

Olimia 22.01.2019



Skybox Security

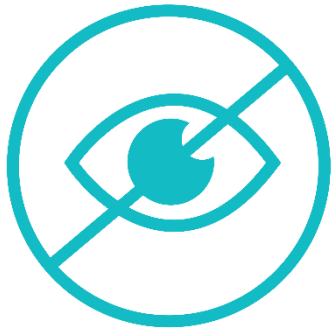
Srdjan Vranic



Co.Next

Why today's organizations need Skybox

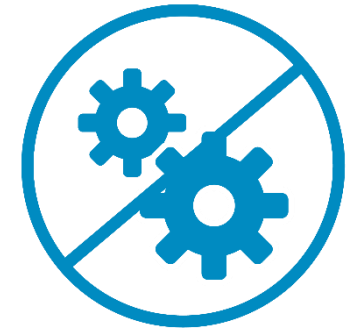
97% of breaches are avoidable through standard controls



Limited visibility



Non-actionable
intelligence and
data silos

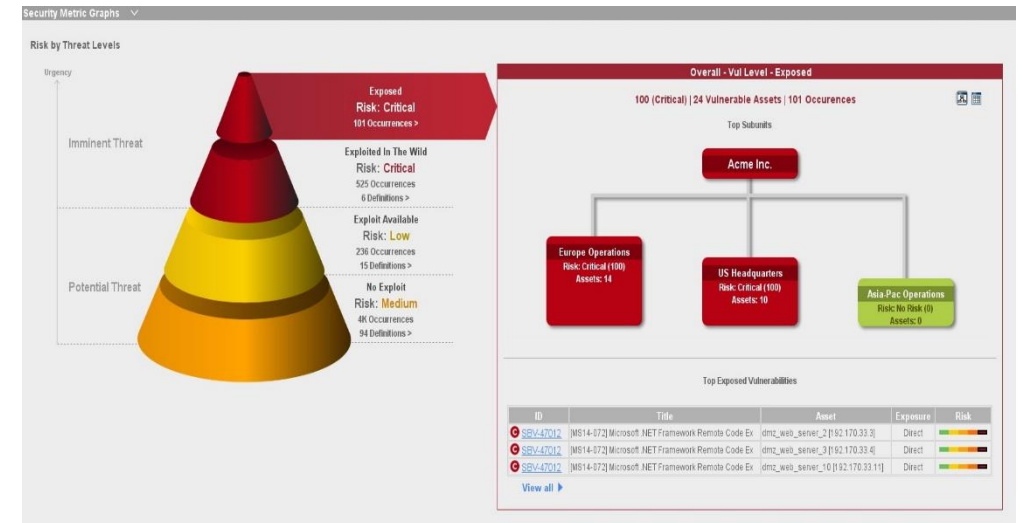
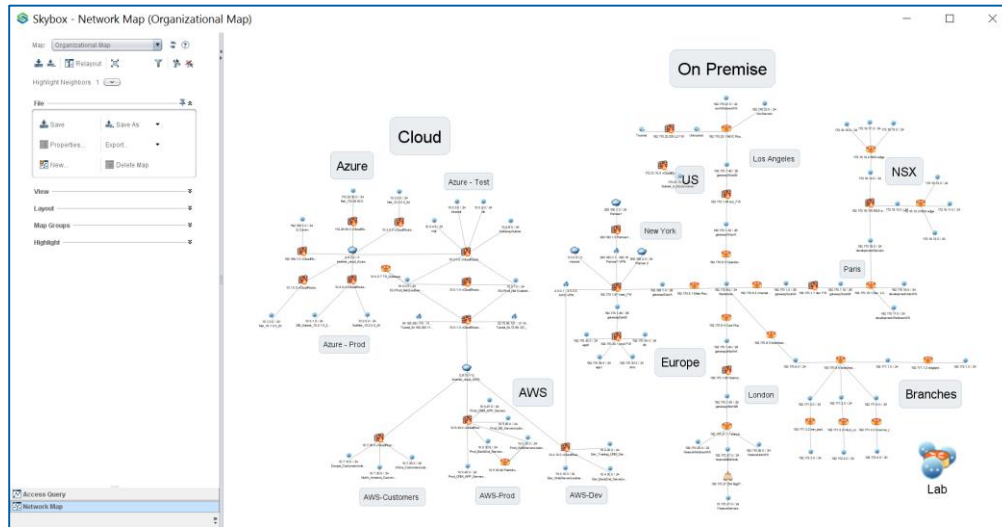


Lack of resources

Skybox is a cream on a Security cake

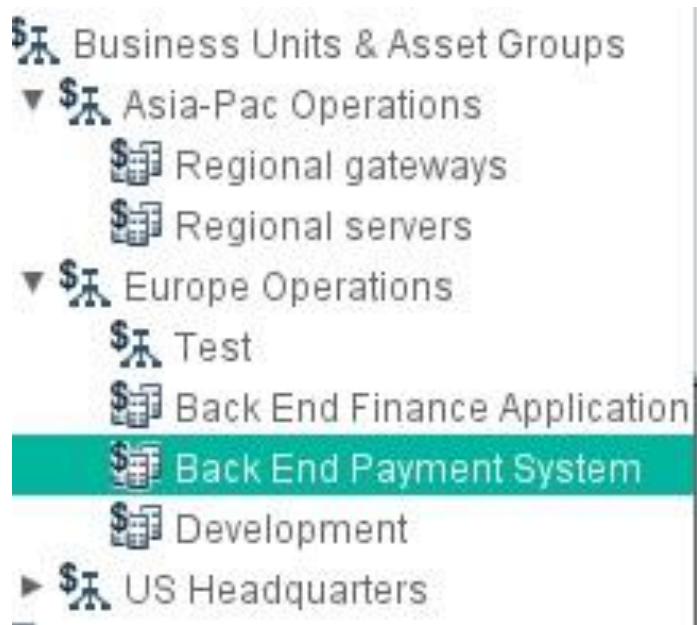
Complete
Infrastructure model

Complete
Attack Surface Visibility
with vulnerability prioritization



Keep business data and services safe

Business context awareness



Business impact awareness

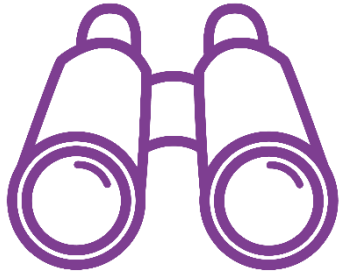


Continuous compliance monitoring



Why today's organizations need Skybox

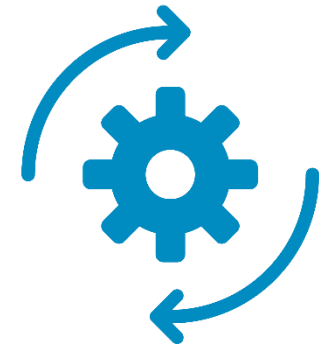
Skybox helps bridge the security management gap



Unparalleled visibility
and comprehensive
network modeling



Integration with
existing technologies
and added intelligence



Intelligent automation
and orchestration

Improve Existing Resources



Firewall/Network
Security &
Infrastructure



Vulnerability
Management,
SIEM



Endpoint
Security



Cloud/
Virtual



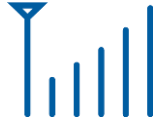
120+
technology
integrations



Who Relies on Skybox



Financial Services



Service Providers



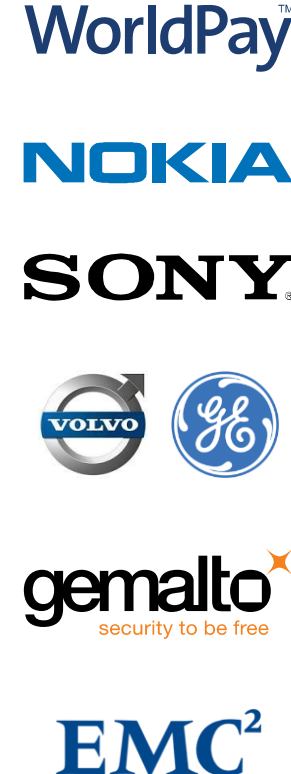
Government & Defense



Energy & Utilities



Technology & Manufacturing



Healthcare



Consumer



Skybox Security Suite

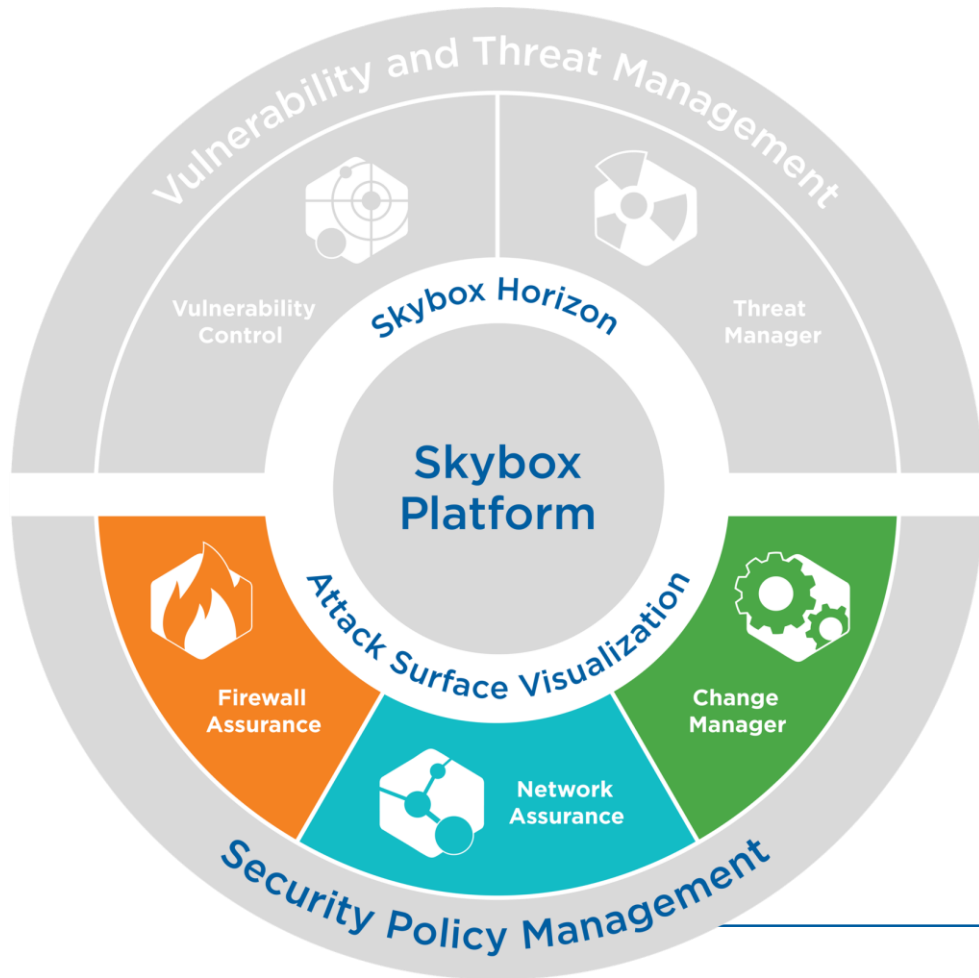


Integrated Security Management

Attack Surface Visualization

- Total visibility of the attack surface
 - Physical, virtual, cloud and OT environments
 - Vulnerabilities and threats
- Measurable risk reduction
- Improved communication across teams and up management chain

Skybox Security Suite



Integrated Security Management

Security Policy Management

- Easy, efficient compliance reporting
- Intelligent workflows and automation
- Proactive risk assessments of security and network changes

Security Policy Management



Model Network

- Network topology view
- Normalized data from 120+ technologies
- Physical, virtual, cloud and industrial
- Access simulation

**Understand
Network Context**



Analyze Security Controls

- Cloud security tags
- Firewalls
- Rule and configuration checks
- Network path analysis
- Rule optimization
- Change tracking

**Confirm
Effective Controls**



Monitor Compliance

- Automated audits
- PCI DSS
- FISMA
- NERC
- NIST
- GDPR
- Custom policies

**Document
Compliance**

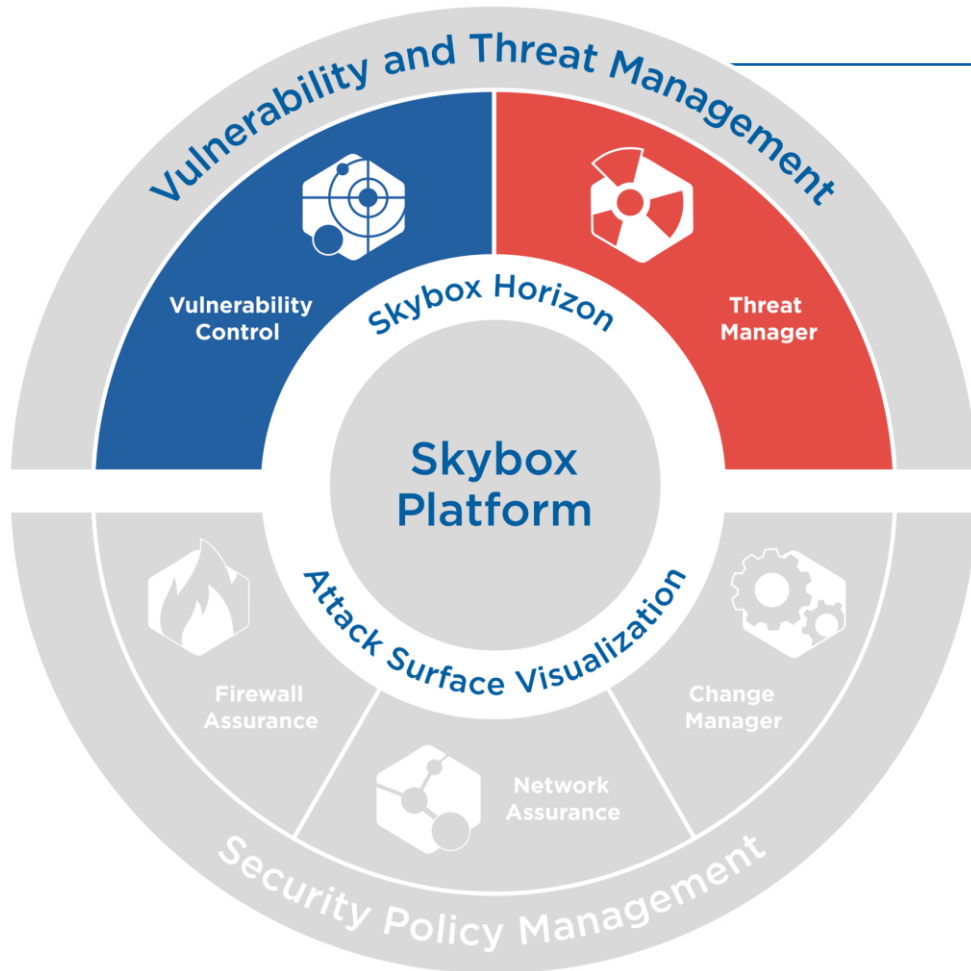


Change Management

- Change request
- Tech details
- Risk assessment
- Provisioning options
- Reconciliation and verification

**Continuously
Verify Rulebase**

Skybox Security Suite



Integrated Security Management

Vulnerability and Threat Management

- Vulnerability prioritization aligned to the current threat landscape
- Exposed and exploited vulnerabilities highlighted
- Resources directed where they're needed most

Vulnerability and Threat Management



Discover Vulnerabilities

- Scanless vulnerability detection (physical/cloud)
- Support for all third-party VA scanners
- Threat-centric vulnerability management

Same-Day Identification



Analyze Attack Surface

- Hot spot analysis
- Attack simulation
- Business impact
- Network topology and compensating controls
- Threat context

Highlight Assets at Risk



Prioritize Response

- Imminent threats (exposed/active exploit)
- Potential threats (known/available exploit)
- Attack vector details

Focus on Areas of Greatest Impact



Remediate & Track

- Remediation planning
- Ticketing and workflow
- Dashboards and reporting

Respond Quickly

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

Firewall Assurance

Comprehensive Multi-Vendor Firewall Management

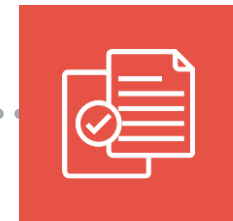
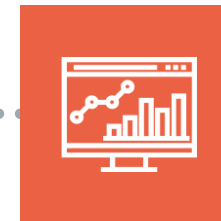
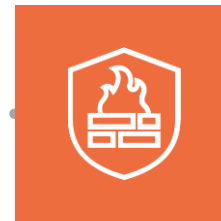
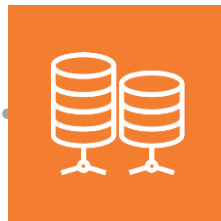


Firewall
Security Assessment

Continuous
Policy Compliance

Firewall Rule
Life Cycle Management

How It Works



Collect & Normalize

Analyze

Report & Act

Optimise Rules

- Spot shadowed and redundant rules quickly
- Gather log data to analyse historical rule usage
- Tighten the rule base, improve security and effectiveness
- Have a consultative conversation



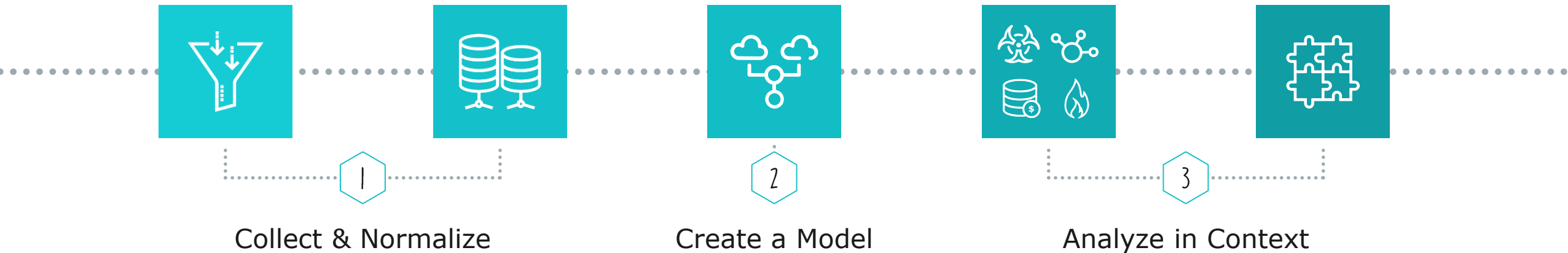
Network Assurance



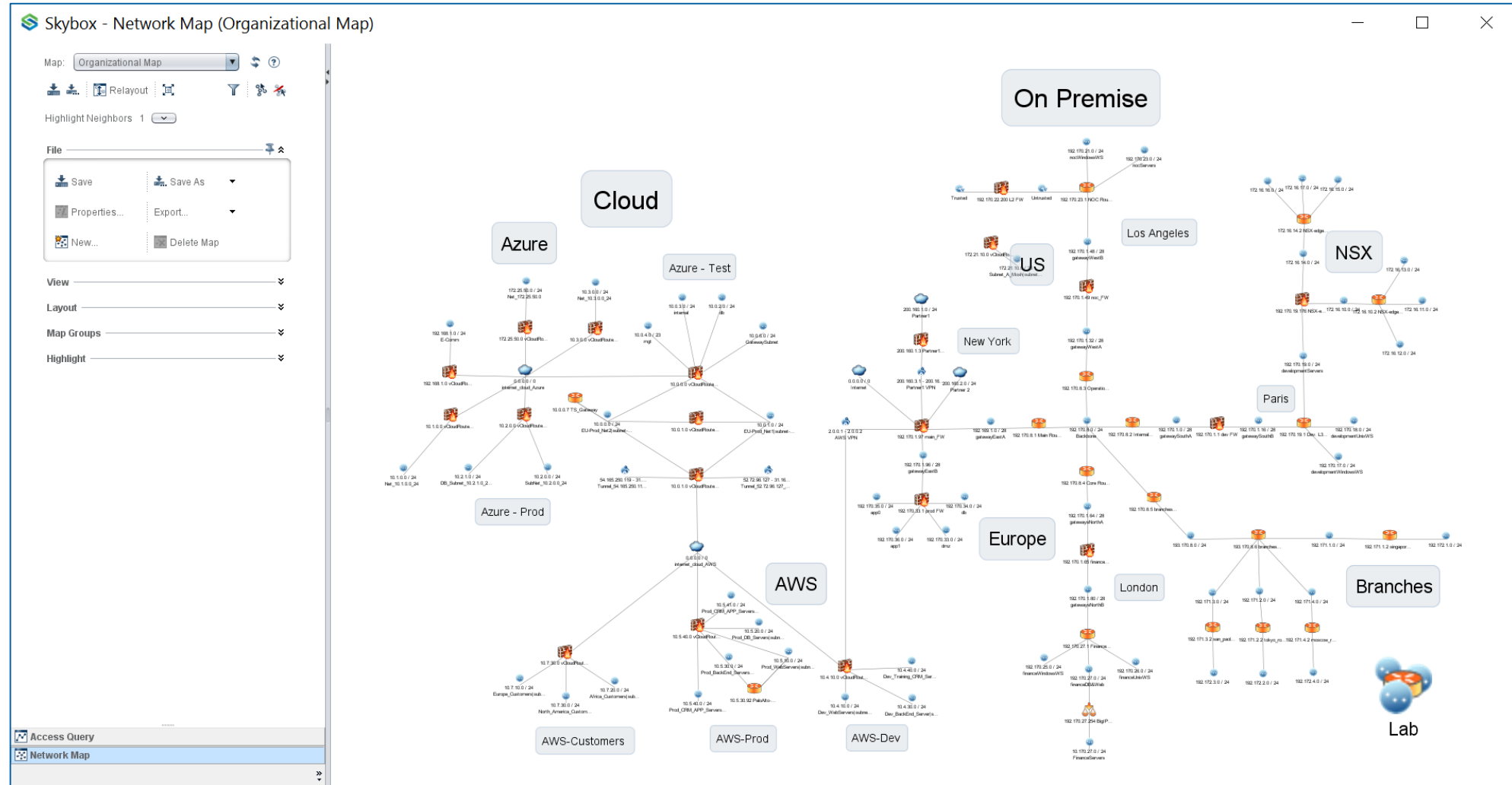
Complete Visibility and Command of Hybrid Network Access and Routes



How It Works



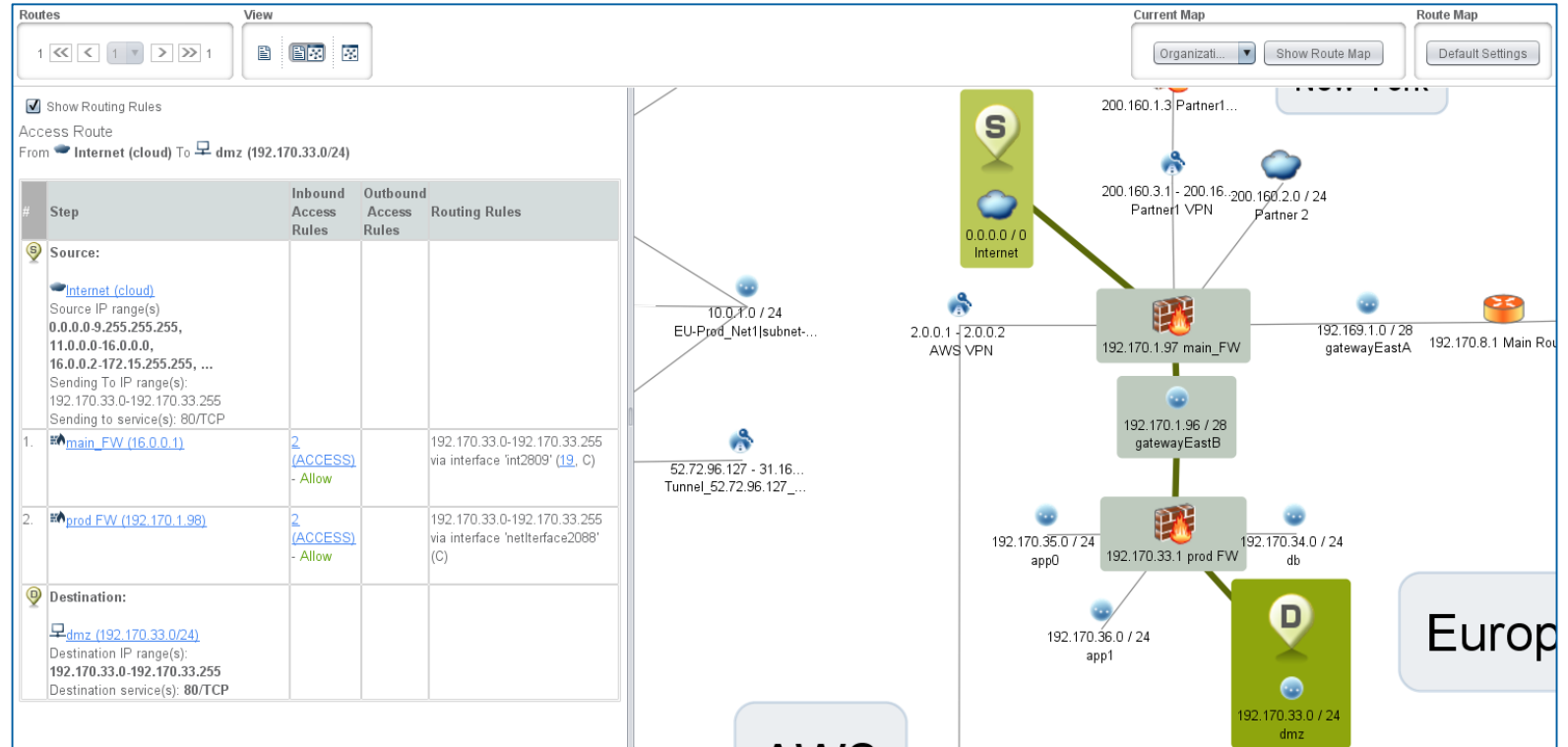
Network Model Visualization



Network Path Analysis

Access Analyzer Understands

- Routing/PBR
- NAT/PAT/VPNs
- Load Balancing
- Firewall rules
- Multiple routes



Change Manager

Secure, Automated Firewall Change Management



Change Management
Automation

Automated Risk
Assessment

Rule Recertification
Workflow

How It Works



1

Request



2

Identify



3

Assess



4

Implement



5

Verify

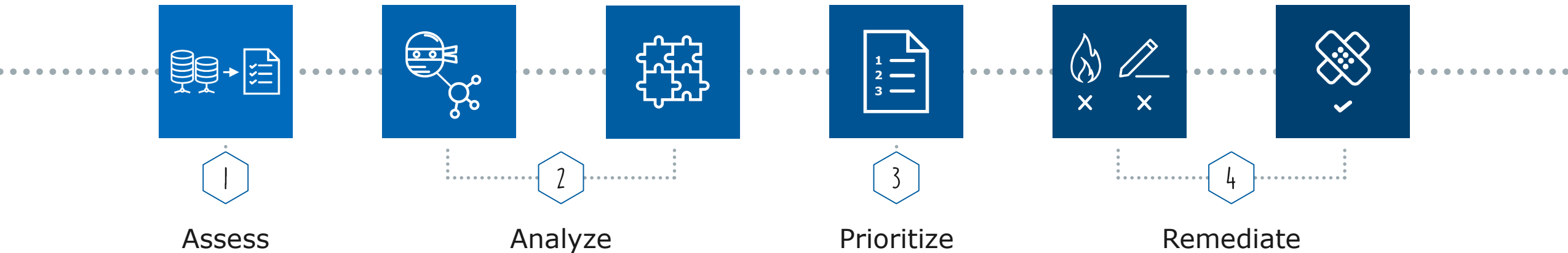
Vulnerability Control



Threat-Centric Vulnerability Management



How It Works



Skybox Vulnerability Database

30+ threat feeds



Dedicated team
verifies, normalizes,
adds more data

Subscribed customers
updated daily



Threat-Centric Vulnerability Management



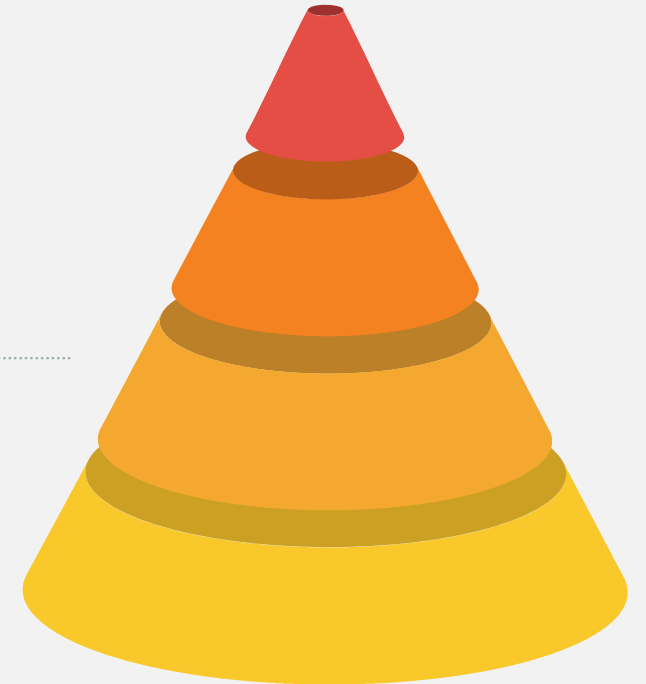
Analytics

A flow diagram consisting of a dark blue square labeled 'Analytics', a light blue right-pointing triangle, and a medium blue square labeled 'Prioritize'.

Prioritize

Imminent Threat
High-priority
remediation/mitigation

Potential Threat
Gradual risk
reduction

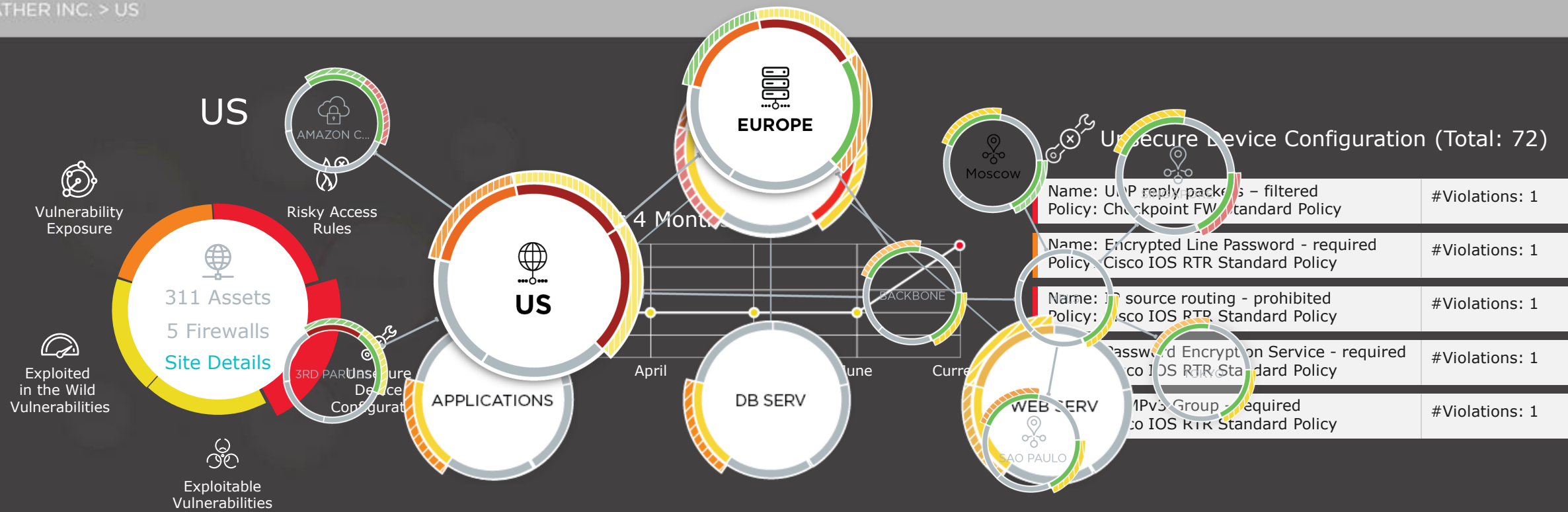


Visualize Your Entire Attack Surface From Multiple Perspectives

Skybox Horizon | CATHER INC

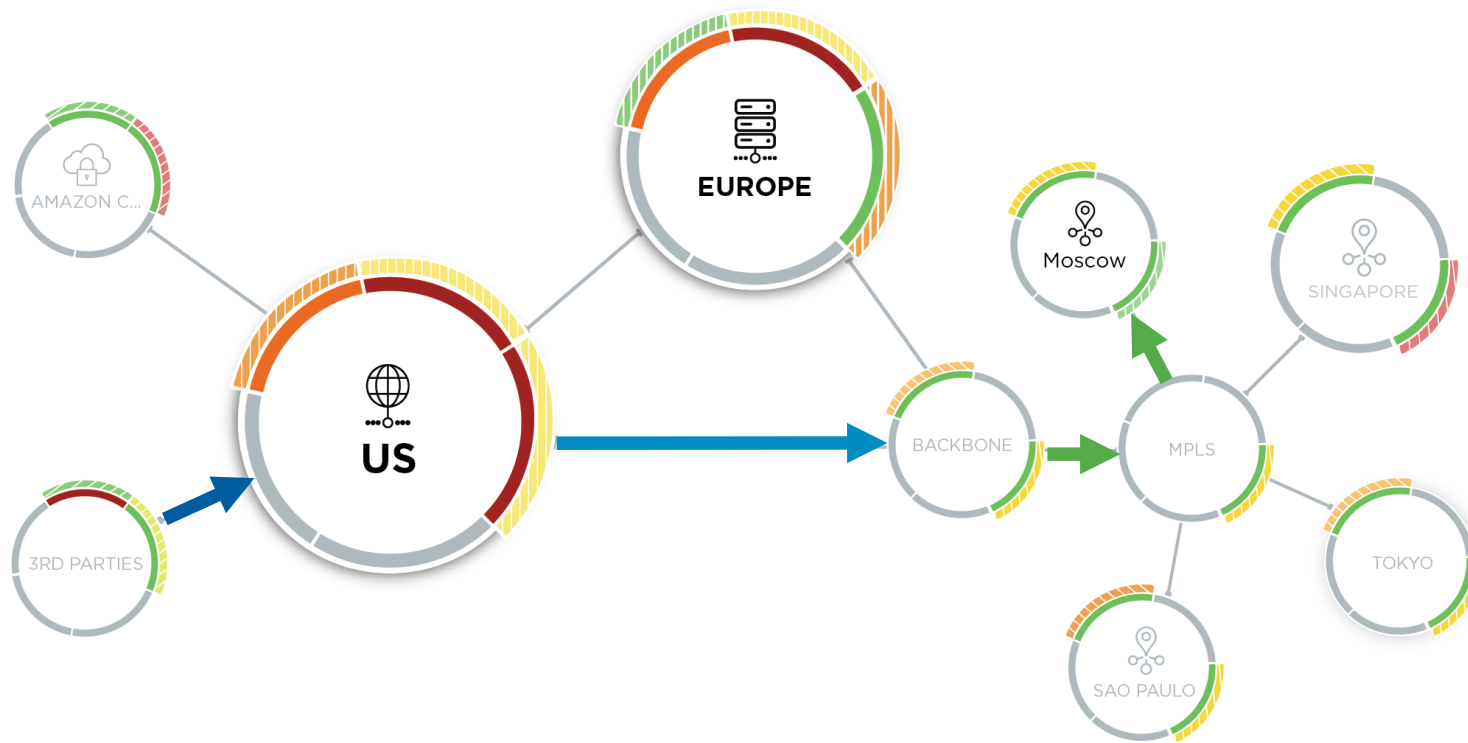


CATHER INC. > US



Skybox Horizon

Attack Surface Visualization



Risky Access Rule

Allows inbound access from DMZ to deeper in network



Exploited in the Wild Vulnerability

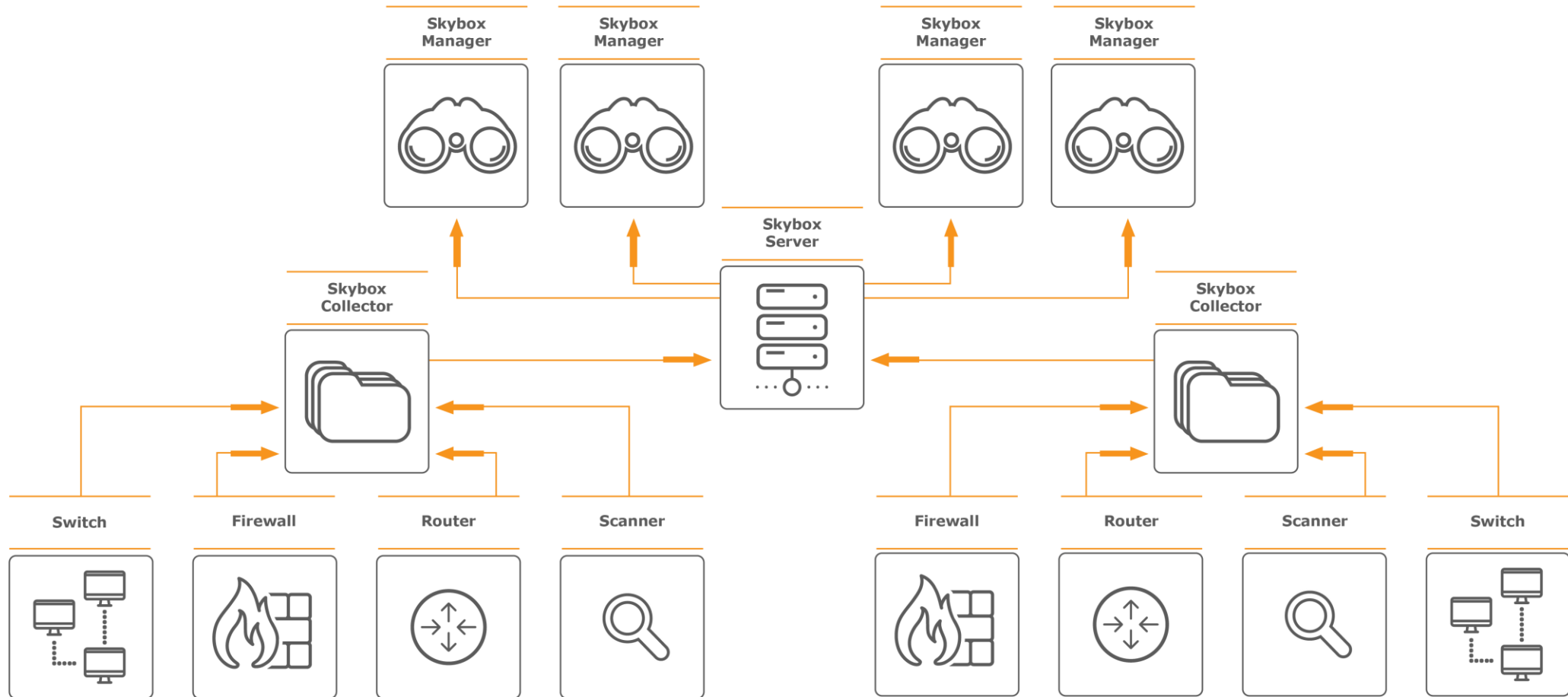
Vulnerability with available and active exploit is attacked



Unsecure Device Configuration

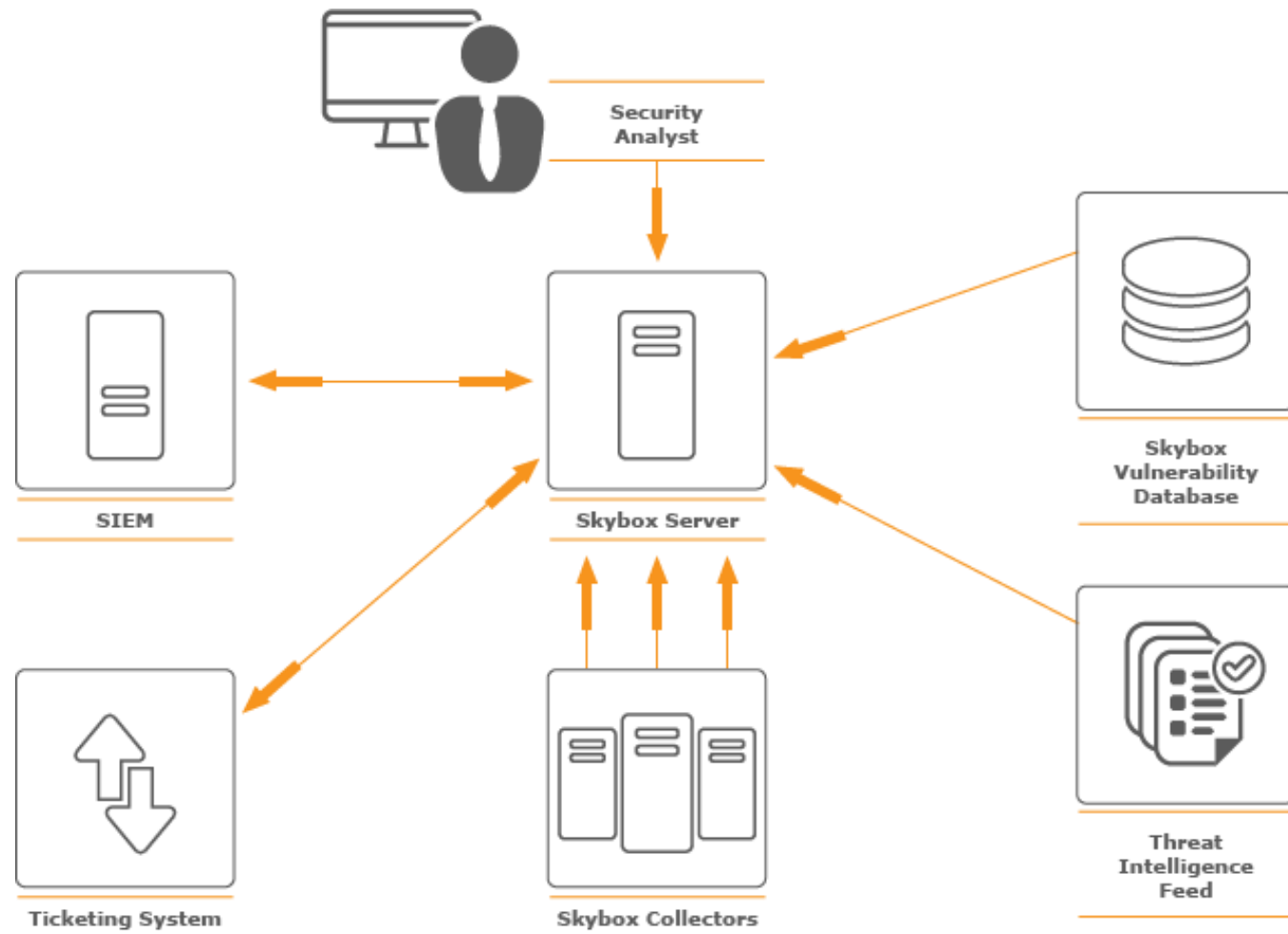
Misconfiguration enables the continuation and spread of attack

Skybox Architecture



Deployment Diagram

- Integrates with existing infrastructure
- Automation, workflows
- Not a scanner, Agentless
- Built-in ticketing system
- APIs for integration with third-party systems
- Appliance, virtual appliance, software only



Skybox licensing

- From architecture perspective Enterprise and Standard version
 - Enterprise – Unlimited number of Collectors and Manager software instances
 - Standard – Five Collectors and Five Manager software instances
- All modules per device license
 - Firewall Assurance – per firewall
 - Network Assurance – per L3 network device
 - Change Manager – per firewall
 - Vulnerability Control – per asset imported into Skybox
 - Threat Manager – per asset imported into Skybox

References in the region

- Air-traffic Control Ljubljana



- National Employment Agency Belgrade





Thank You

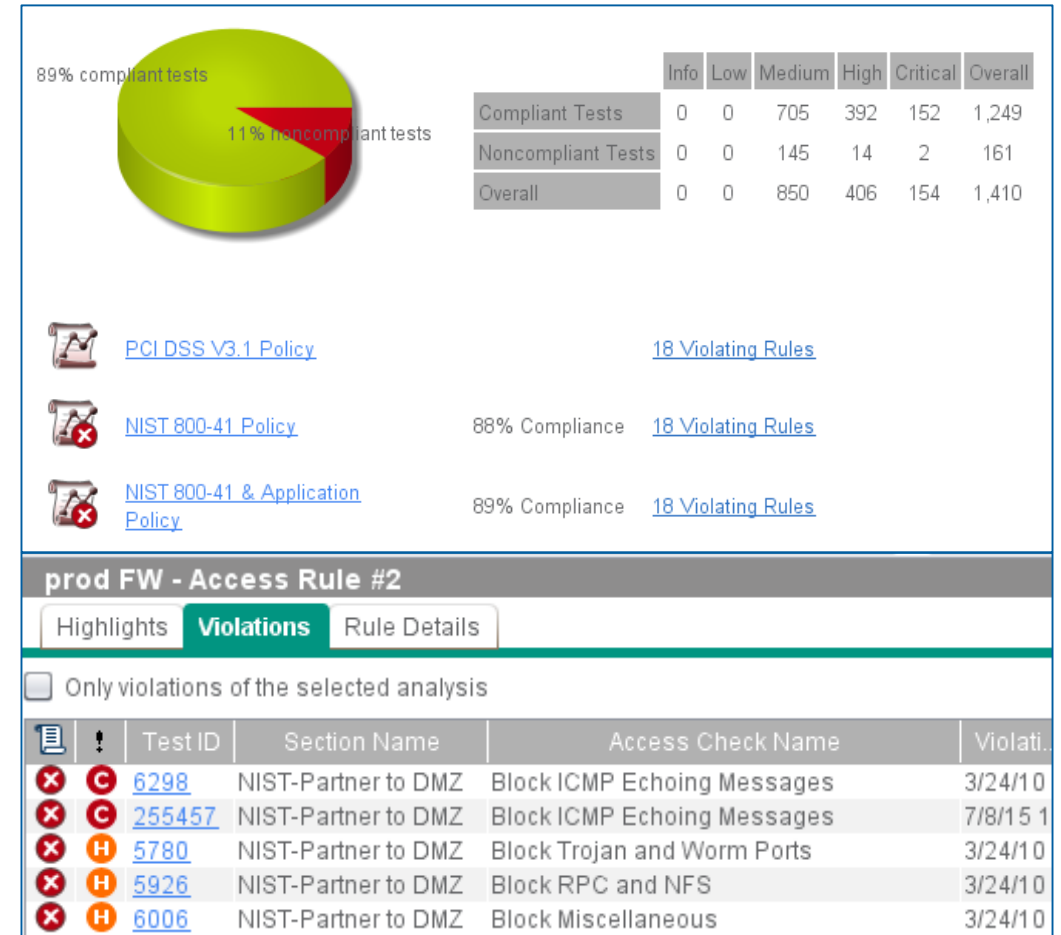


Co.Next

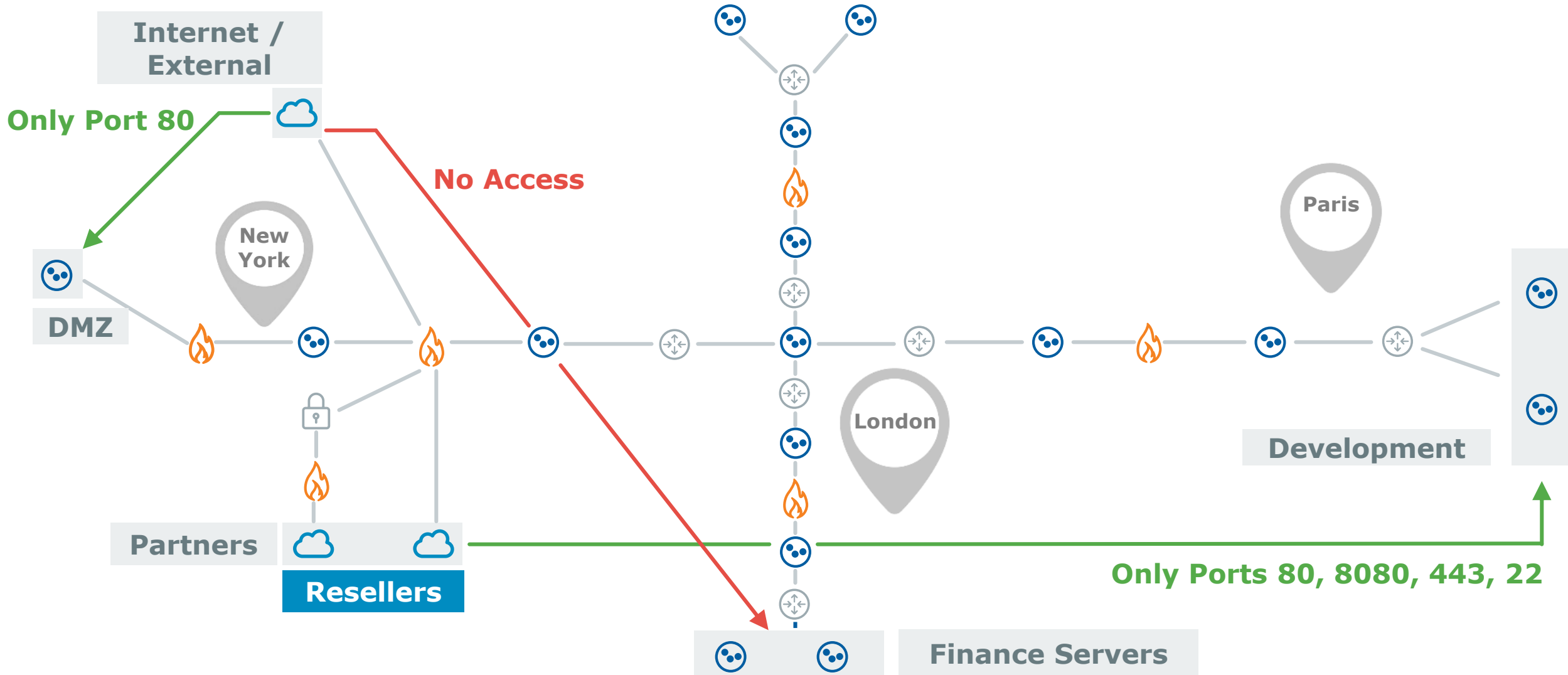
Continuous Compliance Monitoring

Automated Compliance Checks

- **Access** Compliance
- **Configuration** Compliance
- **Rule** Compliance
- PCI, NIST, Custom Policies
- Vendor best practices
- Track exceptions



Zone-to-Zone Access Compliance



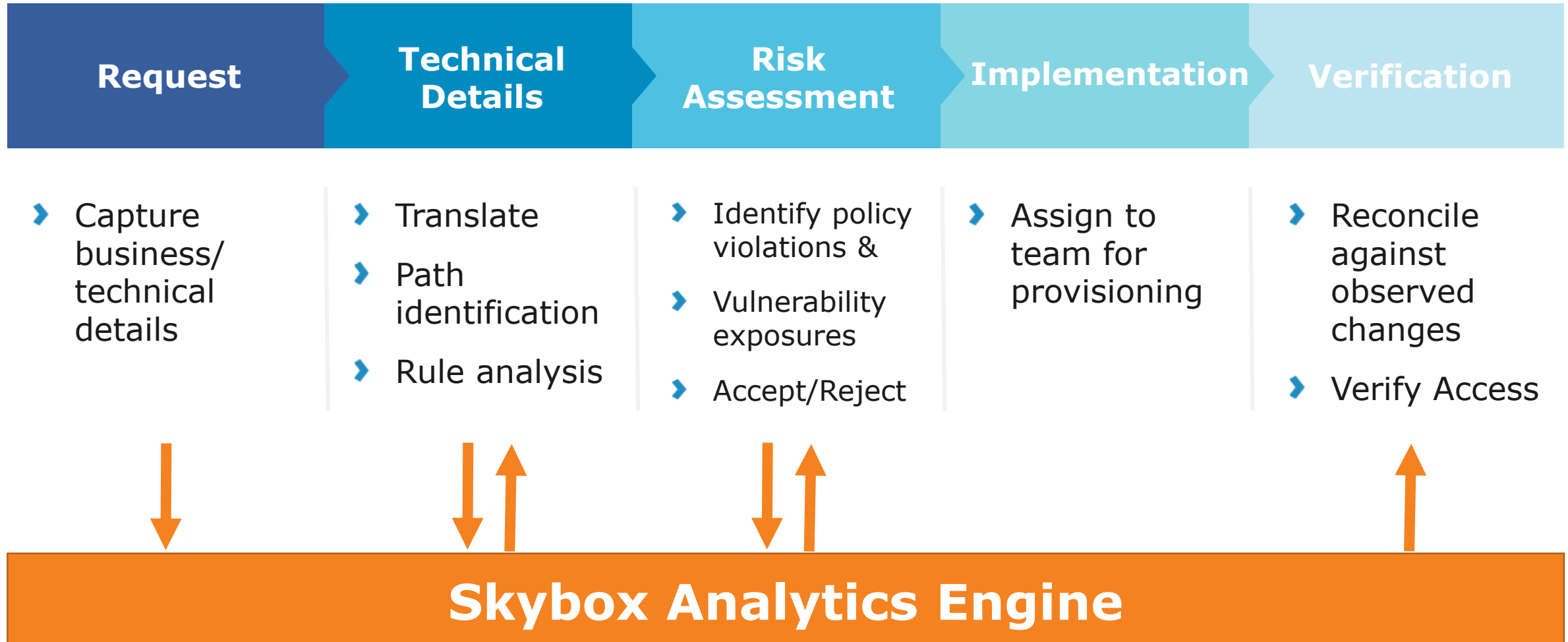
Optimizing Change Management Workflow

Automate Change Management

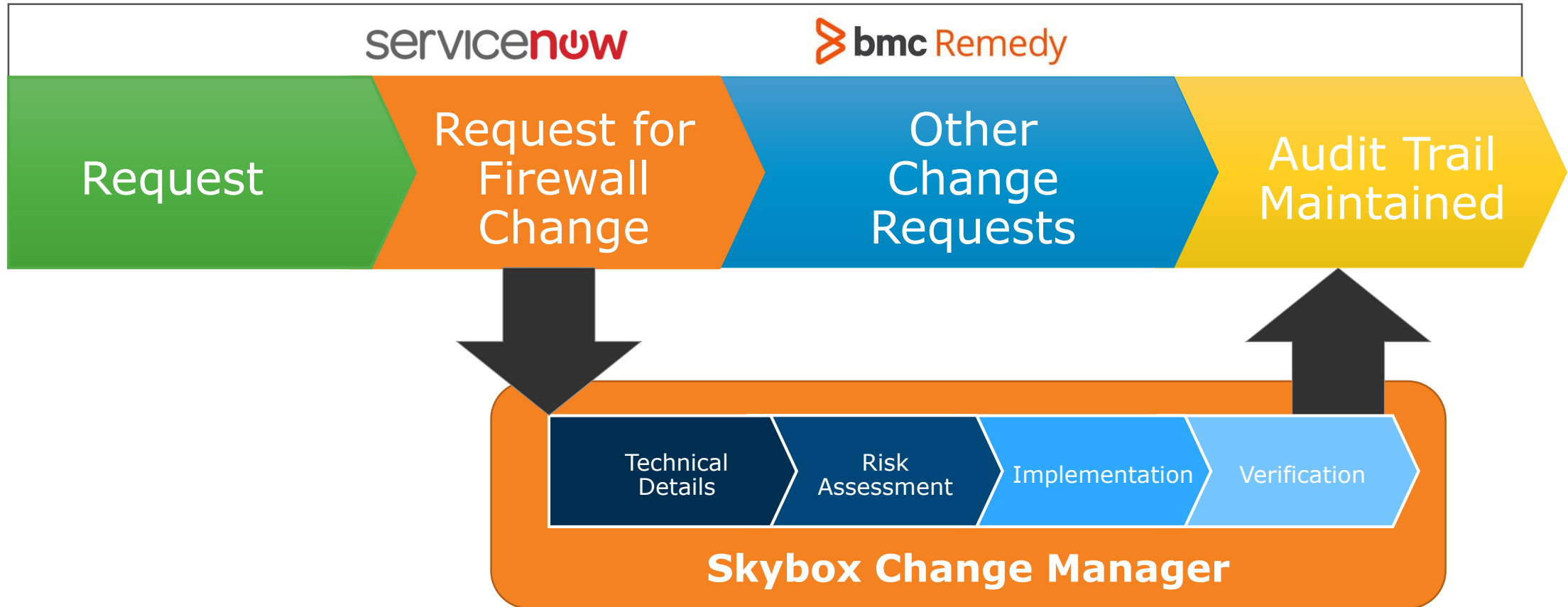
- Vastly improve operational costs
- Reduce time to implement changes
- Risk assessment before change is made
- Automate changes/generate configuration
- Reconcile changes



Change Management Workflow



Change Management Workflow



Skybox Vulnerability Database

- Skybox Research Lab aggregates **30+** vulnerability and threat feeds
- More than **70,000** vulnerabilities on **8,000+** products
- CVE compliant, CVSSv3 standard
- Updated **daily**

ADVISORIES

Adobe
Apple
Cisco

Microsoft
Oracle
Red Hat

SCANNERS

BeyondTrust
Retina
McAfee Foundstone
Qualys Cloud Platform

Rapid7 Nexpose
Tenable Nessus
Tripwire IP360

IPS

Fortinet FortiGuard
McAfee IPS
Palo Alto Networks
Trend Micro TippingPoint
Cisco SourceFire

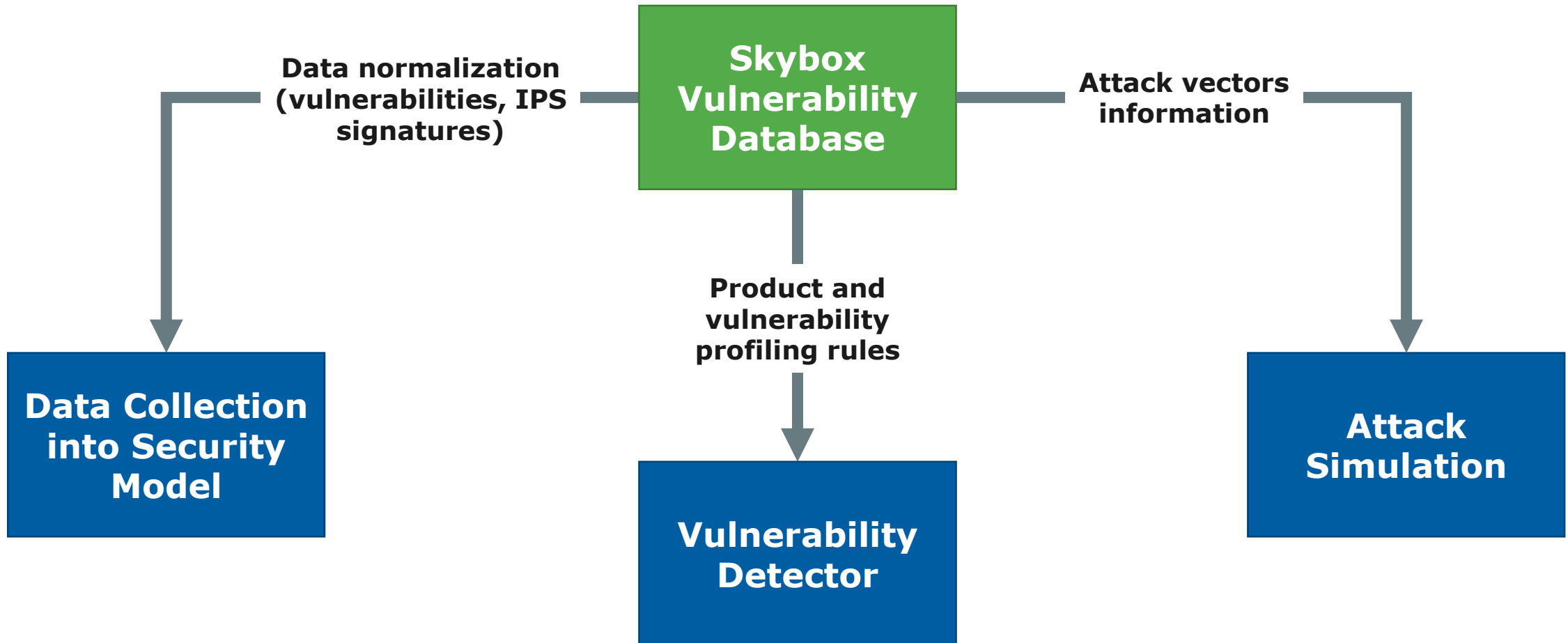
OTHER

CERT, ICS CERT
Flexera Secunia
IBM X-Force
Mitre CVE
NIST NVD
OSVDB

Symantec Security Focus
Rapid 7 Metasploit
Zero-day vulnerabilities for published incidents



Main Uses of the Vulnerability Database



Remediate the stuff that matters!

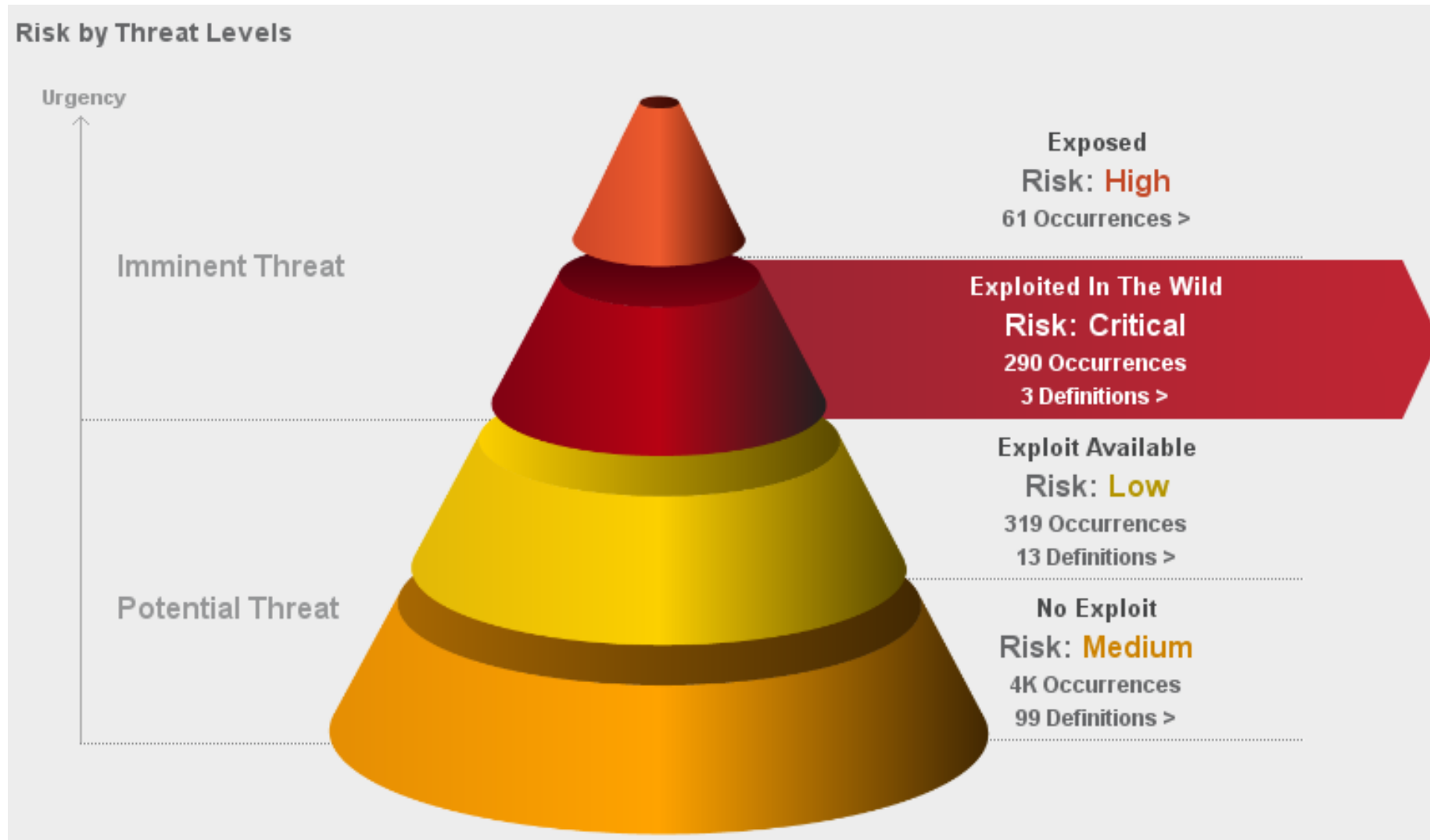
Threat-Centric Vulnerability Management

- How do we prioritize for remediation?
- Are critical assets at risk?
- What's our trend in fixing vs finding vulnerabilities?
- Which vulnerabilities should I fix for the biggest impact?

Vulnerabilities Identified




!	Exposure	Title	ID	CVE	Asset	Risk
H	Direct	ISC BIND 9 DNSSEC NXD...	SBV-24643	CVE-2010-0097	dmz_dns0 [192....	69
H	Direct	ISC BIND 9 DNSSEC NXD...	SBV-24643	CVE-2010-0097	dmz_dns1 [192....	69
C	Direct	[MS12-074] Microsoft .NET...	SBV-37240	CVE-2012-4777	dmz_web_serve...	58
C	Second S...	IBM WebSphere 5.3 HTTP...	SBV-37740	CVE-2012-5955	finance_web_6 [...	51
C	Direct	[MS12-074] Microsoft .NET...	SBV-37240	CVE-2012-4777	dmz_ftp0 [192.1...	46
C	Direct	ProFTPD < 1.3.3g Respon...	SBV-33883	CVE-2011-4130	dev_ftp0 [192.17...	41
M	Direct	Microsoft IIS 6.0 and 7.5 R...	SBV-35467		dmz_web_serve...	33
H	Direct	[MS13-007] Microsoft .NET...	SBV-37940	CVE-2013-0005	dmz_web_serve...	29
H	Second S...	Apache Chunked-Encodin...	SBV-00926	CVE-2002-0392	dev_web5 [192....	28
M	Direct	ISC BIND Internal Memory...	SBV-00492	CVE-2001-0012	dmz_dns0 [192....	3
M	Second S...	Apache Tomcat Remote L...	SBV-39658	CVE-2013-2071	finance_web_8 [...	1
M	Direct	Microsoft IIS 6.0 and 7.5 A...	SBV-35322		dmz_web_serve...	1
M	Direct	Microsoft IIS 1.0, 5.0, 6.0 a...	SBV-35454		dmz_web_serve...	1
M	Direct	Microsoft IIS 6.0 and 7.5 R...	SBV-35467		dmz_web_serve...	1
M	Direct	Microsoft IIS 6.0 and 7.5 A...	SBV-35322		dmz_web_serve...	1
M	Direct	Microsoft IIS 1.0, 5.0, 6.0 a...	SBV-35454		dmz_web_serve...	1
L	Direct	IIS 5.0 with Index Server Di...	SBV-00279	CVE-2000-0951	app_7_web_4 [1...	1
H	Direct	[MS13-007] Microsoft .NET...	SBV-37940	CVE-2013-0005	dmz_web_serve...	1
H	Second S...	Apache Tomcat 7.0.* and ...	SBV-37746	CVE-2012-5568	finance_web_8 [...	1
H	Second S...	Apache Tomcat 7.0.* and ...	SBV-37746	CVE-2012-5568	finance_web_7 [...	1
H	Direct	ProFTPD before 1.3.4d Re...	SBV-41671	CVE-2013-4359	dev_ftp0 [192.17...	1
M	Second S...	Apache 2.0 Encoded Back...	SBV-00897	CVE-2002-0661	dev_web0 [192....	1
M	Second S...	[cpujan2014-1972949, cp...	SBV-39750	CVE-2012-3544	finance_web_8 [...	1
M	Second S...	Subversion 'mod_dav_svn...	SBV-39276	CVE-2013-1849	finance_web_8 [...	1
M	Second S...	ISC BIND Internal Memory...	SBV-00492	CVE-2001-0012	dev_dns5 [192.1...	1
M	Second S...	Subversion 'mod_dav_svn...	SBV-39276	CVE-2013-1849	finance_web_7 [...	1

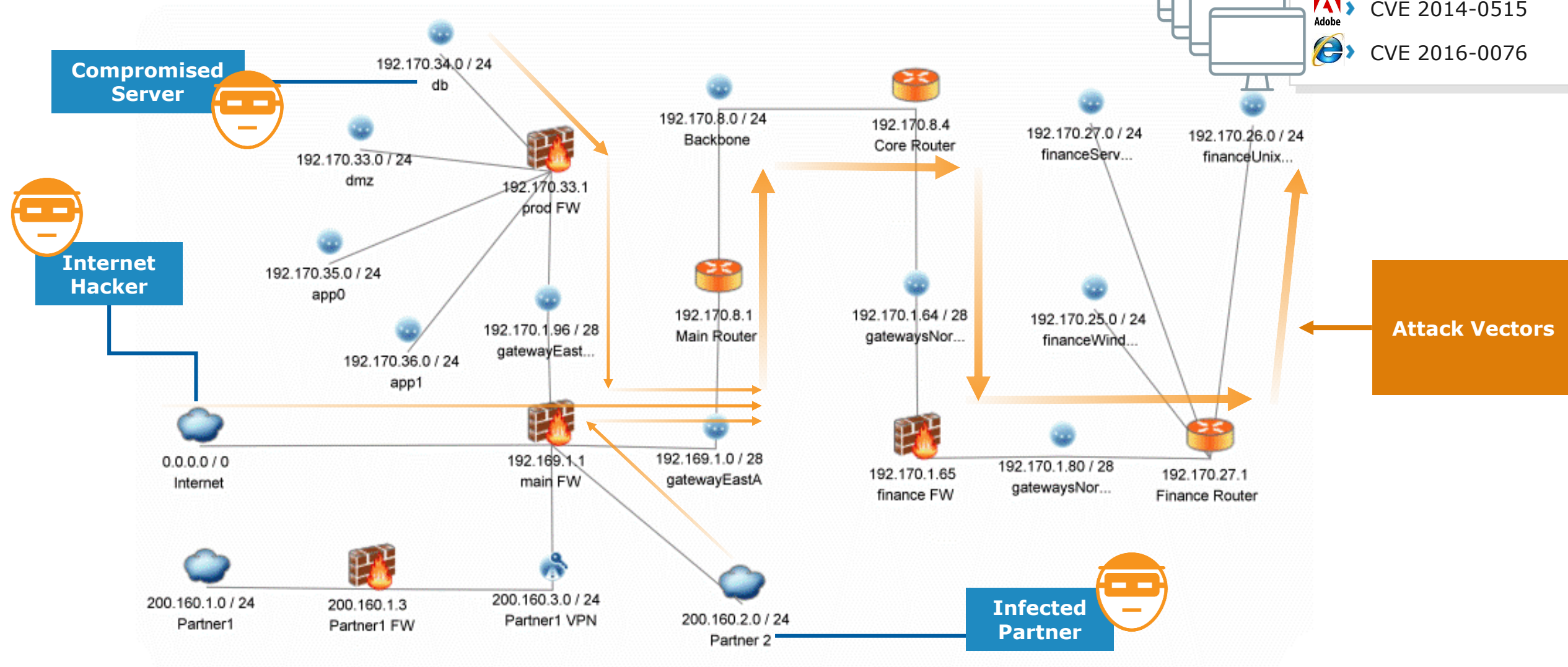
Threat-Centric Prioritization



Attack Simulation

Vulnerabilities

-  CVE 2014-0160
-  CVE 2014-0515
-  CVE 2016-0076



Thank You

