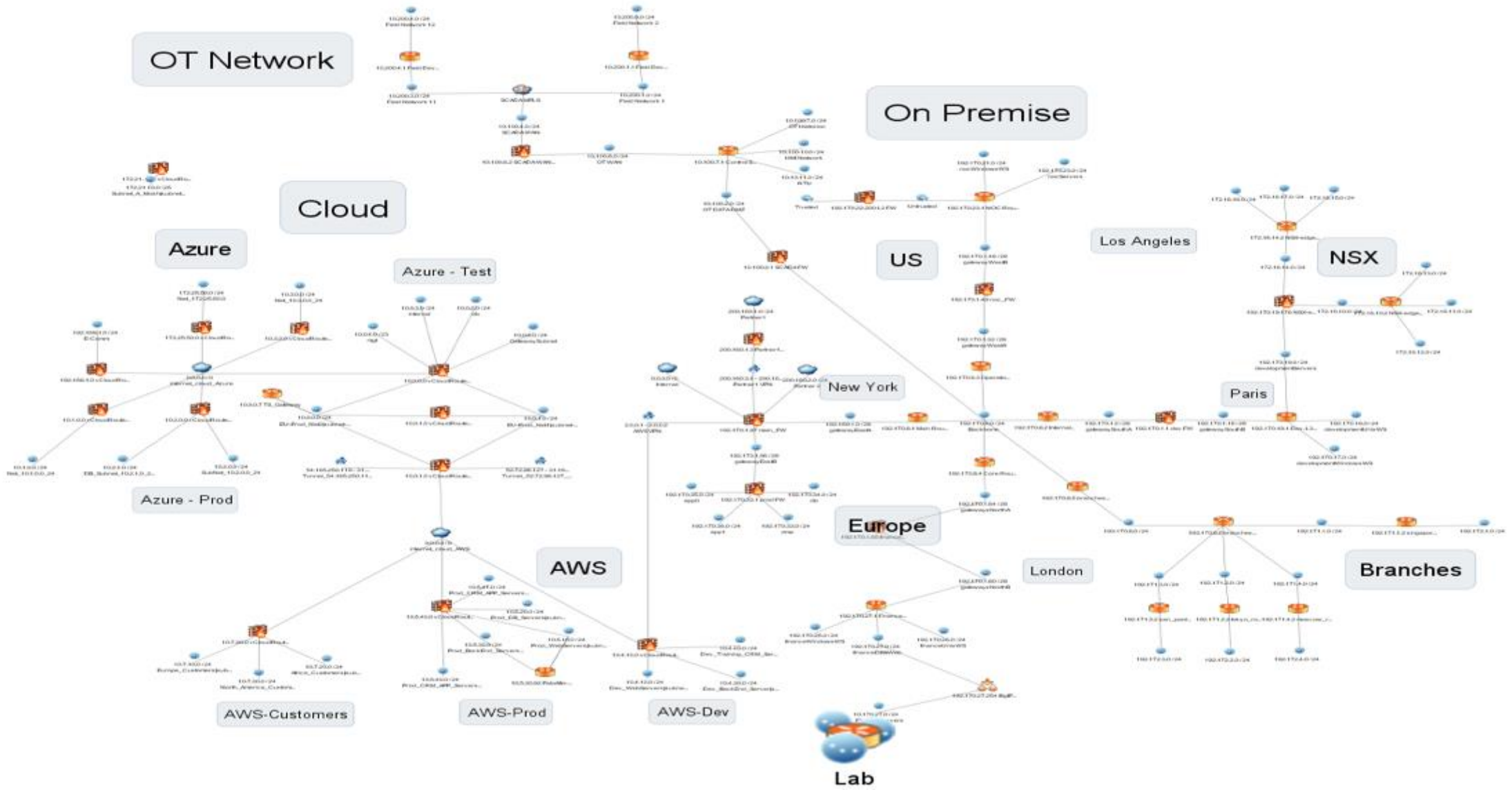
BROCADE

Level 3: Control System LAN

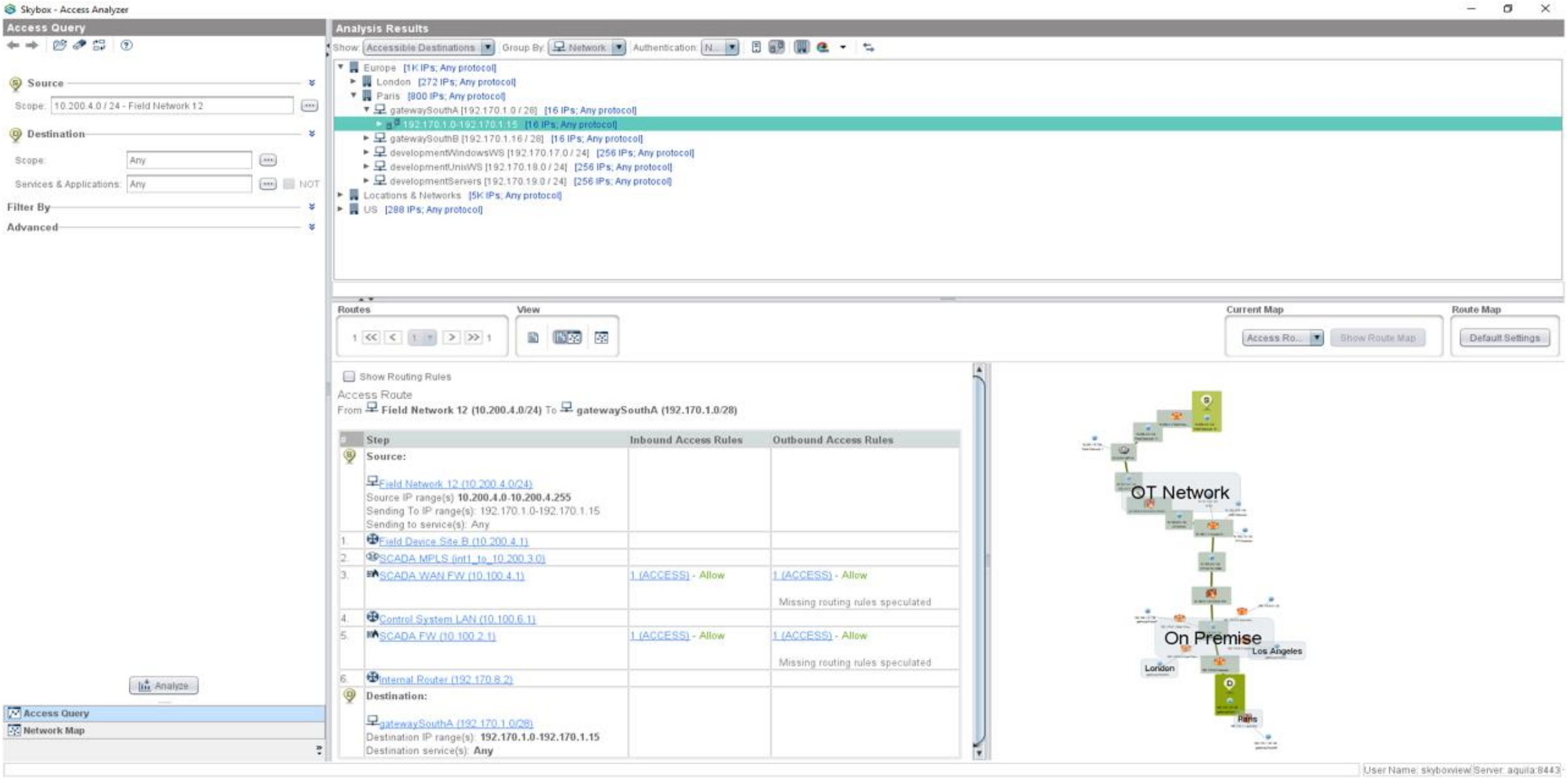
OT Assets

Levels 0-2: Basic Control, Supervisory, Process

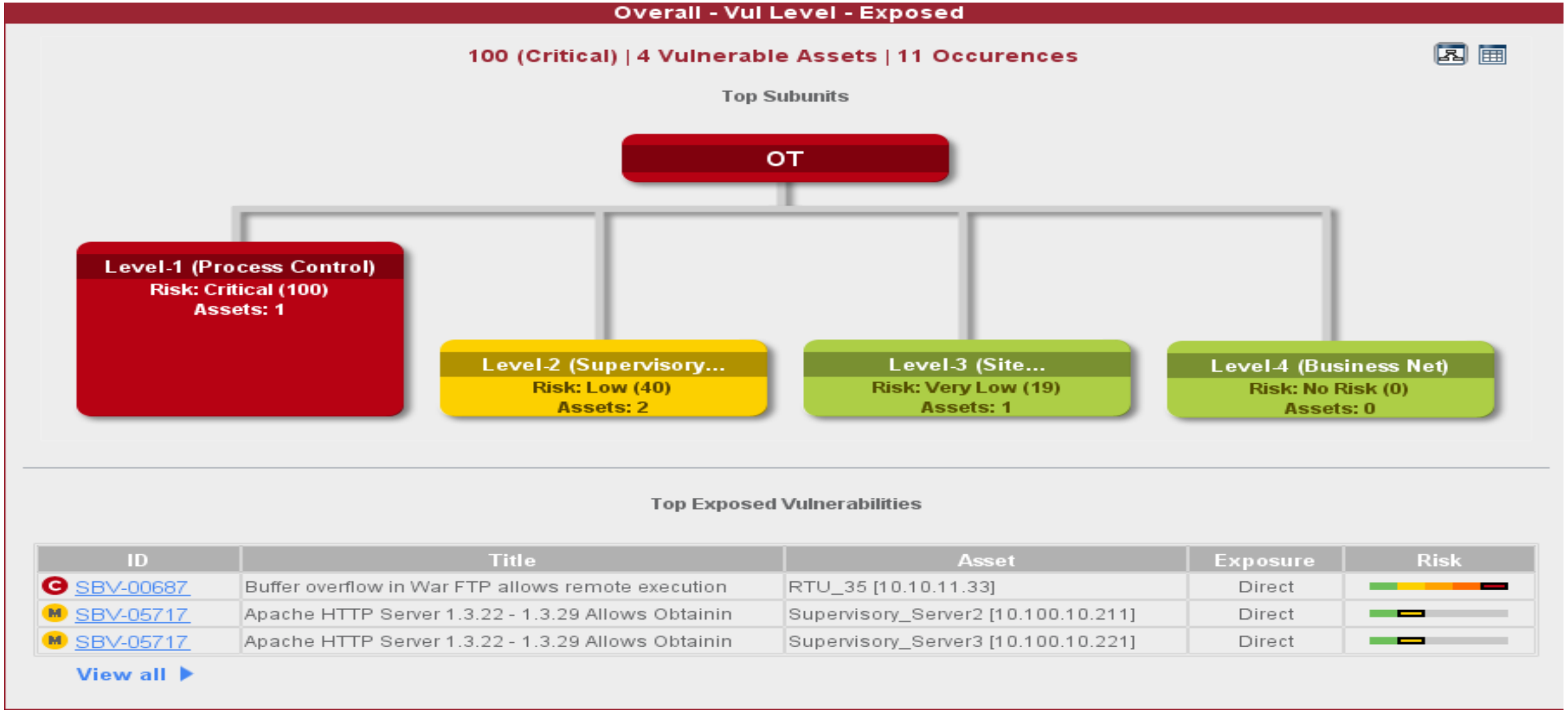
Complete IT & OT Network Model



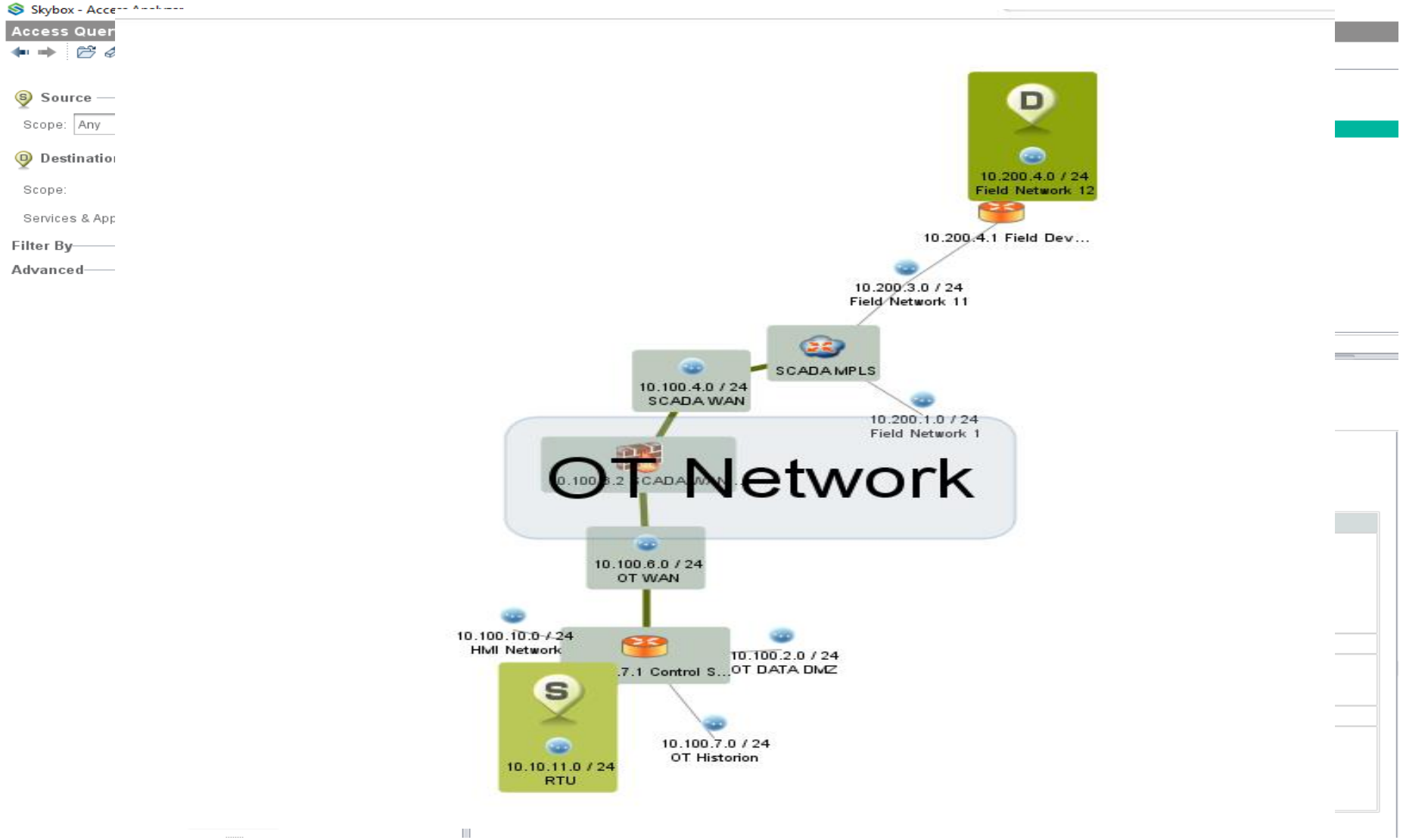
Use Case: Permissive access from Field Devices to Corporate IT



Use Case: Vulnerability Detection on OT assets



Use Case: WannaCry Propagation Path from IT to OT



The Skybox Difference

Unified Visibility

- Networks
- Assets
- Hosts
- Apps
- Services

"Single pane of glass" view

Vulnerability and Threat Analysis

- Vulnerability exposures in IT & OT networks
- Exploits in the wild
- Detection of malware related activity in OT networks

Complete context

Segmentation and Segregation Analysis

- Multiple network and security controls
- Different IT and OT networks
- View of Network Levels 0-5

End–to–end path analysis

Secure Change Management

- Closed–loop, consistent workflows
- Pre–change risk assessments, including exposed vulnerabilities
- Compliance checks

Automated change workflow

Compliance Reporting

- NERC
- FISMA
- NIST
- ISA99

Out–of–the–box and customization

Thank You!

Visit us at Skybox Security booth for more info and a quick demo of our capabilities