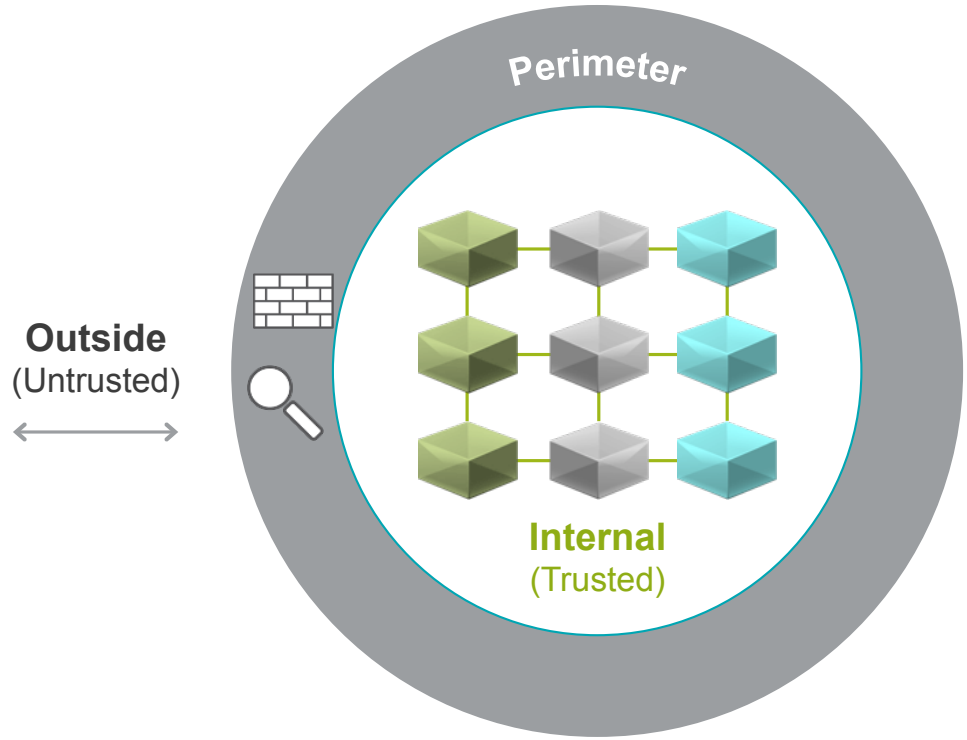
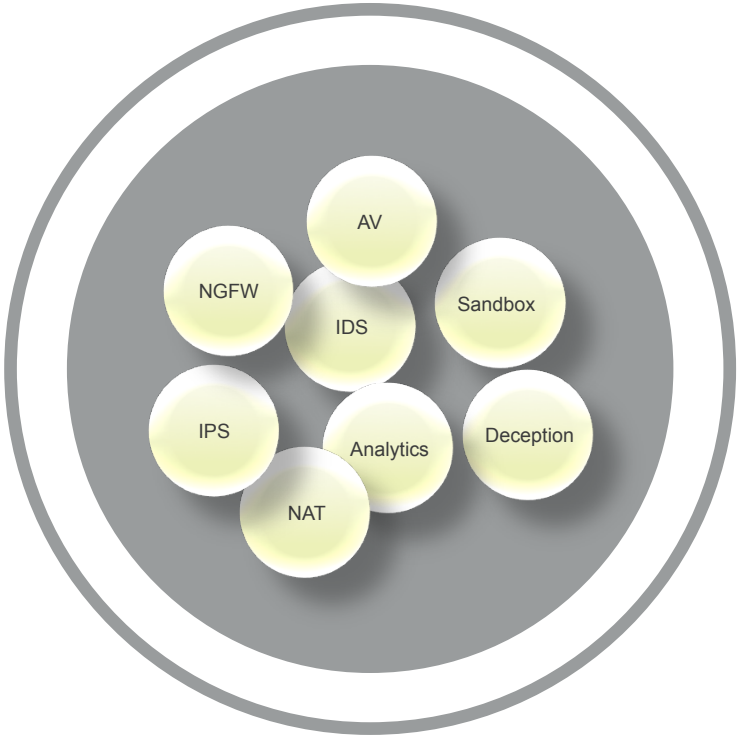

L'AUTOMAZIONE COME SUPPORTO ALLA LOTTA ALLE NUOVE MINACCE DI RETE
Damiano Colla – Regional Security System Engineer
Juniper NETWORKS
Engineering Simplicity

PERIMETER ORIENTED SECURITY



- Hyper-connected Network Security at Perimeter
- Lateral Threat Propagation
- Limited Threat Visibility

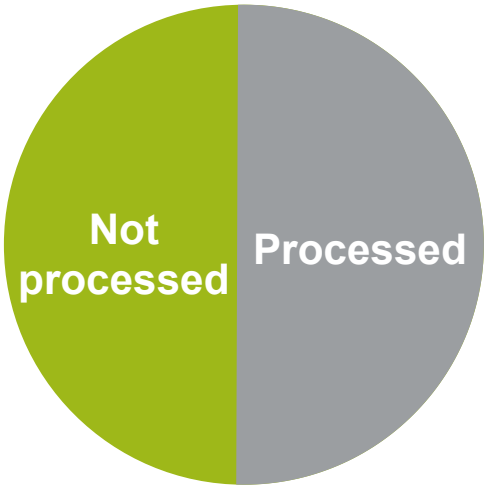
UNCOORDINATED THREAT INTELLIGENCE



- Too many security appliances
- Many different threat scores
- Manual coordination

ALERT OVERLOAD

- 75% of alerts are false positives (73% respondents)[2]
- Most receive over 1000 malware alerts per week (74% respondents)[2]
- Most only process 500 malware alerts per week (67% respondents)[2]



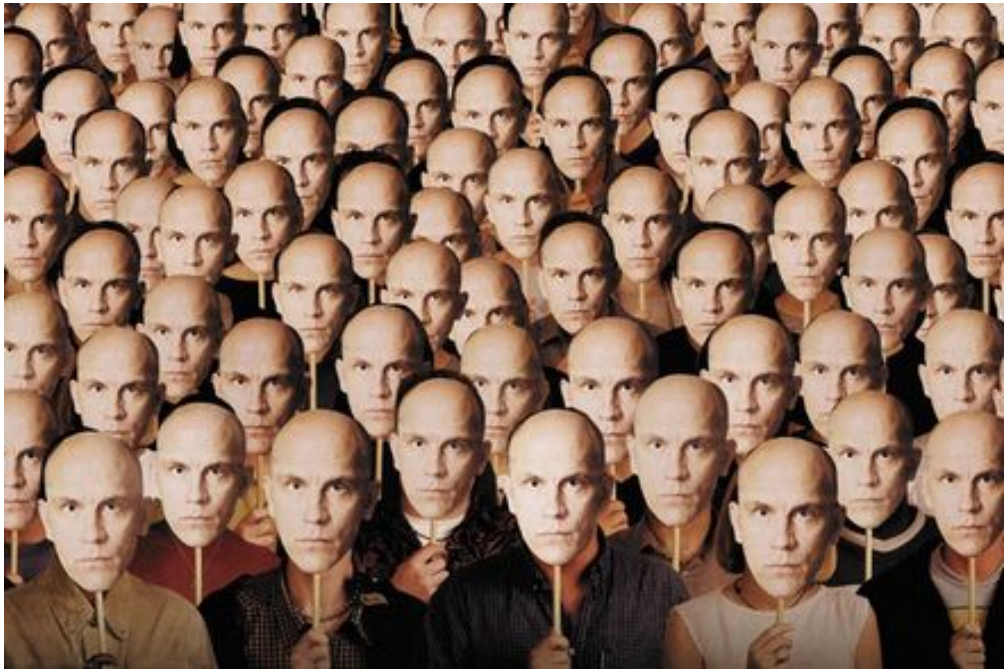
[2] Reducing Cybersecurity Costs & Risks Through Automation Technologies, November 2017

"As a result, they are also suffering from alert fatigue and multiple console complexity and facing the challenges in recruiting and retaining security operations analysts with the right set of skills and expertise to effectively use all those tools. This is all playing against a backdrop a growing attack surface that is no longer restricted to on-premises IT environments." – Gartner, Inc.

COME IL MANAGEMENT VEDE LA SECURITY…

Security Team *vs* *Hackers*

…E COM'È VERAMENTE



L'automazione nel cyber-crime è una realtà fatta di: malware, attacchi, etc.

WE NEED SECURITY INTELLIGENCE
ANALYSIS BEYOND THE TIP OF DATA ICEBERG

Collection

- Log collection
- Signature-based detection

+

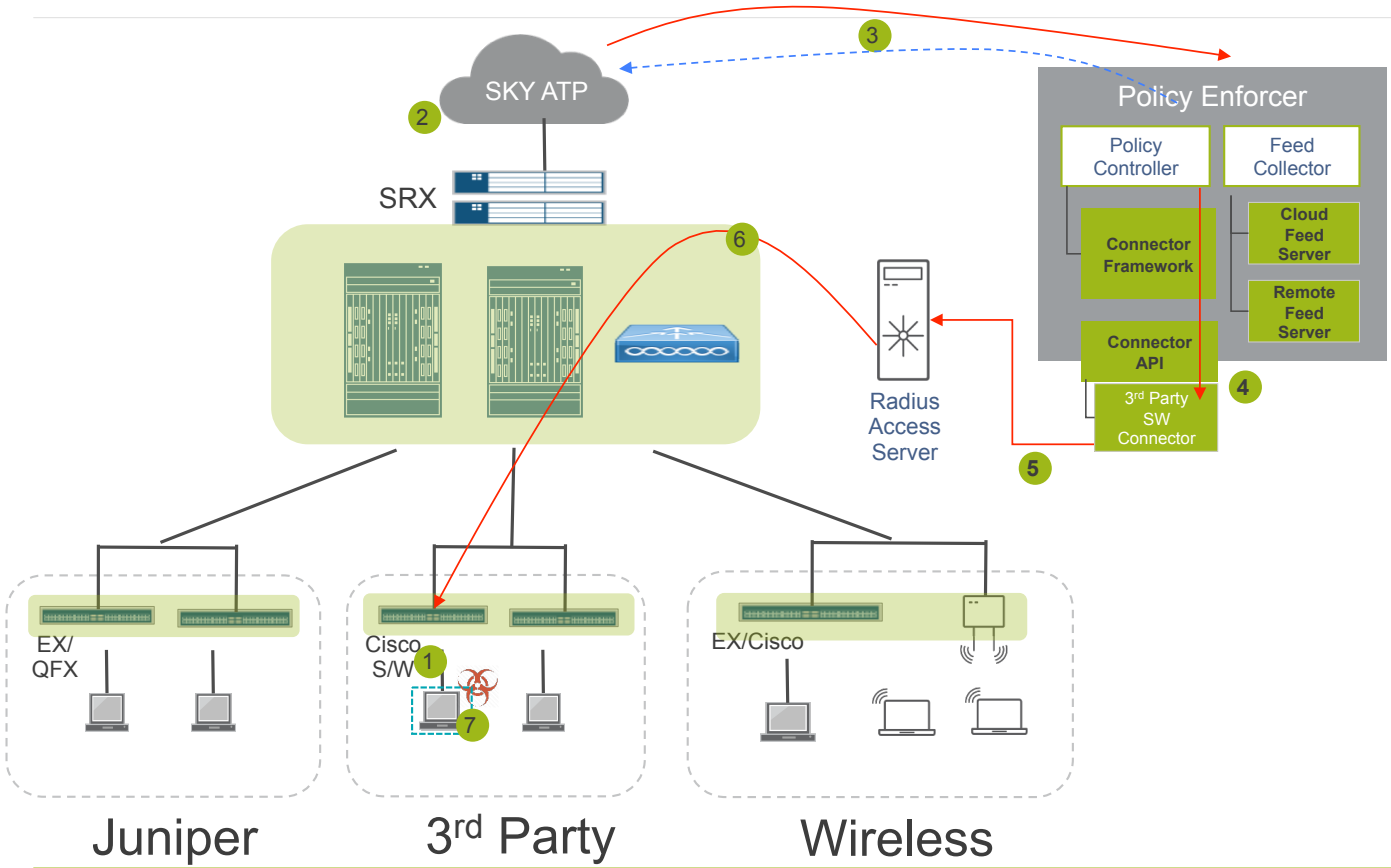
Security Intelligence

- Real-time monitoring
- Context-aware anomaly detection
- Automated correlation and analytics

THE POWER OF UNITY

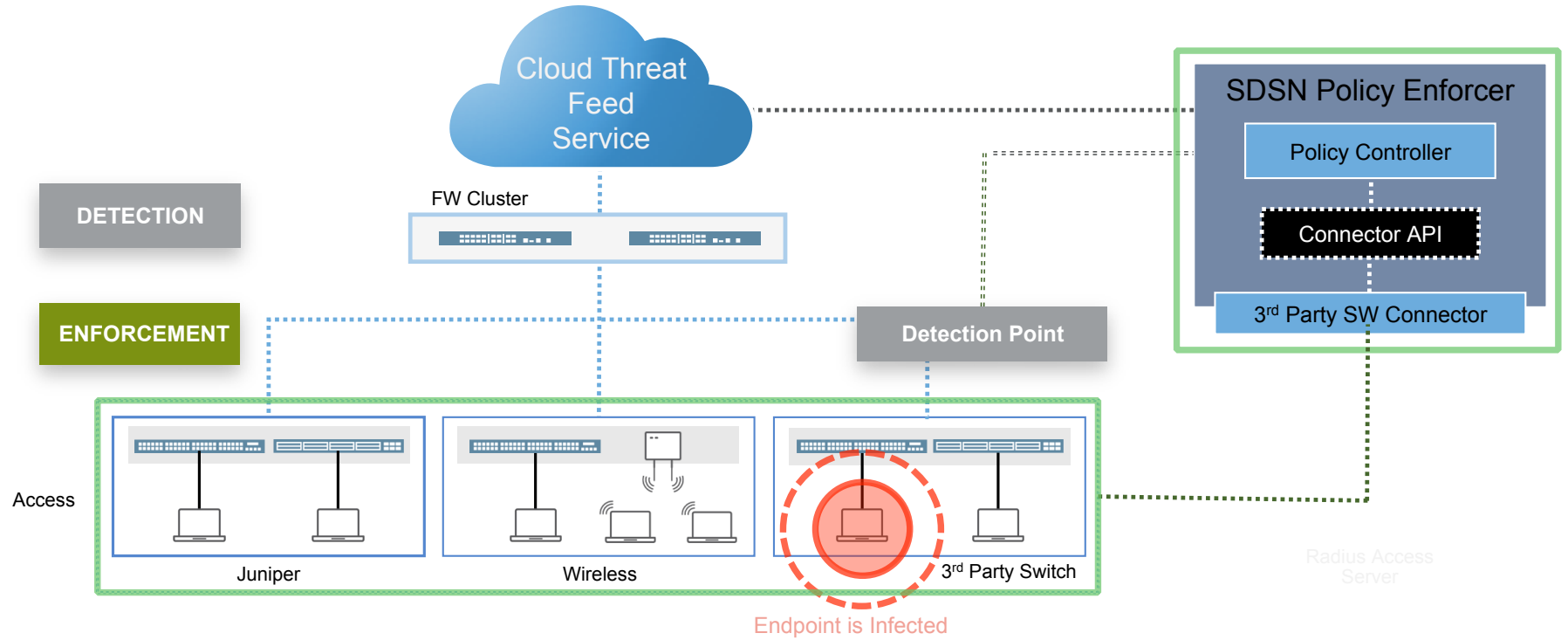
*Increased **Protection** for Customers*

SDSN IN A NON JUNIPER SWITCHED NETWORK



1. End user authenticates to network via 802.1x or mac authentication
2. Sky detects End Point getting the infected
3. Policy Enforcer downloads the Infected Host Feed.
4. PE enforces the Infected Host policy with the 3rd Party SW Connector calling the generic API
5. 3rd Party Connector
   - queries AAA Server for Endpoint details for Infected Host IP
   - initiates CoA for the Infected Host mac.
6. CoA action could be block or quarantine vlan.
7. Enforcement happens on the NAC device End Point authenticated on.
8. Policy enforcer Communicated the end host details back to sky

SOFTWARE-DEFINED SECURE NETWORK IN ACTION



Continuous visibility and control of compromised hosts, preventing laterally spread threats

GRAZIE

Juniper Networks | Engineering Simplicity

MEMBER OF CYBER THREAT ALLIANCE (CTA)

Shared Intelligence for Better Security

What data intelligence is currently being shared?

- Approximately 40,000 STIX™ packages per day, averaging over 300,000 points
- Packages include a range of observables and TTPs across the kill chain
- Observables include: files, Uniform Resource Identifiers (URIs), domain names, and addresses
- TTPs: Over 50 TTPs from Mitre's Common Attack Pattern Enumeration and Classification (CAPEC™) and Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)

CYBER THREAT ALLIANCE

Shared threat intelligence – increased protection for customers

Available April 2018

CHANGE IN MINDSET

Check Point Software Technologies	Cisco	Fortinet	IntSights
Juniper Networks	McAfee	NTT Security	Palo Alto Networks
Radware	Rapid7	ReversingLabs	Saint Security
SK Infosec	Sophos	Symantec	Telefonica's ElevenPaths

All CTA members, regardless of category, are required to meet our minimum sharing requirements and have equal access to the CTA platform and shared intelligence.