

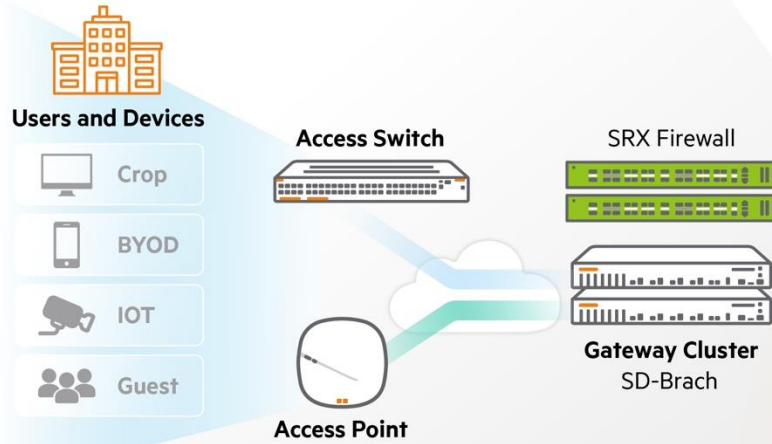
HPE Security Solution

Prado Yang

Aug. 2026

HPE Networking Security Solution

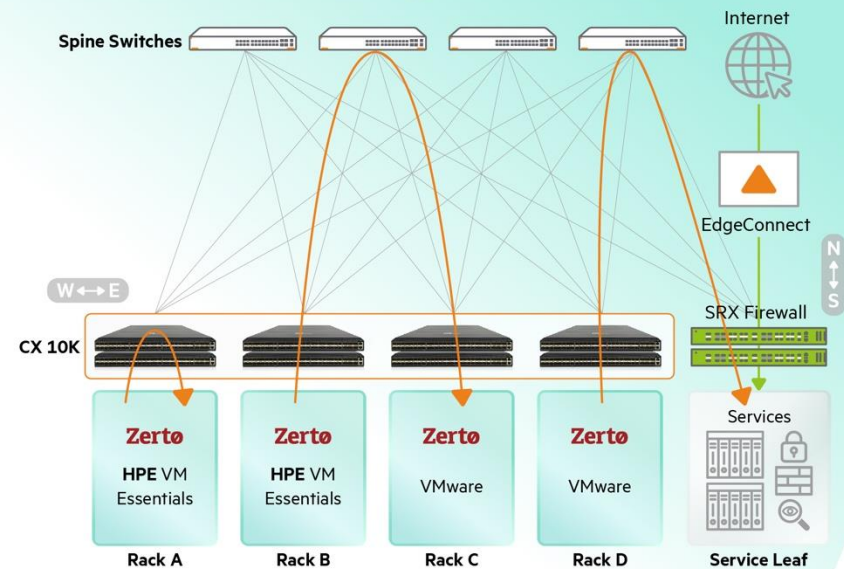
Campus Role-based Segmentation



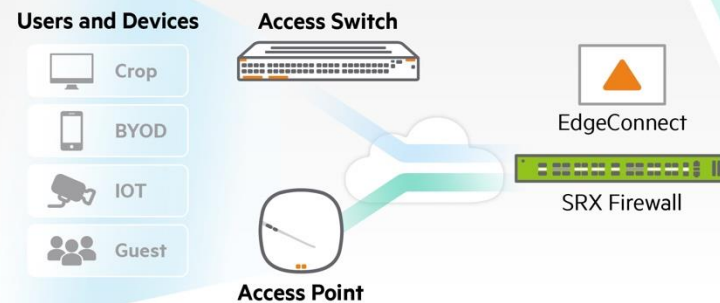
Remote workforce User Segmentation



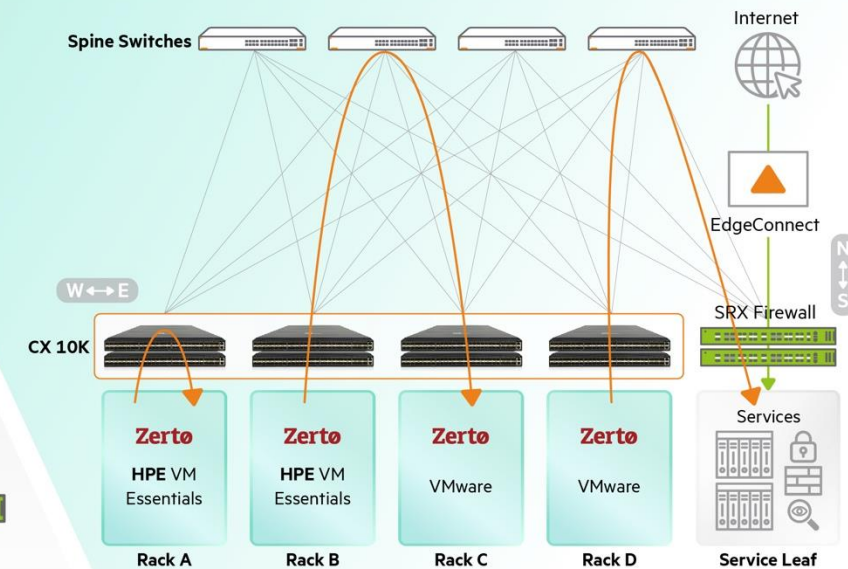
Data Center Micro Segmentation



Branch Role-based Segmentation



DR site



Agenda

01 從防火牆到零信任 – 威脅與因應策略

02 從單點防護到區域聯防 – 阻斷入侵橫向滲透

03 PQC概觀介紹

Zero Trust





74%

of all attacks succeed via network-based attack vectors

78%

of IoT network devices have known vulnerabilities

3.8Tbps

largest recorded DDoS attacked
(stopped by Cloudflare in Sept 2024)

40k+

vulnerabilities reported (CVEs)
in 2024 alone

57%

increase in blocked
AI transactions signaling security risks from AI

And each can have a financial impact

<https://thehackernews.com/2024/10/cloudflare-thwarts-largest-ever-38-tbps.html>
<https://www.sdxcentral.com/articles/analysis/2024-quantum-predictions-in-computing-ai-and-cybersecurity/2024/01/>
<https://www.zscaler.com/blogs/security-research/new-ai-insights-explore-key-ai-trends-and-risks-threatlabz-2024-ai-security>

\$4.88M

Average cost
of a breach

\$9.36M

United States average

\$4.99M

Costliest attack vector Malicious
insider attacks

\$2.2M

Savings from extensive
use of AI

Source: IBM Cost of data breach report 2024

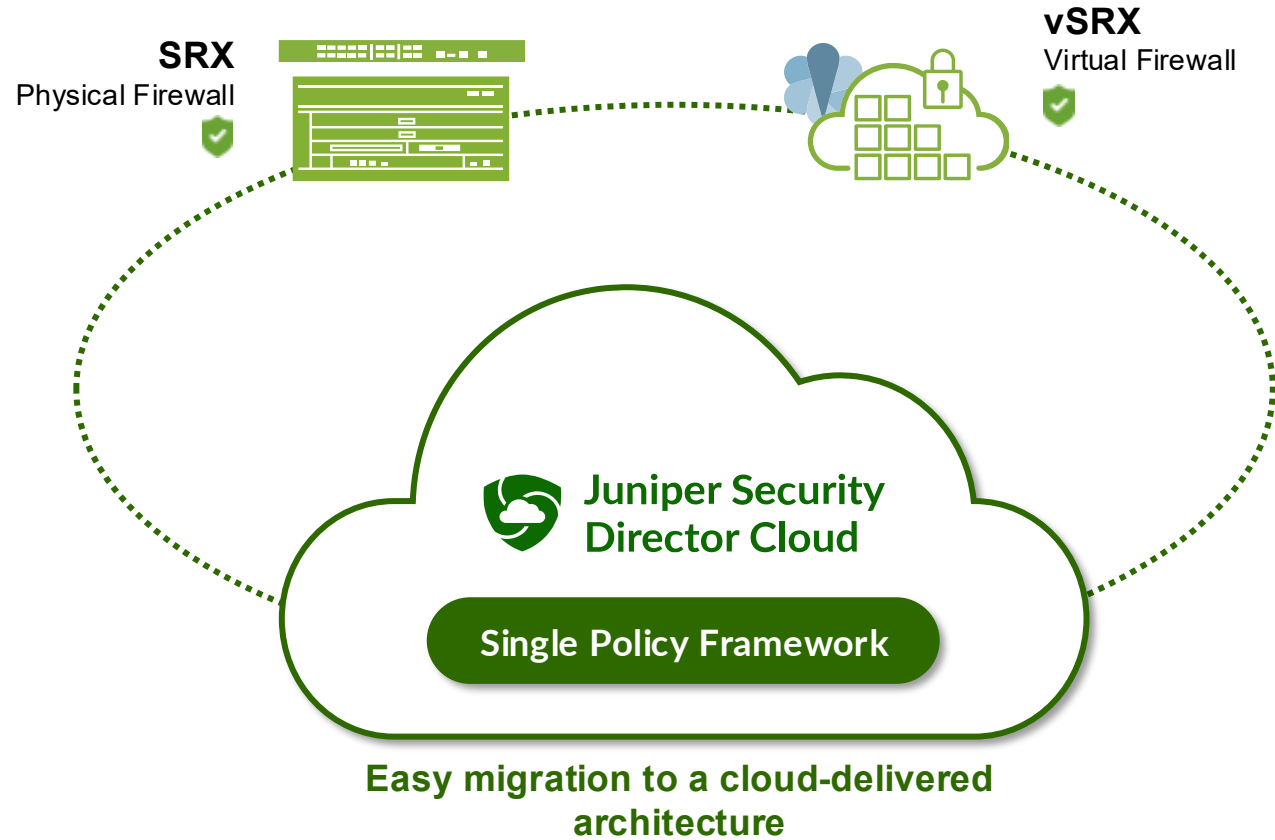




Integral Security

Unified Policy Management and Analytics

Enabling Hybrid Mesh Firewall



Secure Access
Remote Workforce

Campus & Branch
Security

Public & Private
Data Center

HPE Juniper Hybrid Mesh

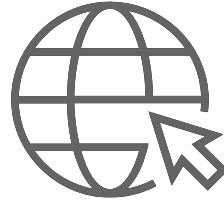


Protecting the enterprise edge

Extend Zero Trust to every application



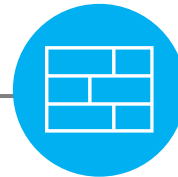
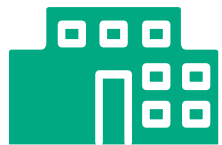
Secure data in on-premises & cloud native applications



Protect user & device access from anywhere - branch or remote locations



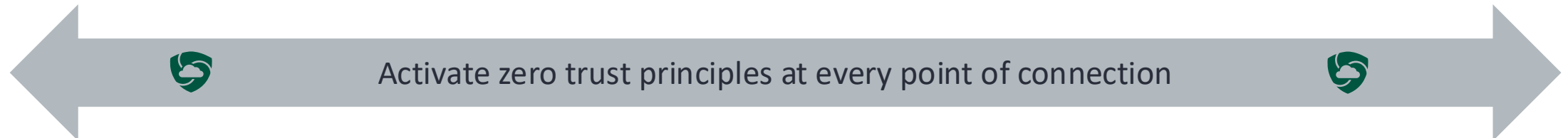
Full visibility from client to application



SRX NGFW

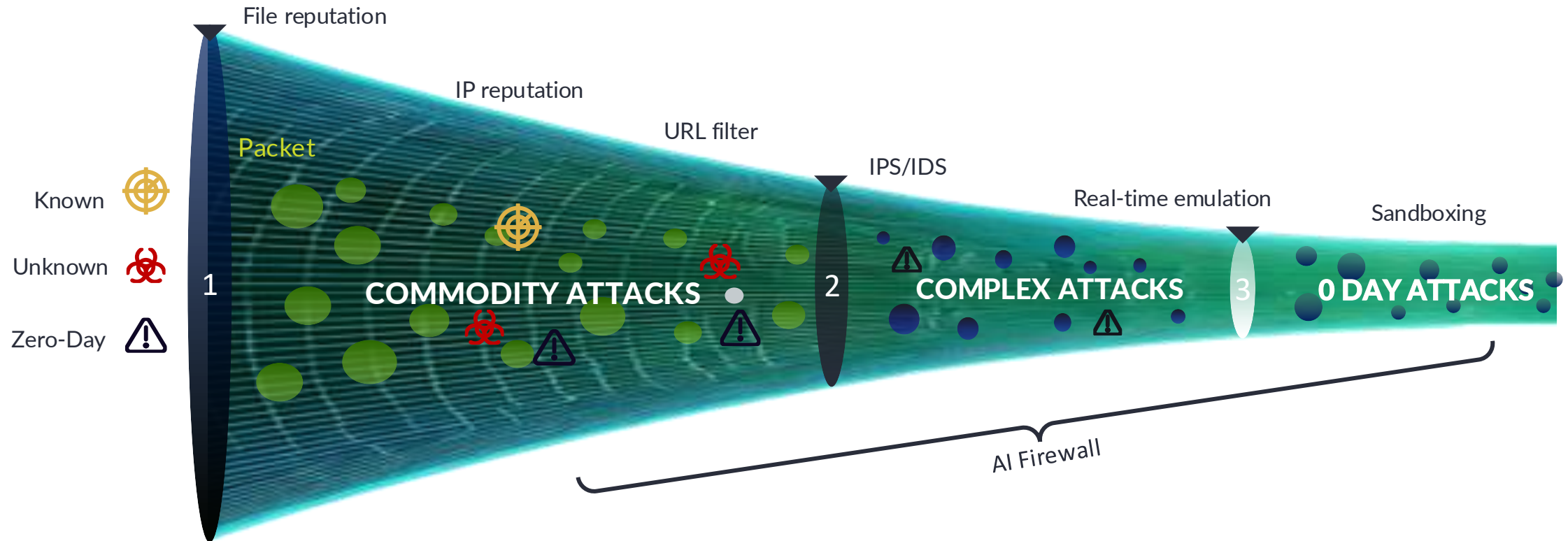


Security Director

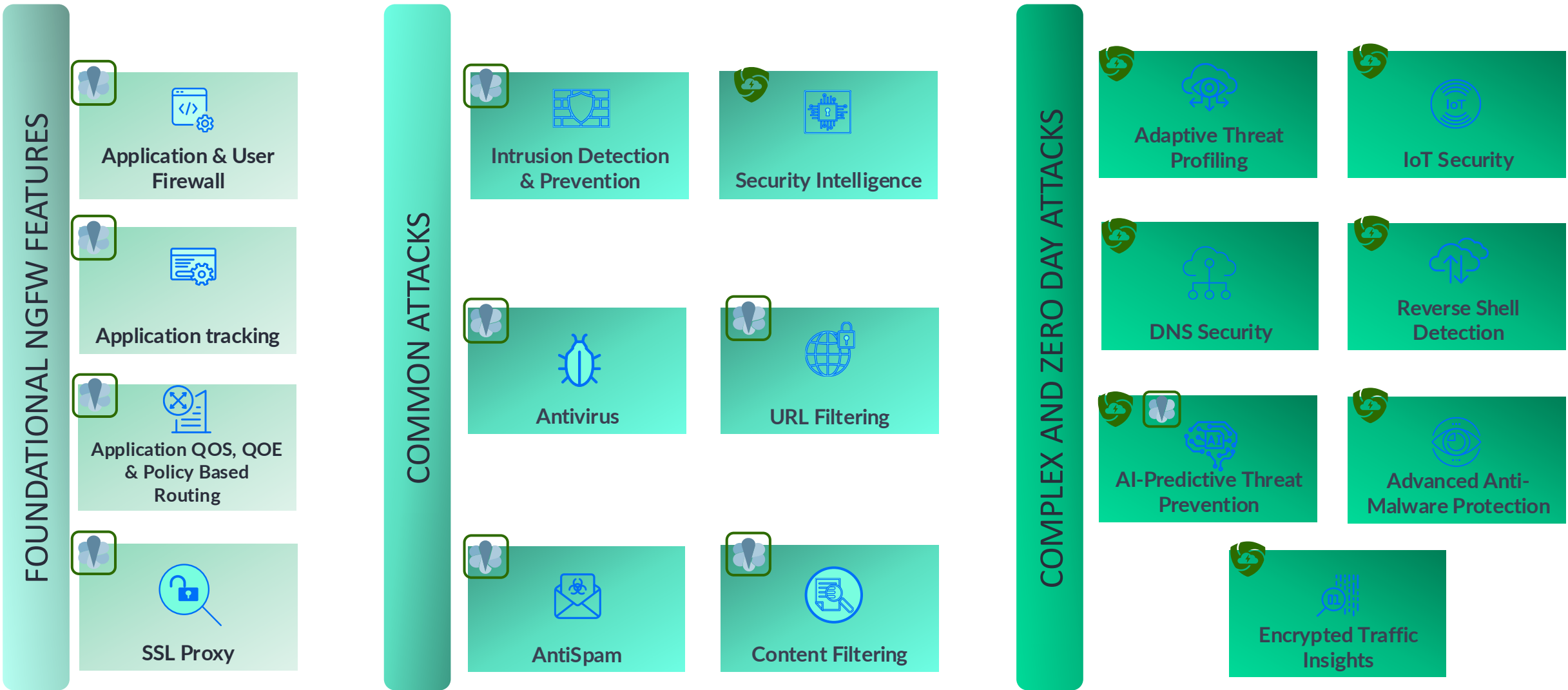


Actionable Security Intelligence

Convergence of Networking & Security Demands Exceptional Integration



Comprehensive security stack for threat protection



Content Security



Web Filtering

- Identify web traffic by category and reputation.
- Block malicious & unwanted web sites



Antivirus

- Keep known malware out of the network
- Prevent threats from installing on internal devices



Anti-Spam

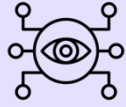
- Prevent unsafe and annoying email out of the network
- Reduce the risk for email as an attack vector



Content Filtering

- Identify and prevent unsafe files or scripts from being downloaded.
- Implement's DLP to reduce the risk for file-based attacks.

Benefits of Security Intelligence (SecIntel)



Continuously Updated Threat Intelligence

- Curated feeds include malicious IPs, URLs, domains, certificate hashes, and GeoIP
- Threat data is updated and validated in real-time to increase threat coverage and reduce FPs



Automated Detection and Mitigation

- Infected host feeds automate detection and mitigation of security events, identifying and blocking threats closer to the source.



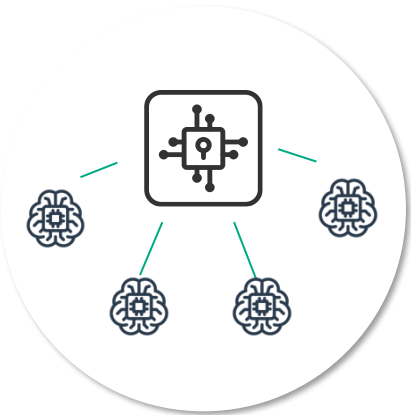
Customizable Threat Intelligence

- Ability to add custom sourced feeds.
- This allows flexibility to utilize their own threat intelligence into the system and delivered across all SRX's.



Real-Time Threat Identification

- SecIntel delivers real-time threat intelligence, enabling automatic and responsive traffic filtering.
- Malicious traffic is blocked at line rate, creating a threat-aware network that actively participates in its own defense.



Benefits of Content Security



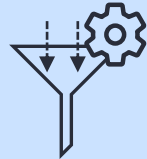
Comprehensive Protection

- Comprehensive protection against malware, viruses, phishing attacks, intrusions, spam, and other security threats.
- Different techniques used for detecting the right content for the right feature.



Streamlined Installation and Management

- Separate Content Security profiles allow security capabilities to be specified on a per policy basis, aligned with customer environment
- Streamlines and simplifies installation and management of multiple security capabilities with selective action



Advanced Filtering Capabilities

- Advanced filtering capabilities such as URL filtering, antivirus filtering, and content filtering, which can be configured using custom objects (file types or categories for local web filtering) and feature profiles which make it more effective to mix and match



Scalability

- Different SRX platforms have different performance, thereby allowing customer to select the right platform for their environment based on scale required for each content security features



Collaboration



Delivered via our Integrated Security Services

Orchestration and Management

Security Director
On-Prem

Security Director
Cloud

Mist
Cloud

Juniper
Secure Analytics

Advanced Security Services

AppSecure

Intrusion Detection
& Prevention

Content Security

Anti-Virus

AI-PTP

Advanced Threat
Protection Cloud

SecIntel

IoT Security

DNS Security

Corero DDoS

Enforcement



Branch SRX



Mid-Range SRX



High End SRX



cSRX



vSRX

JUNOS

Next Generation Firewall



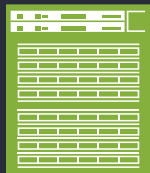
AI-Driven SD-WAN

JUNOS

SD-WAN



NFX Series



EX/QFX Series

JUNOS

Switches



MX Series

JUNOS

Routers

Environments


Data center


VMs


Physical Server


Containers

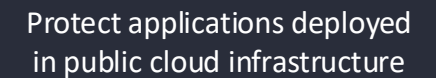

Multi-Cloud


Branch/Campus

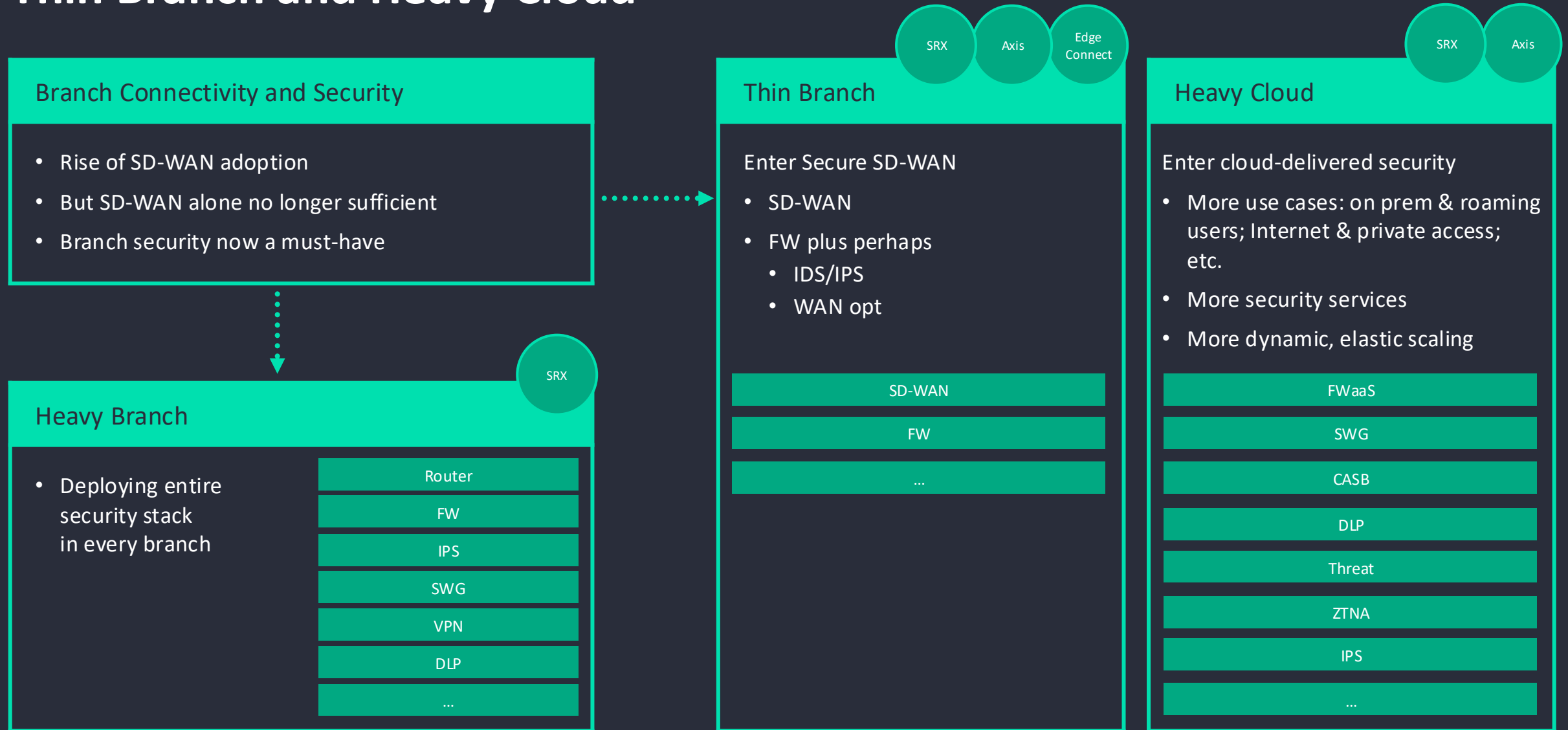

Users

Zero-Trust design principles for the evolving DC

Zero-Trust design principles for the evolving DC

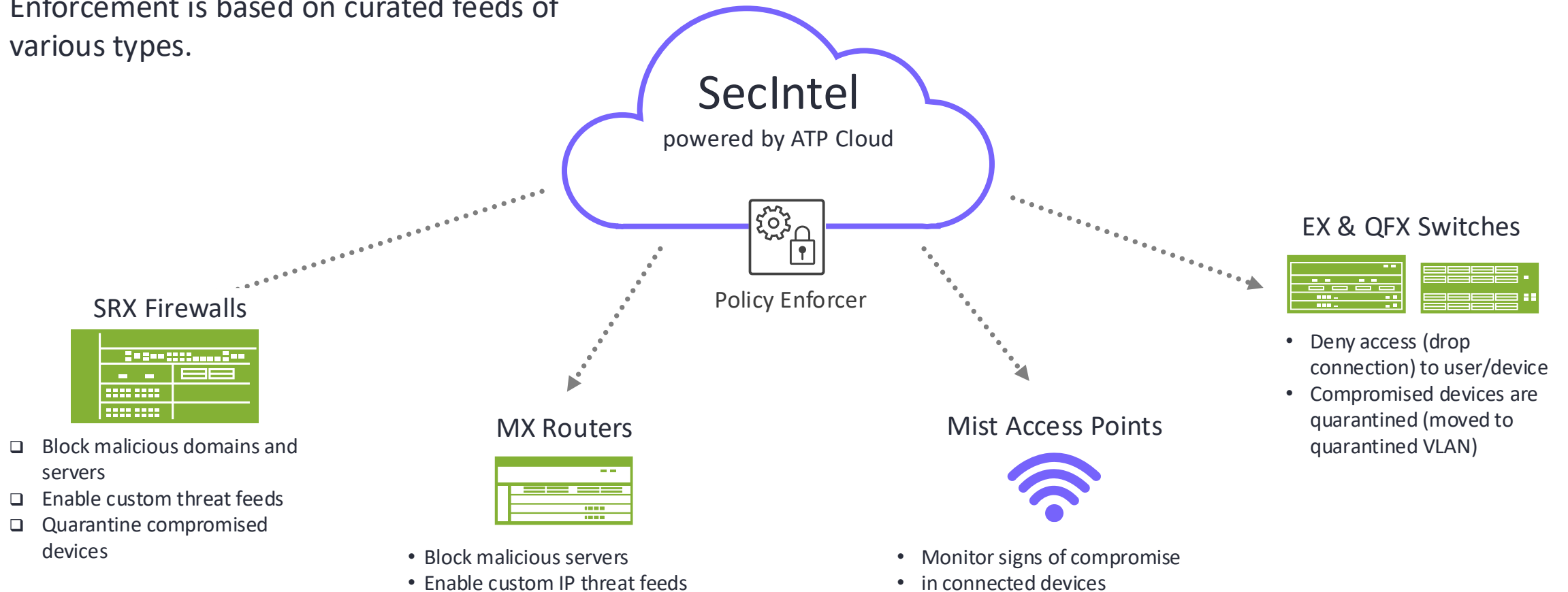


Thin Branch and Heavy Cloud

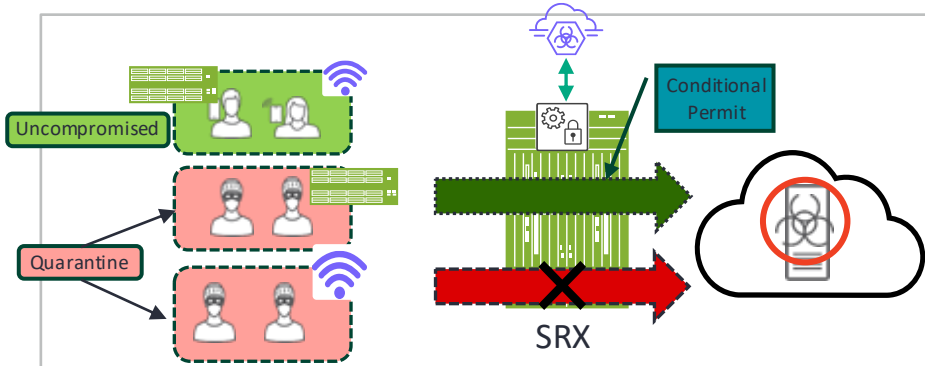


Security Intelligence enables a threat-aware network

- SecIntel extends threat DETECTION & ENFORCEMENT to all points of connection
- Enforcement is based on curated feeds of various types.

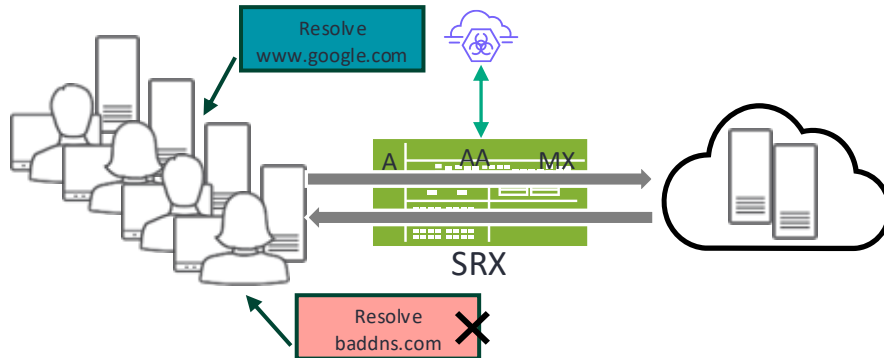


Security Intelligence Use Cases



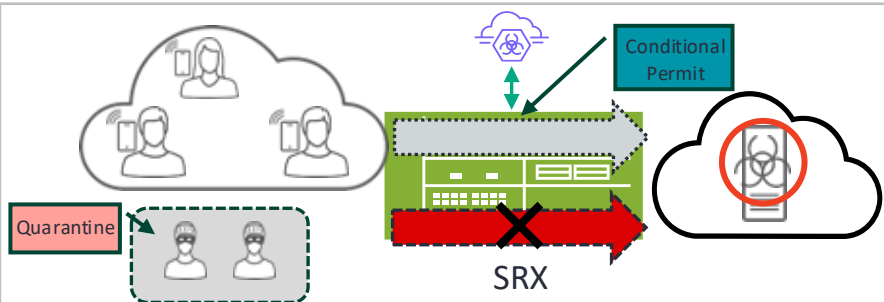
Connected Security

- Protect the infrastructure by quarantining compromised hosts at Switching Infrastructure.
- Integrates with HPE Clearpass and 3rd party tools (Cisco ISE, Carbon Black, Forescout, Pulse Secure etc.) to enforce similar protection where its required (switches, wireless access points)



DNS Server Protection

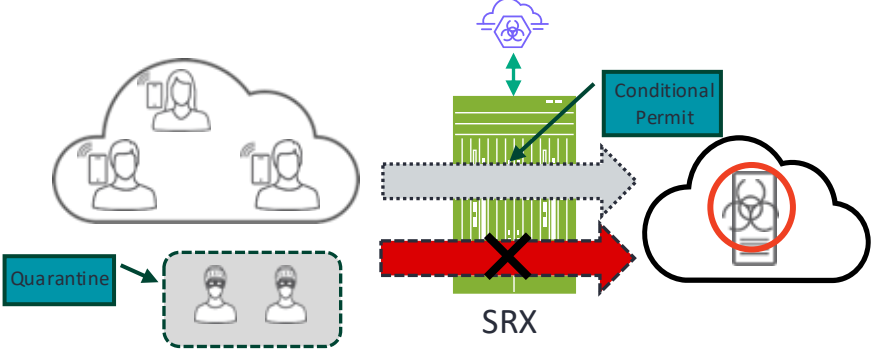
- Protects clients from accessing malicious domains.
- Protects the environment and resources by sinkholing and notifying administrator of compromised hosts.



Threat Protection

- Protects against known threat actors (C&C).
- Administrator controls the risk by deciding the right threat level to monitor, block or permit.
- Ability to quarantine compromised hosts based on the risk verdict.

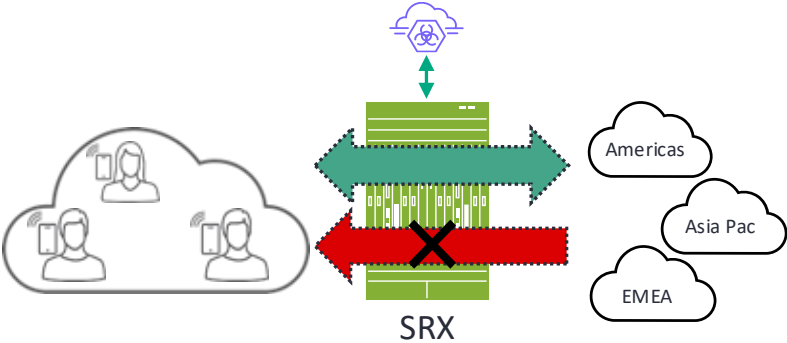
Security Intelligence Use Cases



The diagram shows a cloud on the left containing three user icons. A green arrow labeled 'SRX' points from this cloud to a central green server icon. Above the server is a purple cloud with a biohazard symbol and a double-headed green arrow. A red arrow points from the server to a cloud on the right containing a single user icon with a red circle and a biohazard symbol. A green box labeled 'Quarantine' points to a dashed box containing two user icons. A green box labeled 'Conditional Permit' points to the green arrow. A large red 'X' is placed over the red arrow.

Extend Protection to the Edge

- Protects against known threat actors on the MX Platform leveraging the same C&C feeds that protects the SRX as well
- Administrator controls the risk by deciding the right threat level to monitor, block or permit
- Use of Allowlist and Blocklist provides a better mechanism

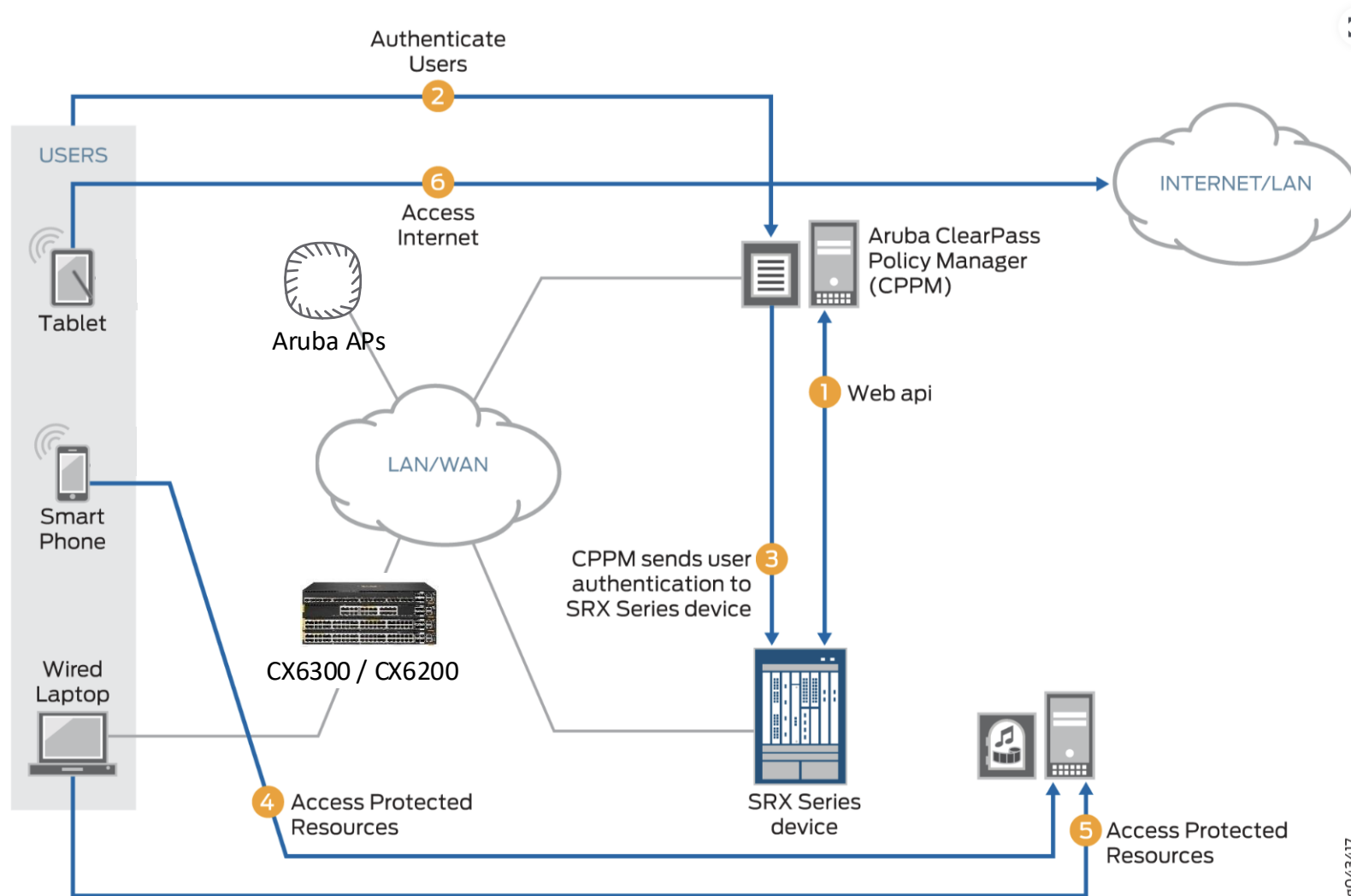


The diagram shows a cloud on the left containing three user icons. A green arrow labeled 'SRX' points from this cloud to a central green server icon. Above the server is a purple cloud with a biohazard symbol and a double-headed green arrow. To the right of the server are three clouds labeled 'Americas', 'Asia Pac', and 'EMEA'. A red arrow points from the server to the 'Americas' cloud. A large red 'X' is placed over the red arrow.

Geo Location Protection

- SecIntel provides Geo Location based feeds (GeoIP feed) that helps administrator create better policy posture by blocking traffic from specific countries
- Geo location feeds provide a way to restrict traffic on emerging attacks for scheduled time duration (e.g. for DDoS attacks from a specific Geo for 2 weeks, ensuring coverage of a particular threat campaign)

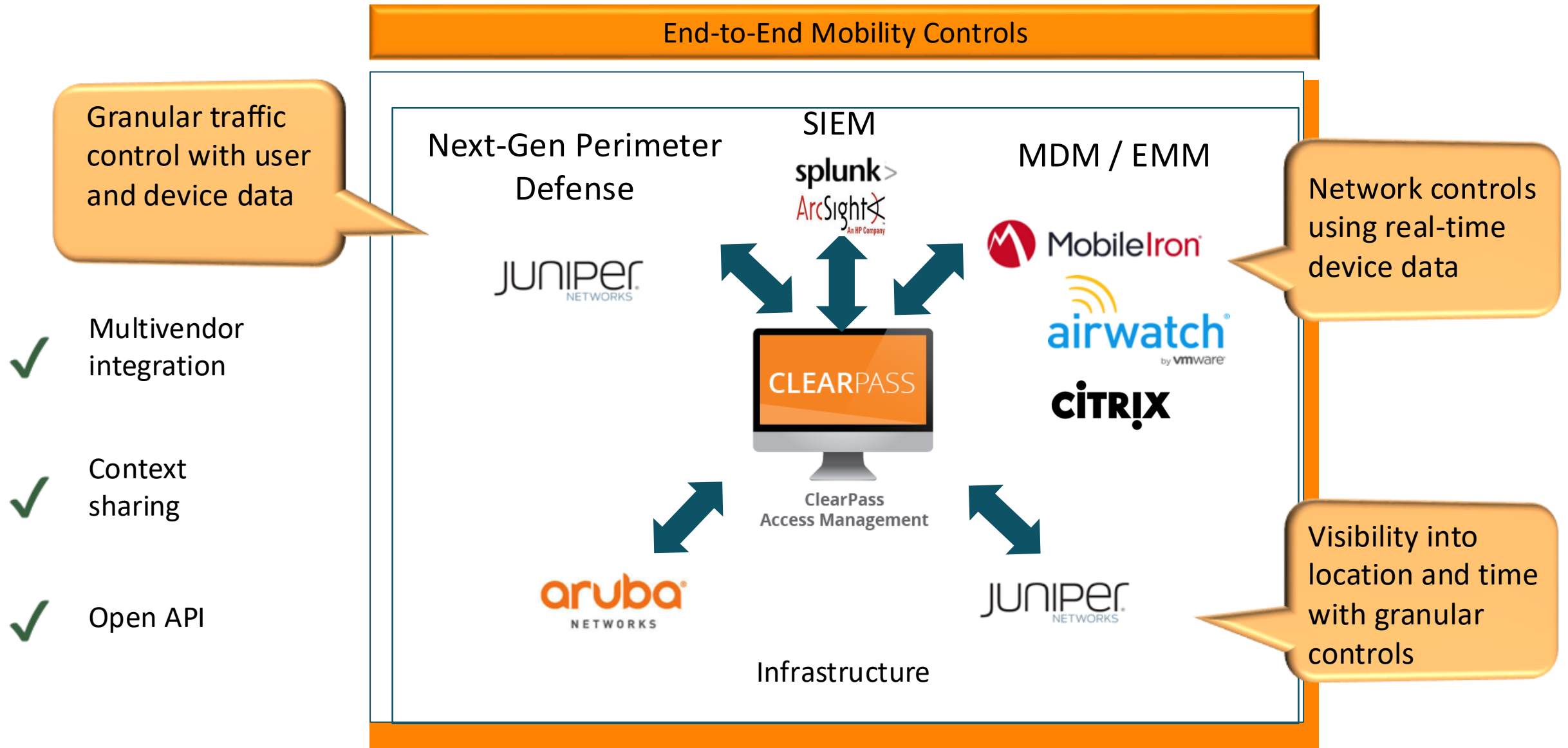
HPE Networking Delivers Comprehensive Threat Prevention from Edge to Data Center



The CPPM sends the **user authentication and identity information** for the users who are logged in to the network to the firewall in **POST request messages** using the **Web API**.

The UserID daemon gets the full IP-user mapping from the CPPM. For each authenticated user, the UserID daemon generates an entry in the Routing Engine authentication table.

Zero Trust for Access



Security Director

Overview, Features and Benefits



Security Management Offerings

On Box Manager

Central Manager

Junos CLI

JWeb



Juniper
Security Director
Cloud



Juniper
Security Director

Operationalize security through a single management & policy experience



sZTP

Juniper
Security Policy Cloud

Demo, New York

2017 > Security Policy > [SSL Policy](#)

Site Policy [®]

Last update: 4 hours ago by gursamy@juniper.net

Total Rules: 150

[Bulk Import](#)
[Set Default Rule Option](#)
[Export All](#)
[Collapse All](#)

	Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions
▼	Global (4 rules)						
	1	denyall	Any	Any	Any	Reject	IPS: ContentSecurity, Denylog Settings: SecureWebProxy Anti-malware: DMZ DXP: Disabled
	2	malwareblock1	Any	Any	Any	Deny	IPS: ContentSecurity, Denylog Settings: SecureWebProxy Anti-malware: DMZ DXP: Disabled
	3	ingress	Any	Any	Any	Deny	IPS: ContentSecurity, Denylog Settings: SecureWebProxy Anti-malware: DMZ DXP: Disabled
	4	blockmaliciousout	Any	Any	Any	Reject	IPS: ContentSecurity, Denylog Settings: SecureWebProxy Anti-malware: DMZ DXP: Disabled

Single Policy Framework

Unbroken Visibility

Rule Analysis

Last refreshed on Dec 16, 2022, 9:58:04 AM

↓

▶

Rule 102 is shadowed by Rule 1

Recommendation 1

Move Rule3 to seq. number 7

Preview

Ignore

Accept

Recommendation 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Preview

Ignore

Accept

Rule 1 is shadowed by Rule2

Rule 1 is shadowed by Rule2

Rule 4 ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore.

Security Assurance



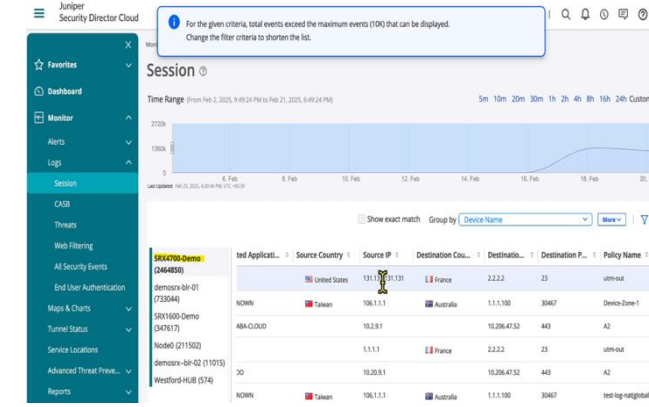
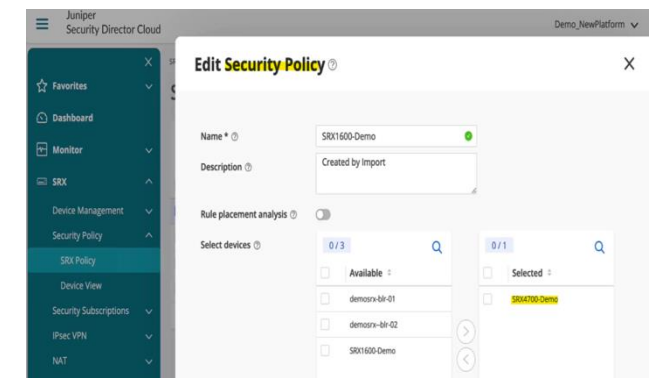
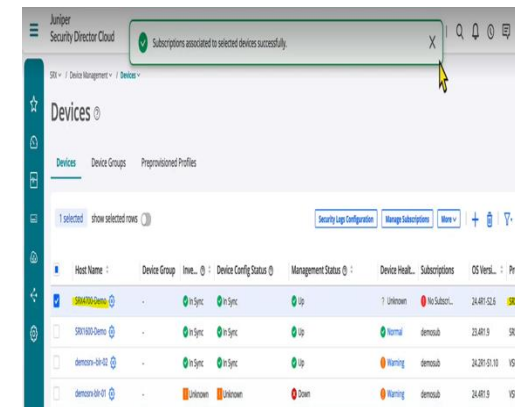
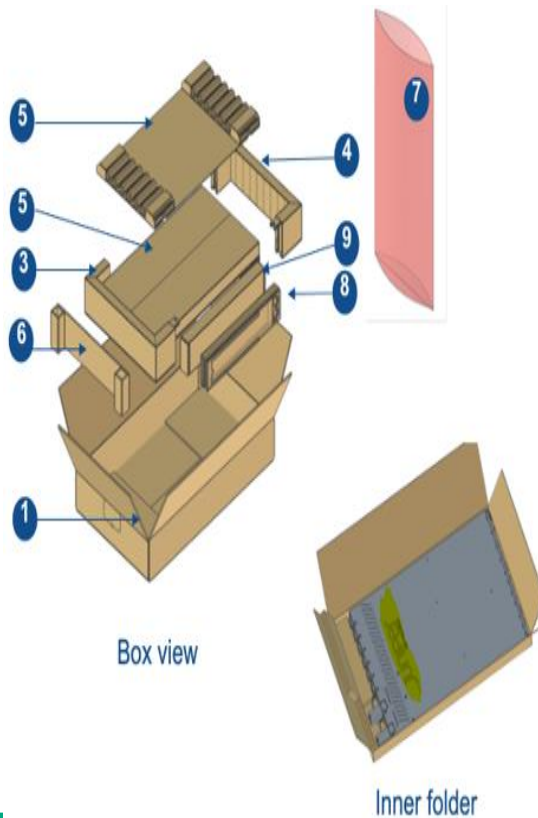
UnBoxing to Securing Your Network: sZTP

UnBox

Rack and Stack

Secure ZTP

Secure your
Network



Day 0 & Day 1 Configuration Support

Discover & Manage Device in your network

❑ **SRX Device Specific Day 0 & Day 1 Configurations**

- ✓ Security Admin can do non-security configurations in SRX via SD user interface

SRX / Device Management / Devices

demo-srx-blr

Deploy pending. Last Deployed: Never

OverviewChassisInterfacesDevice AdministrationConfiguration TemplatesDevice Configurations

Basic SettingsNetwork SettingsSecurity SettingsAdvanced Settings

Interfaces

Static RoutesPolicy OptionsBGP> OSPF> RIPForwarding OptionsRouting Instances

Interfaces

Interface

	Name	Native Vlan Id	Speed	Mtu
☐	ge-0/0/0			
☐	ge-0/0/1			
☐	ge-0/0/2			
☐	ge-0/0/3			
☐	st0			

5 items

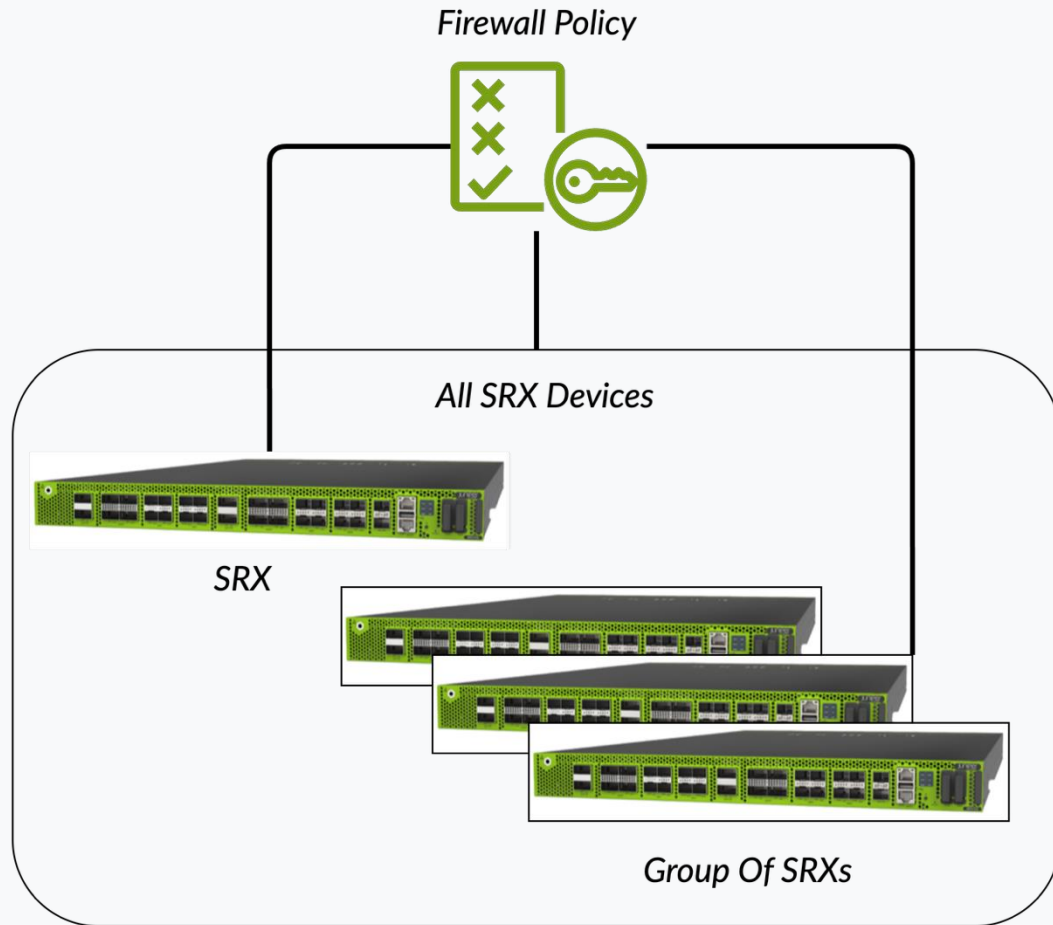
Interface Range

More +

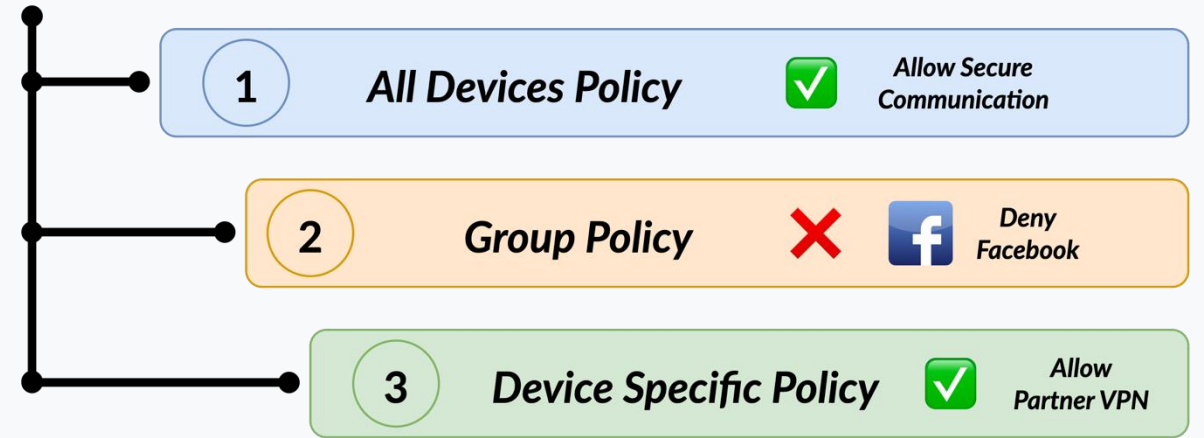
CancelSave

Simplified Policy Management

Policy Management



Policy Hierarchy



Unified Policy Management

Juniper Security Director Cloud

HPE-Juniper-Demo | Search | Notifications | Clock | Chat | Help | User A

SRX / Security Policy / SRX Policy

paris-fw1 ?

Last update: 3 days ago by phattiangadi@juniper.net | Total Rules **519** | Redeploy required | **Deploy**

1 selected

	Seq	Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
☒	1 0 hits	paris-fw1-1 Description	+ Sources	+ Destinations Destinations	+ Applications/Services	- Deny		Schedule (Optional) Session initiate logs ☐ Session close logs ☐ Log count ☐ Rule options ☐

▼ ZONE (518 Rules)

☐	1 0 hits	gavin-demo Gavin Rule to show SRX policy creatio...	guest 10.10.0.103 +3	lsg-vpn Any	LINKEDIN-POST +3 https	Permit	IPS Content Security Decrypt SecIntel Secure Web Proxy Anti-malware FBAV ICAP Redirect	
--------------------------	-------------	--	-------------------------	----------------	---------------------------	--------	---	--

Page 10 of 10

Page 10 of 10

Firewall Rule Optimization

The screenshot displays the Juniper Security Director Cloud interface for 'Policy_1'. The main area shows a table of firewall rules. A 'Rule Analysis' sidebar is open on the right, showing recommendations for rule optimization. Numbered callouts highlight specific features:

- 1**: Left sidebar navigation.
- 2**: Rule list table.
- 3**: Rule Analysis sidebar.
- 4**: 'Rule Analysis' button in the top toolbar.

A callout box points to the rule list table with the text: "Collapse rules in case the highlighted rule is below the fold."

Seq.	Rule Name	Sources	Destinations	Applications/Services	Action	Security Subscriptions	Options
1	Default	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
2	rule1	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
3	rule2	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
4	rule3	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
95 rules							
100	rule4	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
101	rule5	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
102	rule102	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
103	rule7	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	
104	rule8	Any	Any	a1 +2 s1	✓	IPS, Decrypt, Content Security	

Innovation from Juniper

Rule with anomaly is highlighted

Anomaly comparison without scrolling

Easy to accept or ignore suggested fix

Anomaly status

Firewall Rule Analysis: Report

Juniper
Security Director Cloud

Monitor / Reports / Report Definitions

Report Definitions

Name

Description

mdine-url-report

url report

IPS

IPS Test Report

URLs

Test URLs-per-user

SunnyvaleRuleAnalysis

SunnyvaleRuleAnalysis

ThreatAssessmentReport

ThreatAssessmentRepo

ApplicationUsageReport

ApplicationUsageRepo

testunisuper

Test_purpose

saQQQQ

ASfdaaFW

ips-report

for Ops team

security-events-report

for Ops team

TestReport11

Test report to demons

ThreatReportJuly

Threat report for July 1

CourtneysReport

UX Test Report

SER1

SER1

aaa

aaa

ThreatReportGD

Threat Report

Create Rule Analysis Report Definition

General

Report Name *
Rule Analysis Report Definition

Description *

Content

Anomalies *

Shadowed

Redundant

Expired scheduler

Logging disabled

Unused Rules

Security Policies *

Name	Description
site-policies	Created by Import
Host-171	Created by Import
test-id	
Sunnyvale	Created by Import
50 items	

Schedule

Report Schedule
Specify whether you want to run job immediately or schedule it for a later time

Run Now

Create

More

Last Generated

Job ID

12/14/2023, 11:53:46 PM

ebaff8cc-0130-4a4...

12/12/2023, 11:38:21 PM

594166f2-8eab-4e...

12/12/2023, 11:28:57 PM

099e5f27-4687-447...

11/13/2023, 11:17:39 AM

e7a00233-289f-40...

11/13/2023, 10:05:22 AM

9f93c67-7fbb-41e4...

11/13/2023, 10:02:36 AM

9aae027b-fdbd-46...

10/26/2023, 9:24:23 AM

3d11c9de-6554-48...

11/13/2023, 10:13:39 AM

3ea7ef42-447d-4af...

9/13/2023, 11:32:56 PM

5810487c-8c22-44...

9/8/2023, 12:58:04 AM

aa100d06-a165-46...

11/18/2023, 12:09:49 AM

a44ea44d-c43e-4e...

9/8/2023, 1:04:40 AM

9fae00a1-b03e-47...

6/20/2023, 10:23:20 AM

009b1cc6-997b-43...

6/15/2023, 6:56:28 PM

032c3e08-1b51-49...

11/18/2023, 12:08:16 AM

b13ae6a4-45c1-48...

Rule Analysis Report - Sunnyvale

REDUNDANT

A rule is redundant if there exists some preceding rule within the policy which performs the same action on the same packets as performed by the current rule. Removing redundant rules can increase performance by reducing rule comparisons.

No	Name	Sources	Destinations	Applications/Services	Action
Problem: Rule 26 (R1_oob_1), Rule 27 (R1_oob_2) are redundant with Rule 25 (trust-to-untrust2)					
Recommendation: Delete Rule 26 (R1_oob_1), Rule 27 (R1_oob_2)					
25	trust-to-untrust 2	trust Any	untrust Any	any defaults	PERMIT
26	R1_oob_1	trust Any	untrust Any	any defaults	PERMIT
27	R1_oob_2	trust Any	untrust Any	any defaults	PERMIT

No	Name	Sources	Destinations	Applications/Services	Action
Problem: Rule 27 (R1_oob_2) is redundant with Rule 26 (R1_oob_1)					
Recommendation: Delete Rule 27 (R1_oob_2)					
26	R1_oob_1	trust Any	untrust Any	any defaults	PERMIT
27	R1_oob_2	trust Any	untrust Any	any defaults	PERMIT

Bringing it all together

Data Center Next-Generation Firewall Use Case—Juniper Validated Design (JVD) | Juniper Networks



jn-000855

SRX Form Factors



**Modular Form Factor Firewalls
(SRX5000 Series)**



Fixed Form Factor Firewalls



Software based Firewalls

SRX Series Firewall

Branch Firewalls

SRX300/
SRX320
KMD 1RU

SRX340/
SRX345
KMD 1RU

SRX380
KMD 1RU

4FW (Fixed Form Factor Firewall) + Virtual & Containerized

Security micro-
services

cSRX
(20vCPU + 48G)

vSRX
(17vCPU + 32G)

SRX1600
IKED 1RU

SRX4120#
IKED 1RU

SRX4200
KMD + IKED 1RU

SRX4300
KMD + IKED 1RU

SRX4600
KMD + IKED 1RU

SRX4700
IKED 1RU

Modular Firewall

SRX5400X
KMD + IKED 5RU

SRX5600X
KMD + IKED 8RU

SRX5800X
KMD + IKED 16RU

Advanced Security Acceleration
(SPC3)

earlier was called SRX2300

SRX4700

Fastest 1U FW in the World



SRX is #1 in every test for over 5 years

HPE Networking Threat Labs

Independently validated security efficacy

NetSecOPEN
2022

99.8%

effectiveness against exploits

NSS Labs / Cyber Ratings
2024 Cloud Network Firewall

99.7%

against client & server-side exploits

NSS Labs \ Cyber Ratings
2025 Enterprise Firewall

99.16%

Exploit block rate

PQC Intro

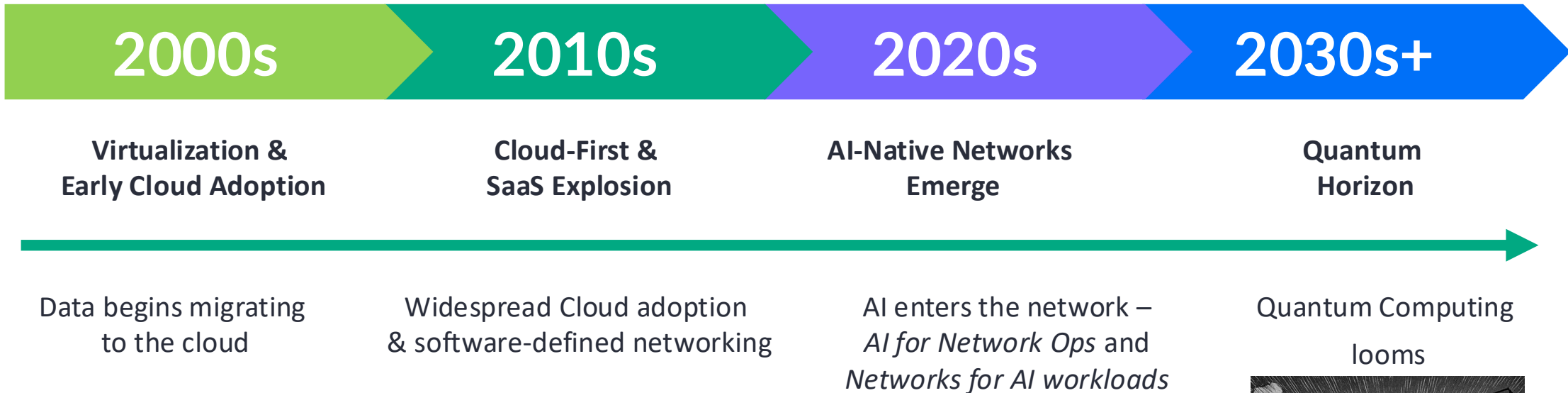


Post-Quantum Cryptography (PQC)



Evolution of Networking Infrastructure

Waves of Technology Shifts



The Challenge

Shor's Algorithm can break RSA and ECC public key crypto

Grover's Algorithm halves the security of symmetric keys, requiring larger key sizes

Harvest Now, Decrypt Later means collecting encrypted data now to decrypt in the future



21

Quantum Computers running Shor's algorithm have only managed to factor numbers as large as 21 so far

State of NIST Standards as of March 2026

Replace current algorithms - RSA, ECDSA, Diffie-Hellman (DH), Elliptic Curve Diffie-Hellman (ECDH)

Old Name	New Name	Branch	Status
Kyber	ML-KEM (FIPS 203) Module-lattice based key-encapsulation mechanism standard	Lattice-based	Published Aug 2024
Dilithium	ML-DSA (FIPS 204) Module-lattice based digital signature standard	Lattice-based	Published Aug 2024
SPHINCS ⁺	SLH-DSA (FIPS 205) Stateless hash-based digital signature standard	Hash-based	Published Aug 2024
Falcon	FN-DSA (Proposed as FIPS 206) FFT over NTRU lattices digital signature standard	Lattice-based	To be released in 2026
HQC (Hamming Quasi-Cyclic)	Backup for ML-KEM (Possibly FIPS 207) Error-correcting codes concept	Codes-based	To be released in 2027

Three Bit Strengths of ML-KEM and ML-DSA

Level	ML-KEM Variant	Classical Equivalent	Comparable to	ML-DSA Variant
Low	ML-KEM-512	~128-bit security	AES-128	ML-DSA-44
Medium	ML-KEM-768	~192-bit security	AES-192	ML-DSA-65
High	ML-KEM-1024	~256-bit security	AES-256	ML-DSA-87

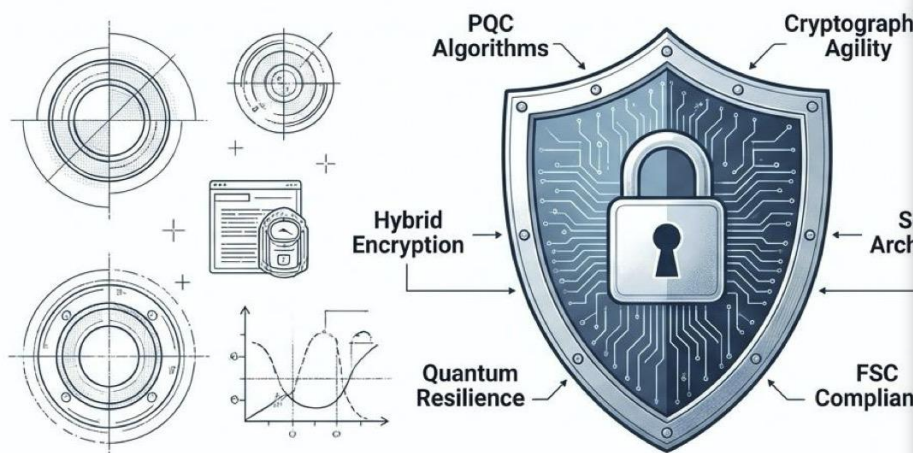


台灣現況

2026/04 數發部

2026/06 金管會

金融業後量子密碼(PQC)遷



金融監督管理委員會
2026年6月

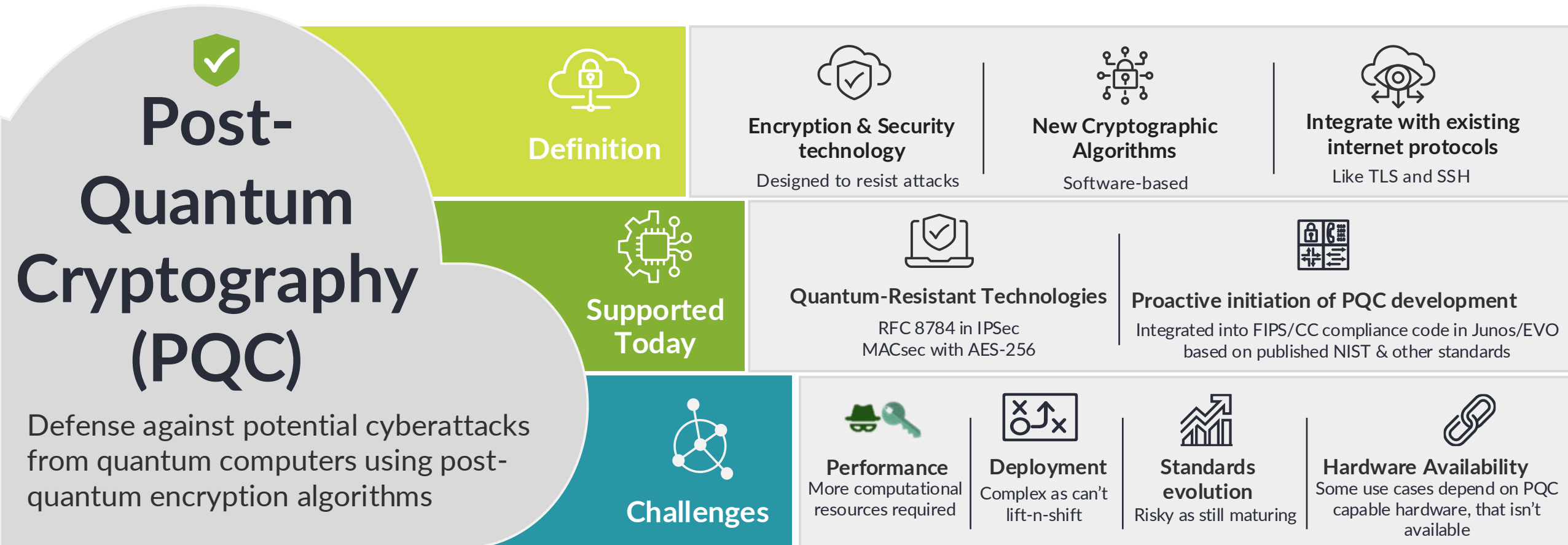


金融業後量子密碼遷移參考指引

金融監督管理委員會

中華民國 115 年 6 月

PQC and Quantum-Resistant Technologies



PQC is a Journey

Available Today

QUANTUM-RESISTANT APPROACHES

- RFC 8784 in IPsec
- MACsec when implemented with AES-256

2025-2026

DELIVER FOUNDATIONAL CHANGES TO JUNOS/EVO

Data encryption and digital signing software with PQC, based on standardized NIST algorithms (ML-KEM, ML-DSA, and so on)

2026-2028

INTEGRATE PLATFORM SPECIFIC & TRACK OTHER GOVT REQUIREMENTS

- Incorporate platform-specific **protocols and applications** changes (e.g. TLS proxy, SSH)
- Plan & **track requirements** from other Govts & Common Criteria

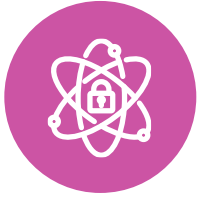
2028-2030

PURSUIT FOR CERTIFICATIONS

Compliance verification and validation for FIPS/CC and additional security certifications

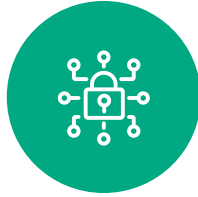


Quantum-Resistant Networks: Key Takeaways for PQC



Quantum Threat is Real, but not immediate

Universal quantum computers remain years away, but proactive preparation is essential



Post-Quantum Cryptography (PQC) is the Foundation

NIST-standardized algorithms are being integrated into HPE's platforms



Hybrid Approaches Recommended

RFC 8784 (IPsec) and MACsec with AES-256 provide quantum-resistant options available today



HPE Networking's PQC Roadmap

Quantum Buffer (crypto-agility), PQC-enabled image signing, updated crypto libraries, and protocol & application upgrades rolling out through 2026 and beyond



Challenges & Next Steps

Standards evolution, Hardware availability, and interoperability remain hurdles

Thank You

