Automatizált, testreszabott és biztonságos hálózatok - esettanulmány

Nemes László

Vezető presales mérnök

nemes.laszlo@euroone.hu

EURO ONE Számítástechnikai Zrt.

Bevezető

- A legújabb technológiai kihívás a IT hálózati biztonság területén: az idő faktor.

Mennyi időre van szükség …

- Az eddig ismeretlen támadás felismerésére, beazonosítására?
- A következmények elhárítására, mérséklésére?
- A sérülékenység kiküszöbölésére?
- A teljes védettség megteremtésére?

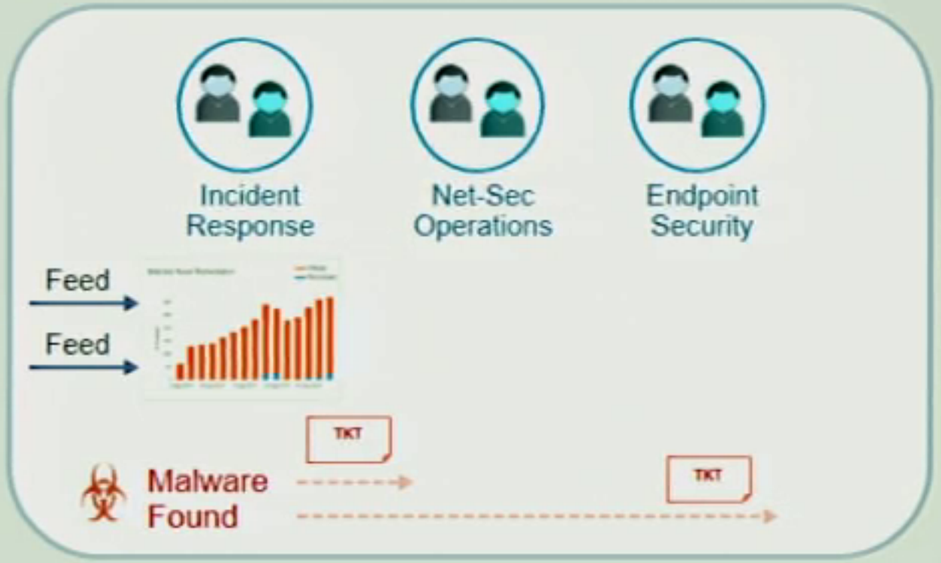
Esettanulmány:

- A Juniper Networks által felállított koncepció és annak megvalósításáról az ismeretlen rosszindulatú programkódokkal (malware) szembeni védekezésről – gyakorlatilag valós időben.


JUNIPER
NETWORKS
Software Defined
Secure Network
(SDNS)

Threat Remediation

Manual Threat Workflows



Multiple Teams

Threat Detection → Enforcement Delays

Vendor specific threat feeds

Threat Remediation

Manual Threat Workflows

Auto Threat Remediation

- Multiple Teams
- Threat Detection → Enforcement Delays
- Vendor specific threat feeds

- Cohesive Threat Management System
- Automation across Network & Security
- Open API and 3rd Party Threat Feed Collation

Software Defined Secure Networks (SDSN) Unified Security Platform

Detection

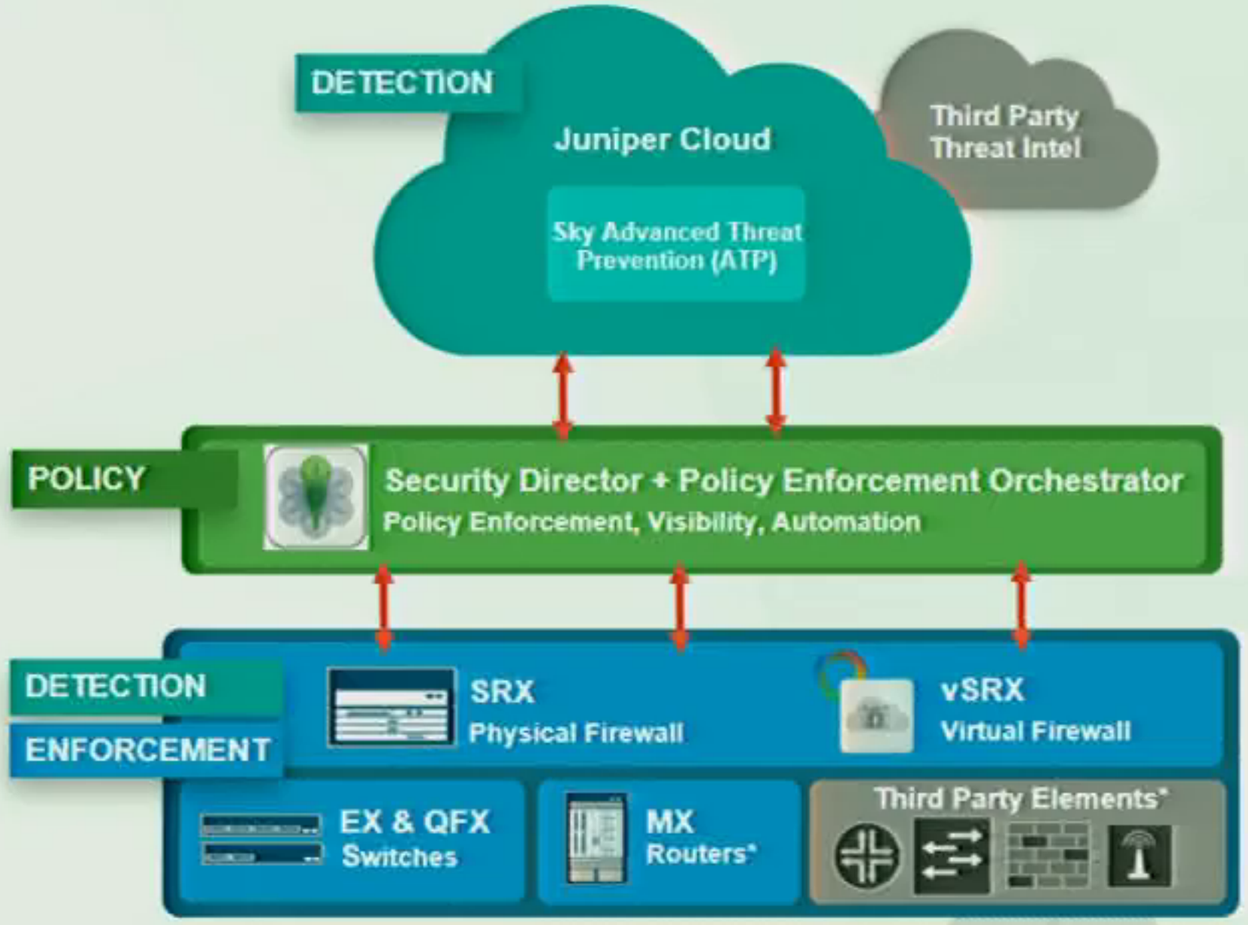
- Fast, effective protection from advanced threats
- Integrated threat intelligence

Policy

- Adaptive enforcement to firewalls, switches, 3rd party devices and routers
- Robust visibility and management

Enforcement

- Consistent protection across physical/virtual
- Open and programmable environment



Software Defined Secure Networks (SDSN) Unified Security Platform

Detection

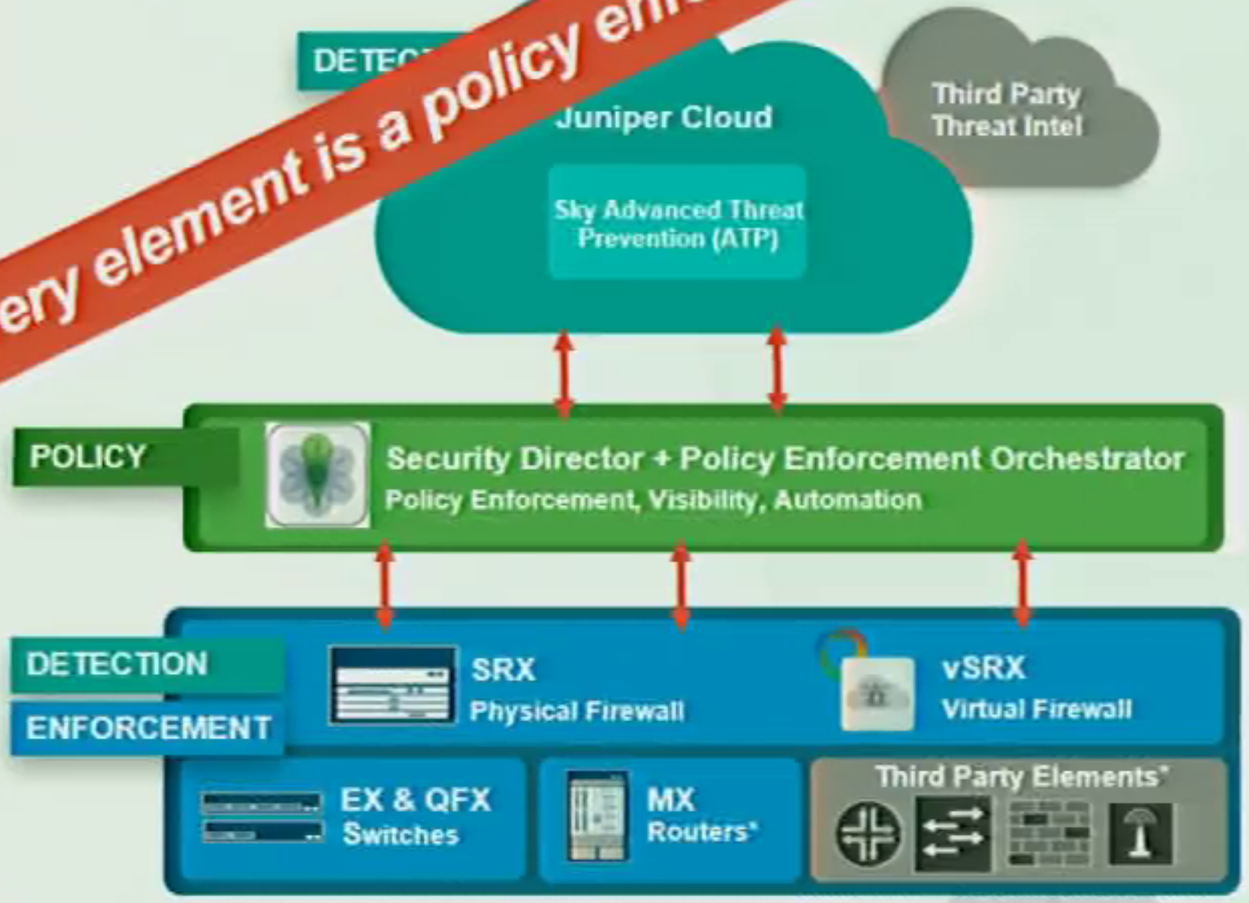
- Fast, effective protection from advanced threats
- Integrated threat intelligence

Policy

- Adaptive enforcement to firewalls, 3rd party devices and routers
- Robust visibility and m… …nt

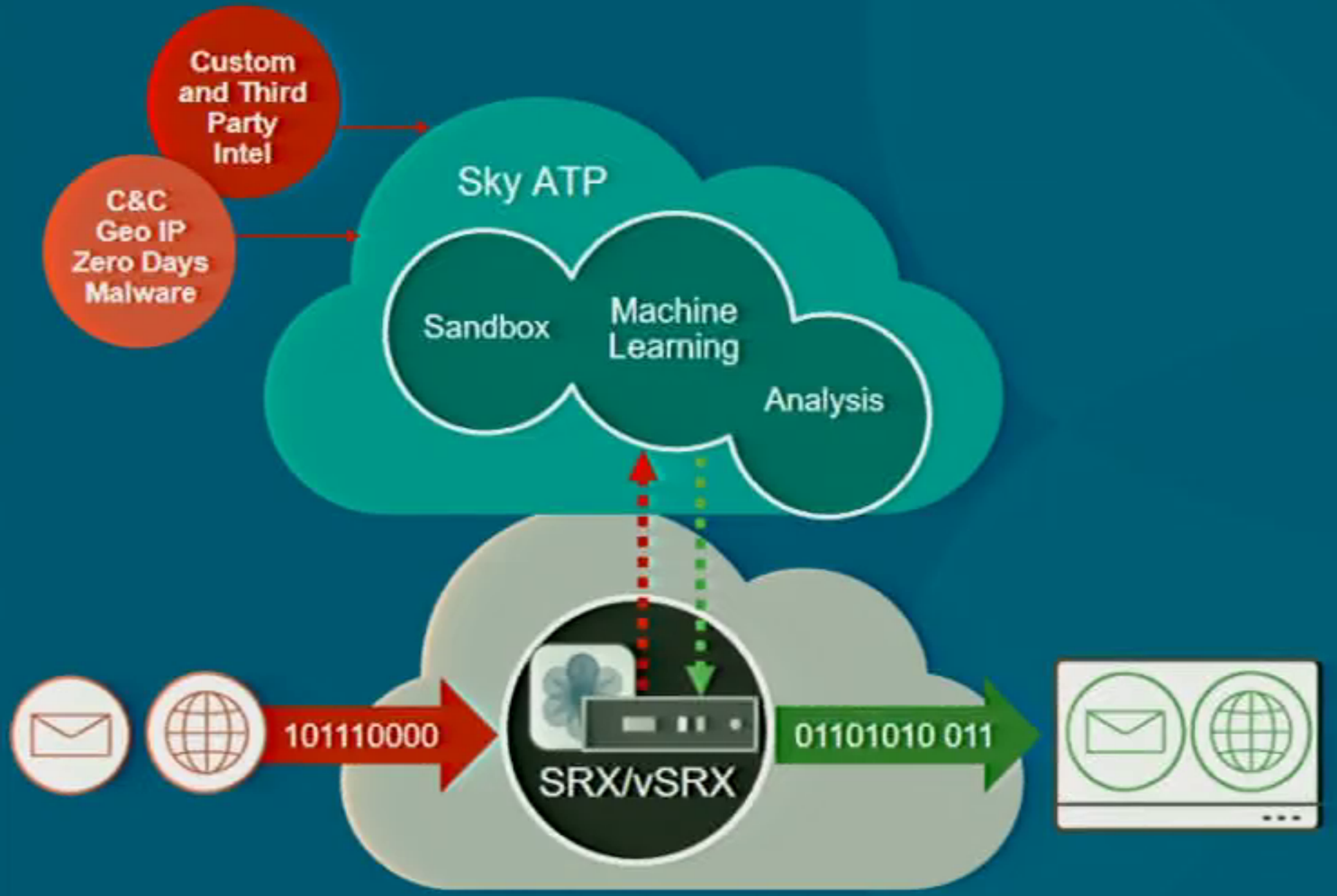
Enforcem…

- C… protection across physical/virtual …and programmable environment



Network as a single enforcement domain - Every element is a policy enforcement point

Sky Advanced Threat Prevention (ATP)



- Protects against advanced malware like ransomware
- Stops advanced persistent threats
- Sophisticated deception techniques to expose evasive malware
- Key component of the Software Defined Secure Networks (SDSN) platform

The Sky ATP Verdict Chain

Staged analysis: combining rapid response and deep analysis

Suspect file

Suspect files enter the analysis chain in the cloud

The Sky ATP Verdict Chain

Staged analysis: combining rapid response and deep analysis

Suspect files enter the analysis chain in the cloud

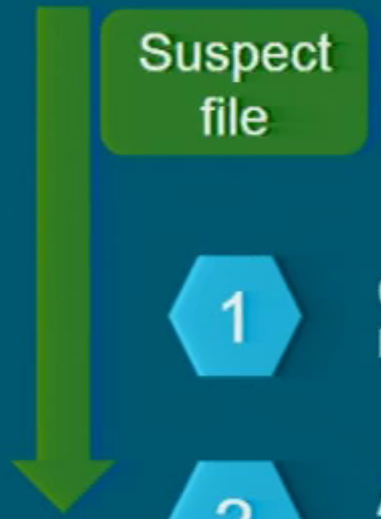
1

Cache lookup: (~1 second)

Files we've seen before are identified and a verdict immediately goes back to SRX

The Sky ATP Verdict Chain

Staged analysis: combining rapid response and deep analysis



Suspect files enter the analysis chain in the cloud

1

Cache lookup: (~1 second)
Files we've seen before are identified and a verdict immediately goes back to SRX

2

Anti-virus scanning: (~5 second)
Multiple AV engines to return a verdict, which is then cached for future reference

The Sky ATP Verdict Chain

Staged analysis: combining rapid response and deep analysis

Suspect file

Suspect files enter the analysis chain in the cloud

1

Cache lookup: (~1 second)
Files we've seen before are identified and a verdict immediately goes back to SRX

2

Anti-virus scanning: (~5 second)
Multiple AV engines to return a verdict, which is then cached for future reference

3

Static analysis: (~30 second)
The static analysis engine does a deeper inspection, with the verdict again cached for future reference

The Sky ATP Verdict Chain

Staged analysis: combining rapid response and deep analysis

Suspect file

Suspect files enter the analysis chain in the cloud

1

Cache lookup: (~1 second)
Files we've seen before are identified and a verdict immediately goes back to SRX

2

Anti-virus scanning: (~5 second)
Multiple AV engines to return a verdict, which is then cached for future reference

3

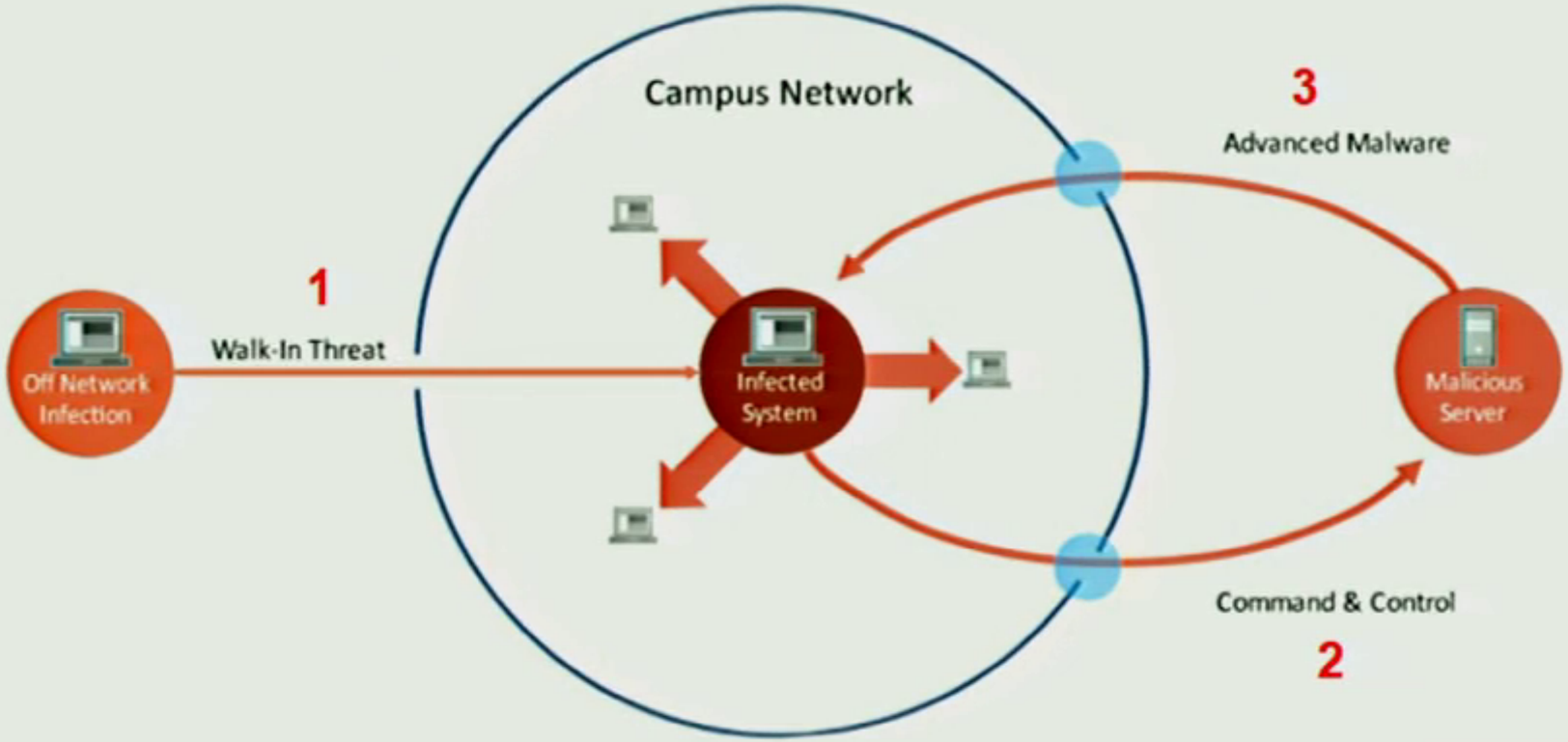
Static analysis: (~30 second)
The static analysis engine does a deeper inspection, with the verdict again cached for future reference

4

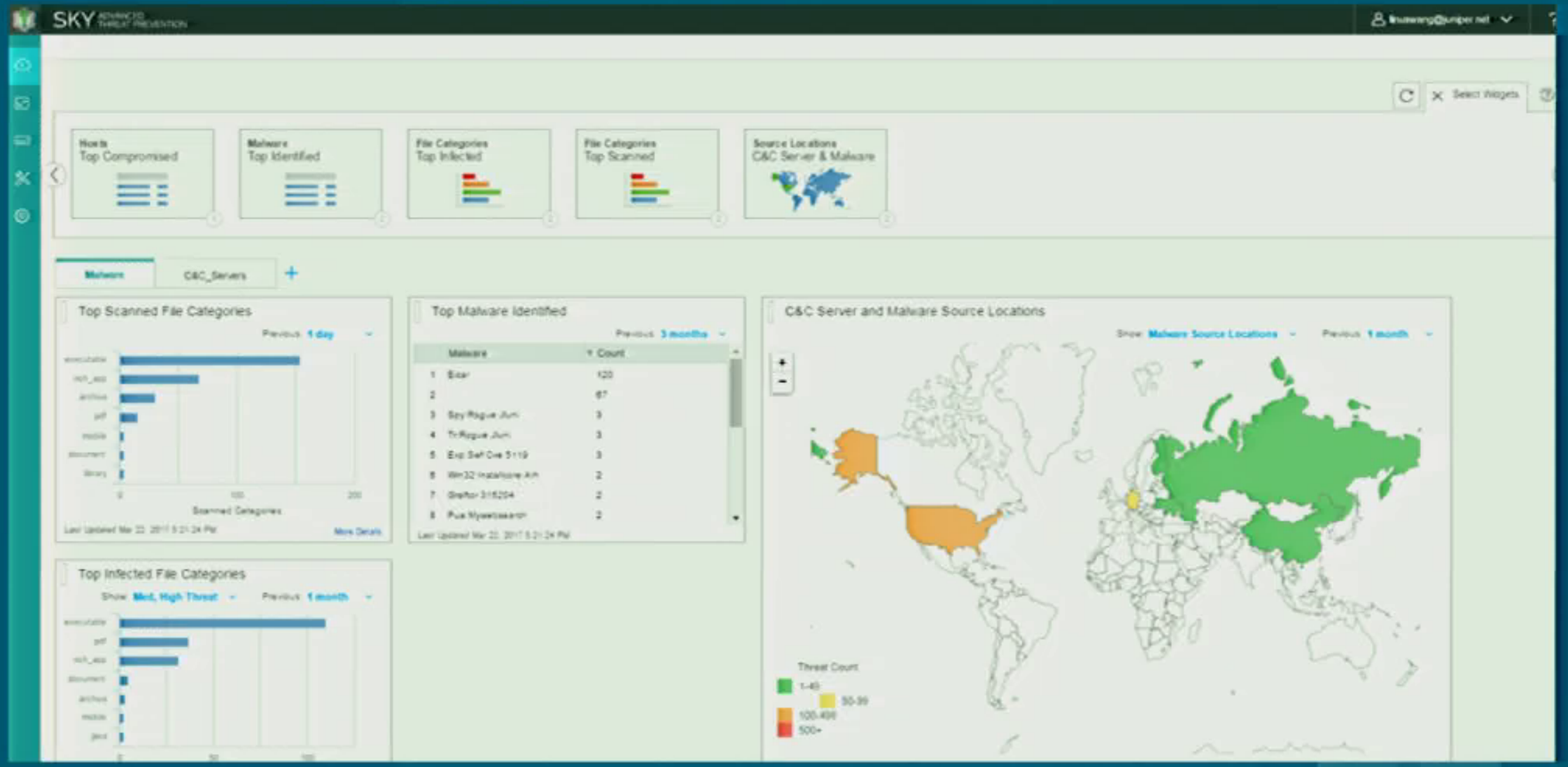
Dynamic analysis: (~7 minutes)
Dynamic analysis in a custom sandbox leverages deception and provocation techniques to identify evasive malware

The Walk-in Threat

- An infected device attached the to protected network

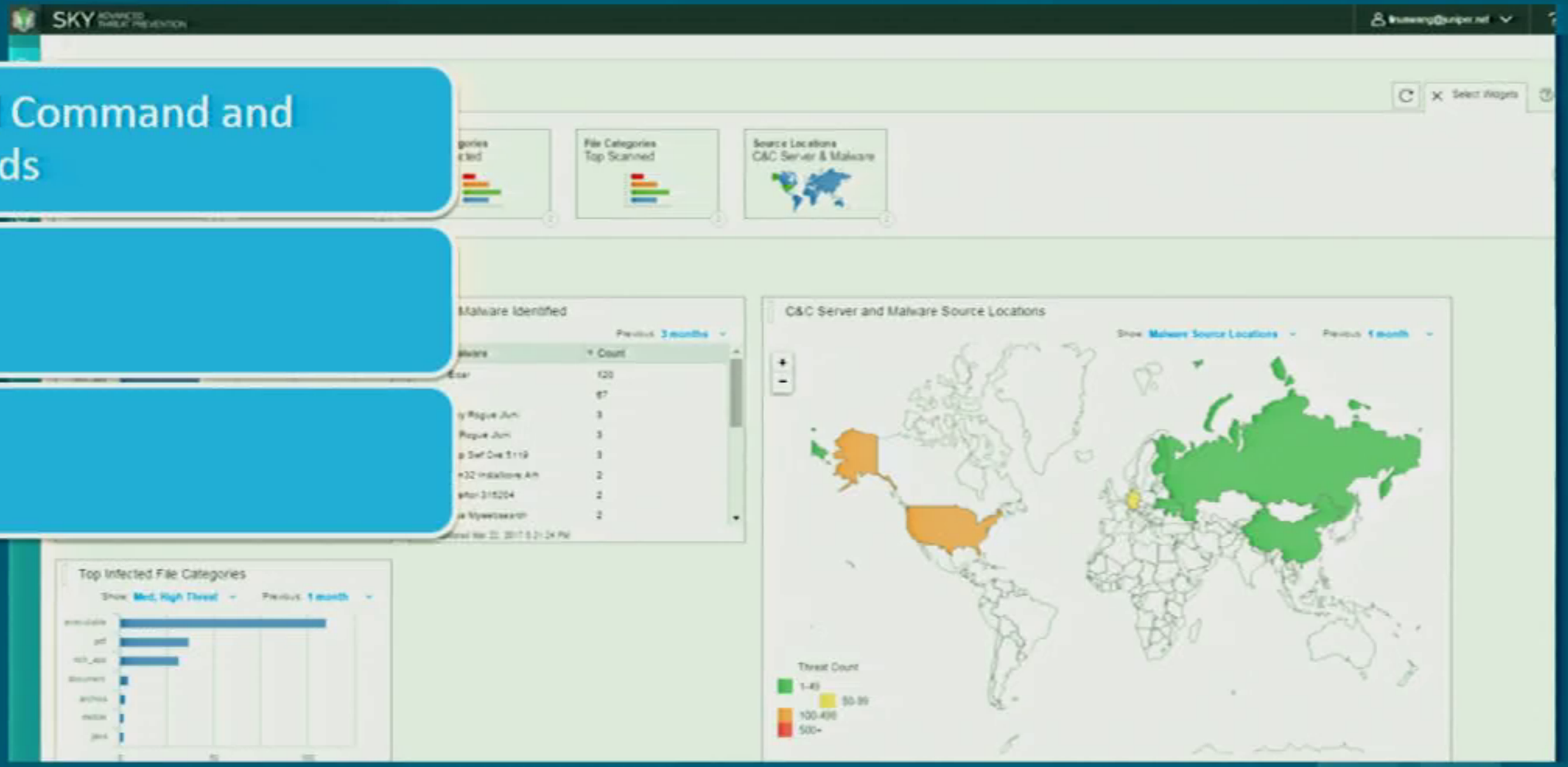


Sky ATP Threat Intelligence Feeds

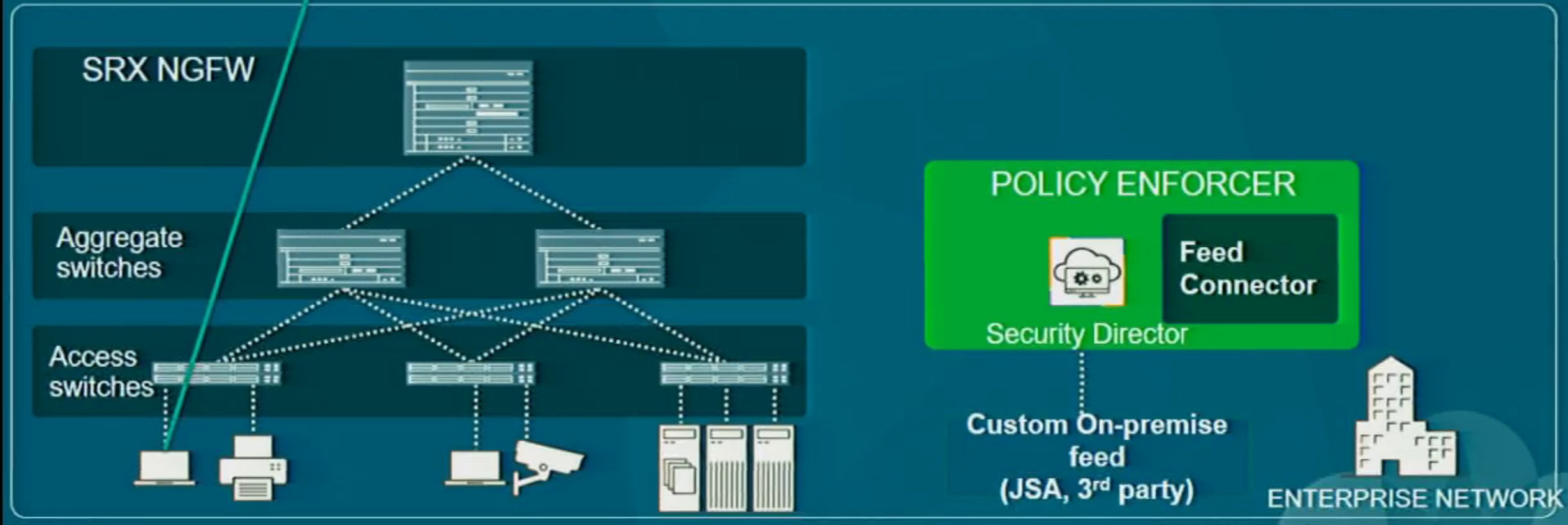


Sky ATP Threat Intelligence Feeds

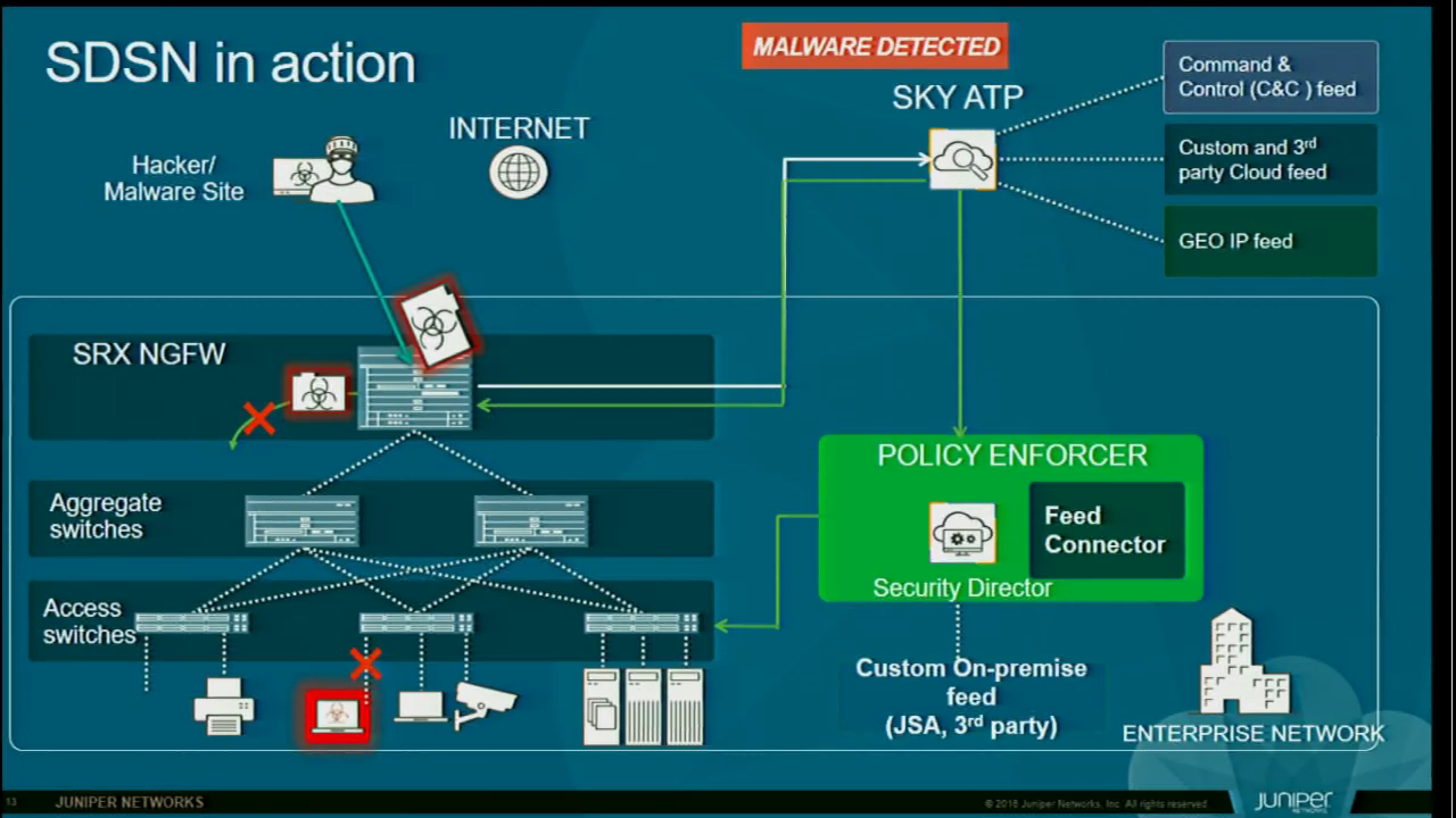
- Reputation based Command and Control (C&C) feeds
- GeoIP feeds
- Custom Feeds



SDSN in action



SDSN in action



Architecture for 3rd Party Enforcement Domains

Use Case: Support for SDSN enforcement on 3rd party systems

ENFORCEMENT

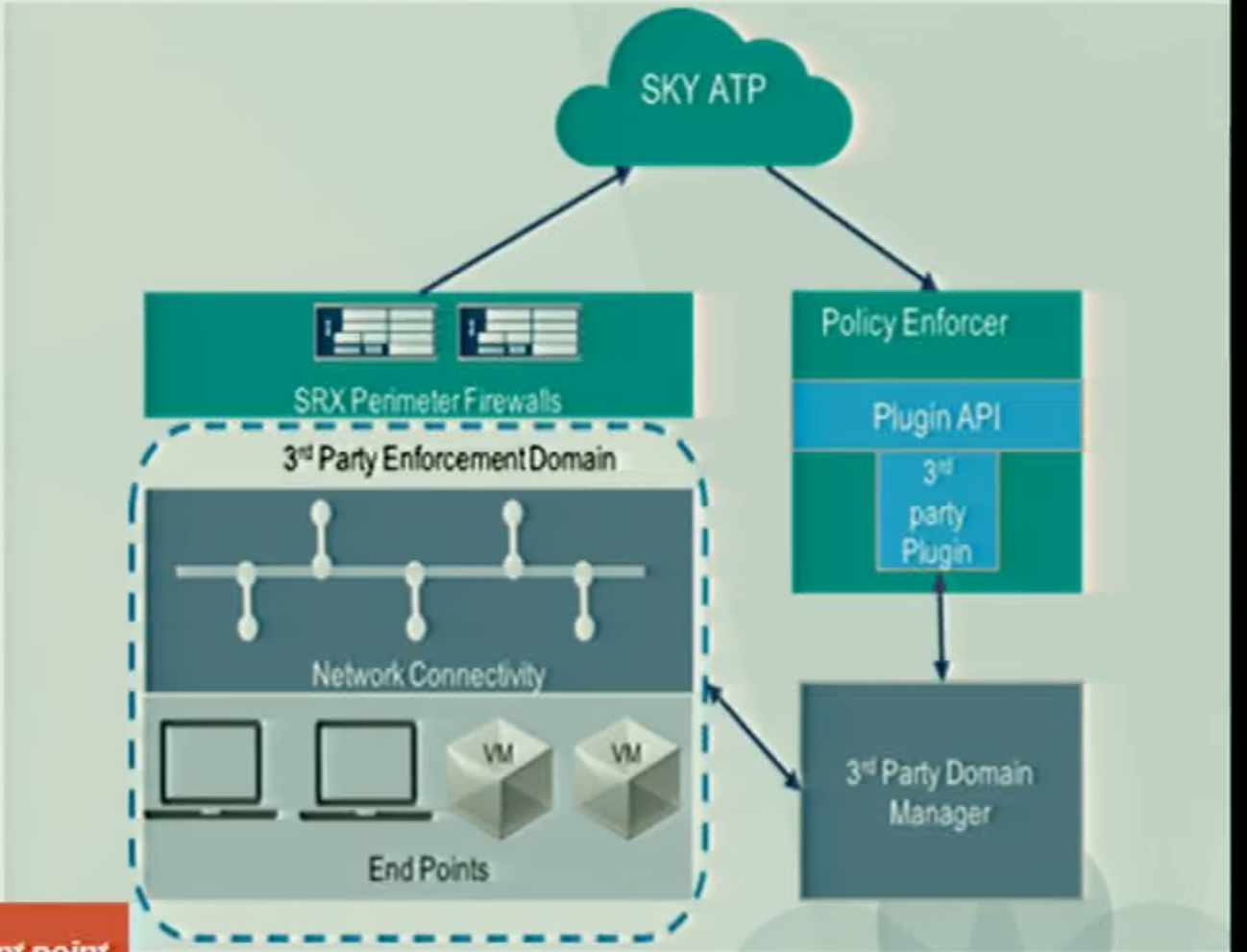
3rd Party Enforcement Domains

Data Center: SDN platforms like NSX, Contrail etc

Campus: NAC platforms like Forescout, Clearpass etc

End point: End point solutions like Carbon Black etc

Cloud: Cloud platforms like AWS, Azure etc



Network as a single enforcement domain - Every element is a policy enforcement point

Case Study A: Malware detection at scale

- Sky ATP deployed in TAP mode on SRX5600 by ISP in North America – primarily serving educational institutions
- Ingress and egress traffic inspected. Inline blocking not enabled
- 7 day period in March 2017

535,302
Total Files Processed

55,629
Unique Files

142
Files Determined to be Malware

69%
Discovered Malware was Previously Known

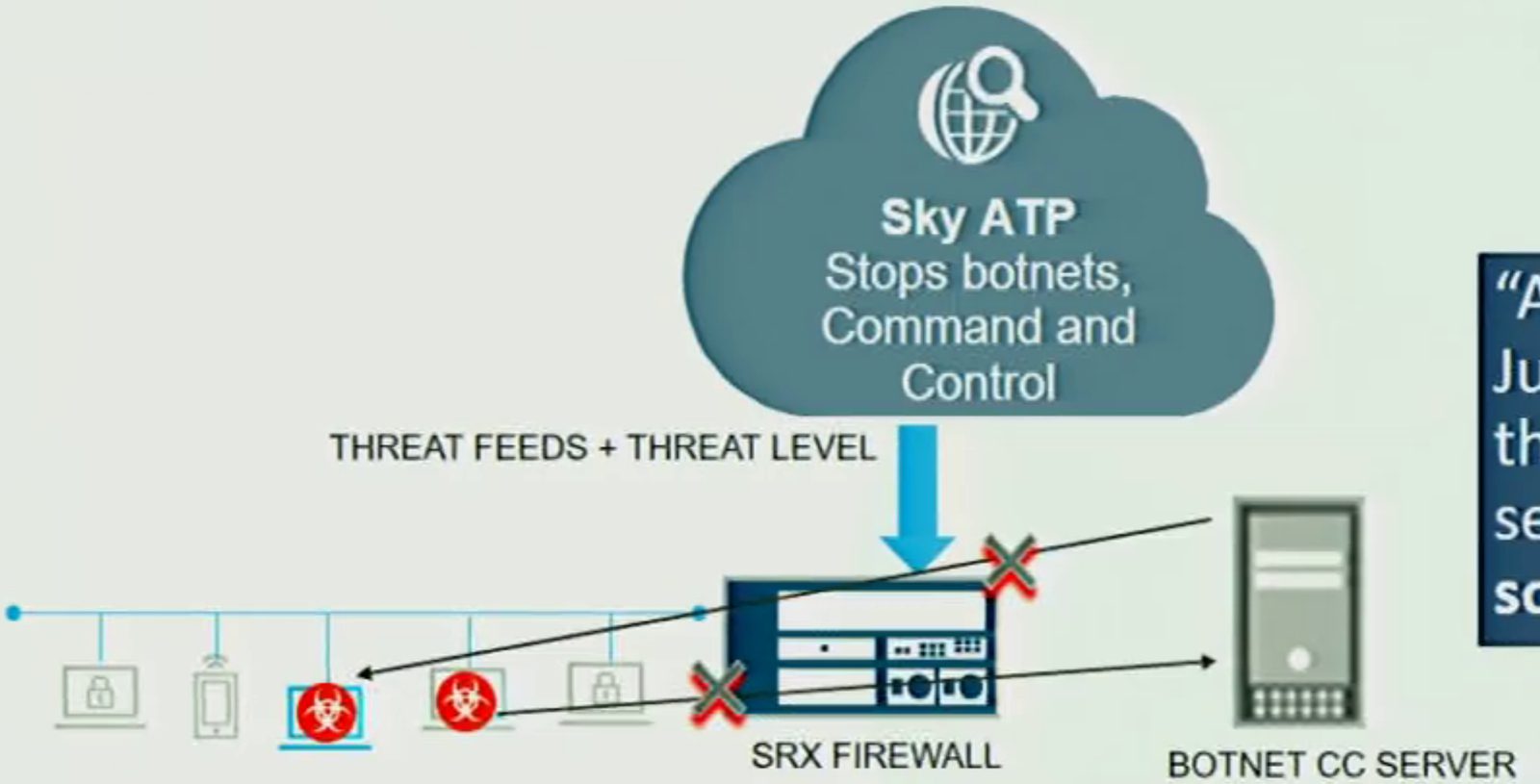
31%
Discovered Malware was previously unseen

Outbound high risk CC connections: 843,346 (1 day)

Case Study B: Botnet detection with Sky ATP feeds

- Large IT consulting and managed IT service provider wanted a robust edge protection solution for its campus and branch offices
- Existing desktop and server based AV solutions not detecting advanced threats

Solution: Juniper SRX1500 + Sky ATP



"After less than a day with Juniper Sky, we knew about threats that we had never seen before." – **Senior IP solutions architect**

Köszönöm a figyelmet