네트워크 보안 자동화를 통한 비즈니스 위협 방어

박달수 부장 (Brian Park)

Security Team Leader , Juniper Korea

모바일 단말의 네트워크 연결 ... 시작에 불과

IOT

이제 곧 모든것이 연결된 세상이 옵니다

Security is also in Transformation

정교한 위협

- 제로데이 공격
- APT (Advanced, persistent, targeted attacks)
- Adaptive malware

클라우드

- 가상화 그리고 SDN
- 클라우드로의 전환
- Application 확산

IT 인프라 변화

- Hybrid cloud deployments
- Device 확산 그리고 BYOD
- IoT

Today’s Threats Are More Complex Than Ever

Ransomware

Locky

638M Attacks in 2016 (167x increase from 2015)

$1B Extorted in 2016

Phishing

eMail

85% Organizations Have Seen Attacks

$1.6M Average Financial Cost

DDoS

Mirai

1Tbps Attack From 150,000 IoT Devices

DDoS-as-a-Service Offered on Dark Net

Malware

Keylogger

390,000 Malicious Programs Registered Daily

18M New Samples Captured in 2Q2016

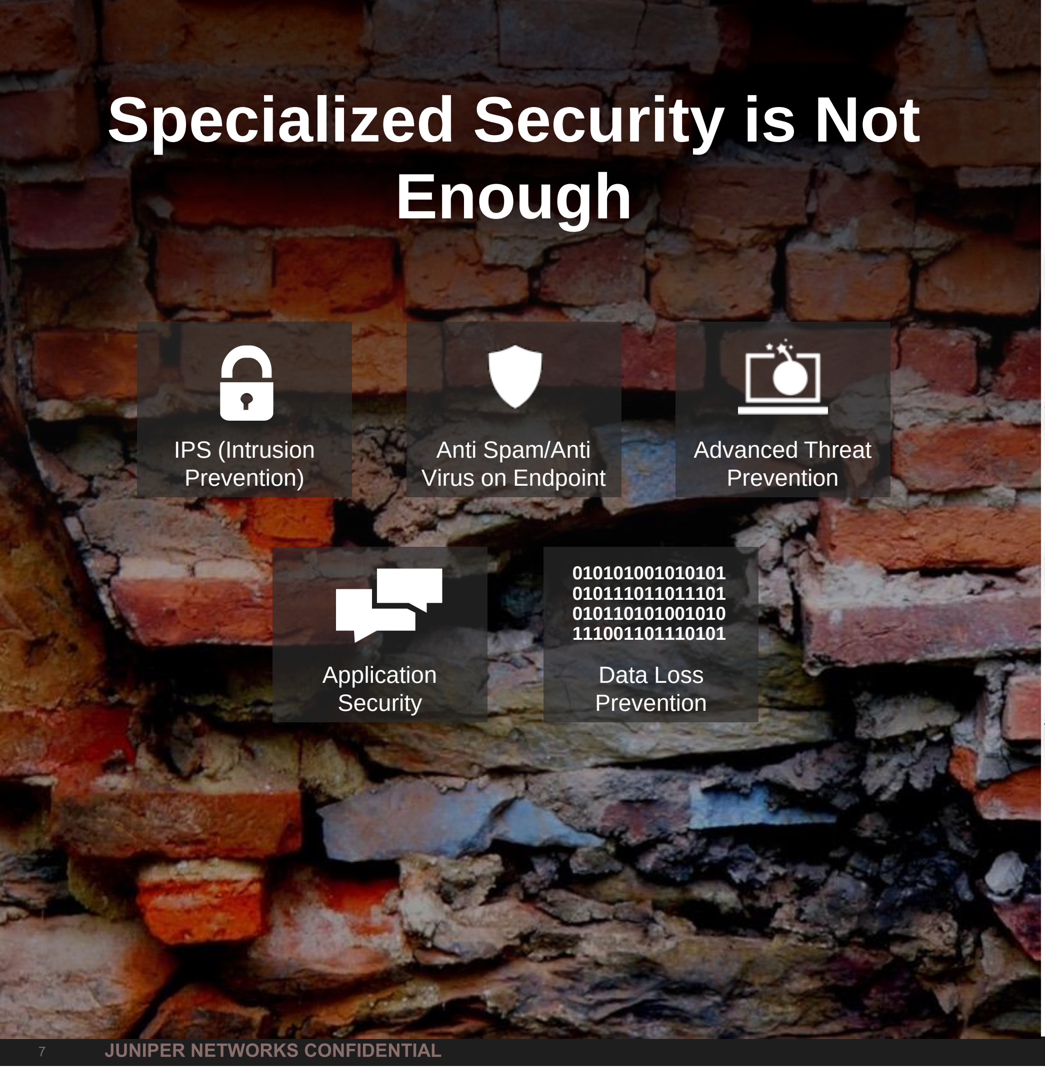
사이버 보안 = 사이버 범죄 퇴치

- Black Hat 해커의 80 %가 조직적인 범죄에 연루
- 사이버 범죄로 인한 피해는 2019년까지 2.1조 달러에 이를 전망
- 공격이 서비스 형태로 거래
  Fraud-as-a-Service , Extortion-as-a-Service and more are here today

하지만 결국 네트웍연결이 필요합니다

if 知彼知己
then 百戰百勝

Specialized Security is Not Enough



IPS (Intrusion Prevention)

Anti Spam/Anti Virus on Endpoint

Advanced Threat Prevention

Application Security

010101001010101
010111011011101
010110101001010
111001101110101

Data Loss Prevention

- Isolated security functions
- Multiple vendors and interfaces
- Intelligence not shared
- Unmanaged risk to business

Machines are fundamentally **dumb**

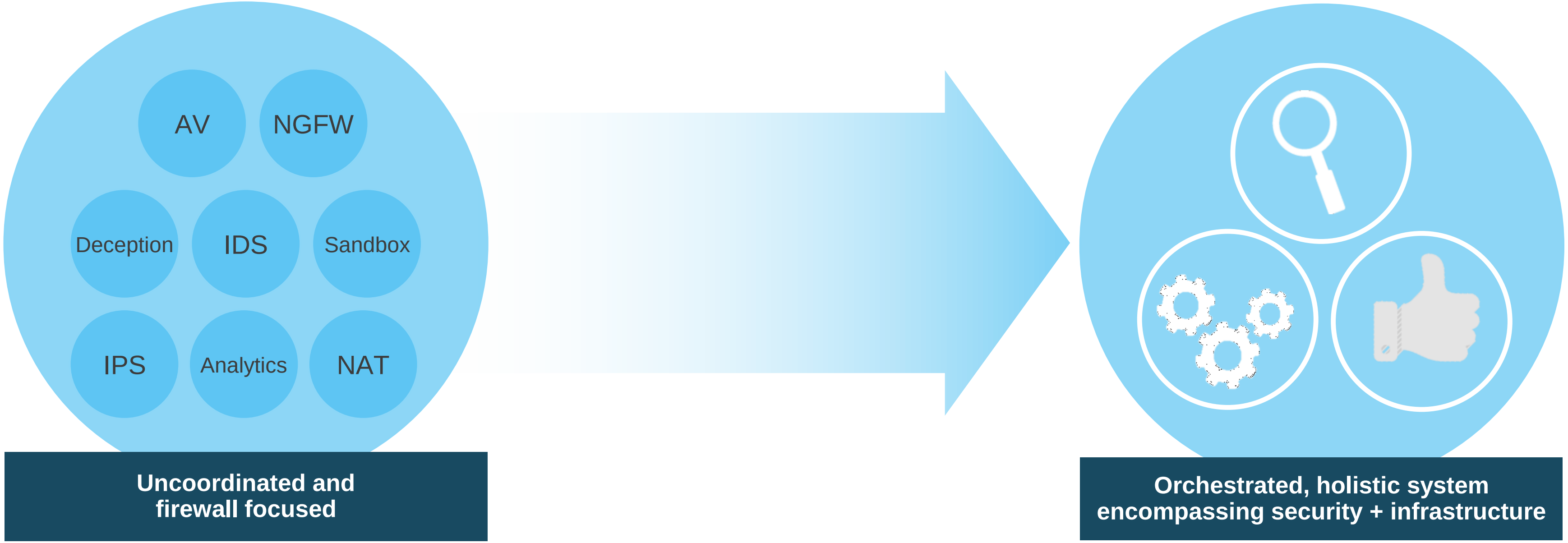
Good for following instructions

Not lateral thinking

Software defined (secure) networks

Leverage the flexible, adaptive, automated, programmable – for security!

Demanding Software Defined Secure Networks



Uncoordinated and firewall focused

Orchestrated, holistic system encompassing security + infrastructure

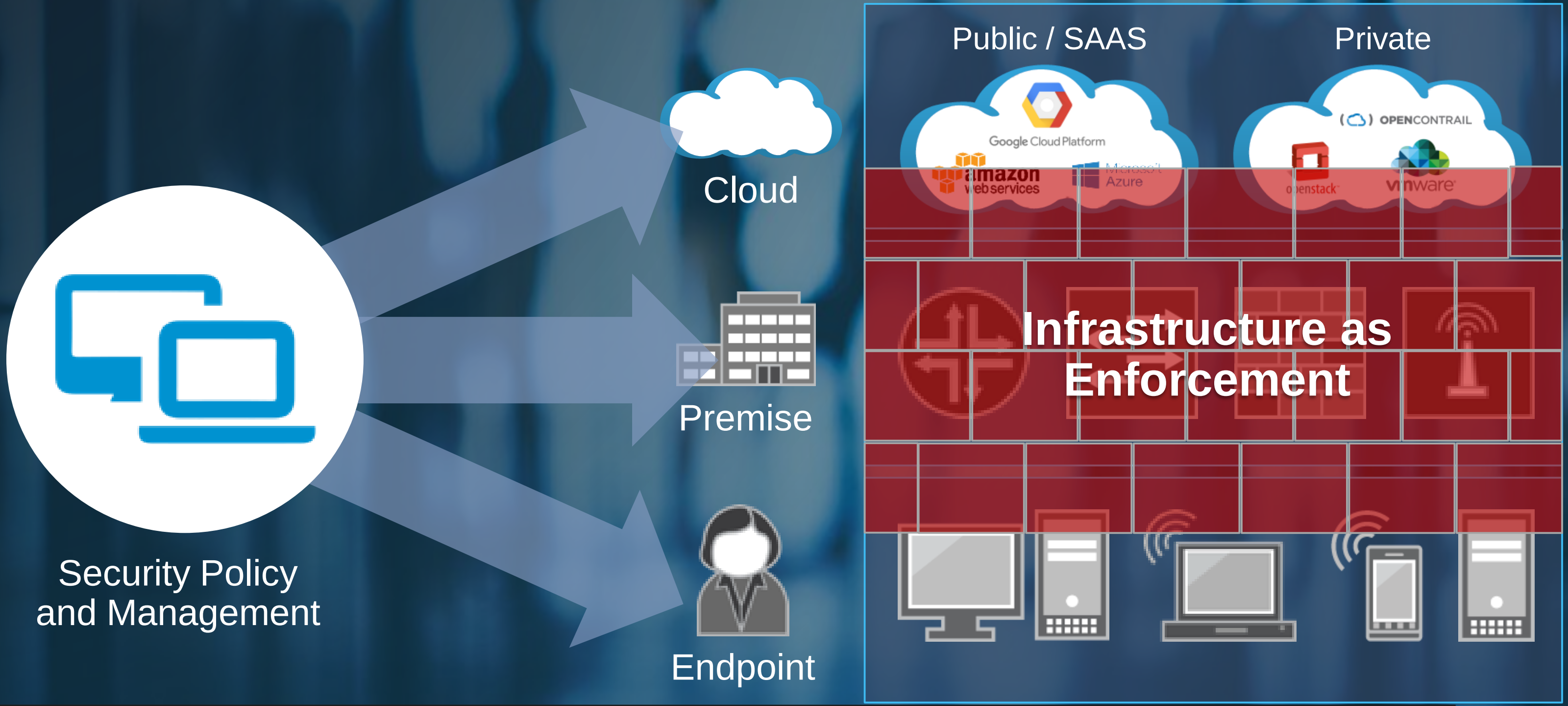
Global Policy Orchestration, Policy Engine

Open and Unified Threat Detection

Dynamic, Automated Enforcement

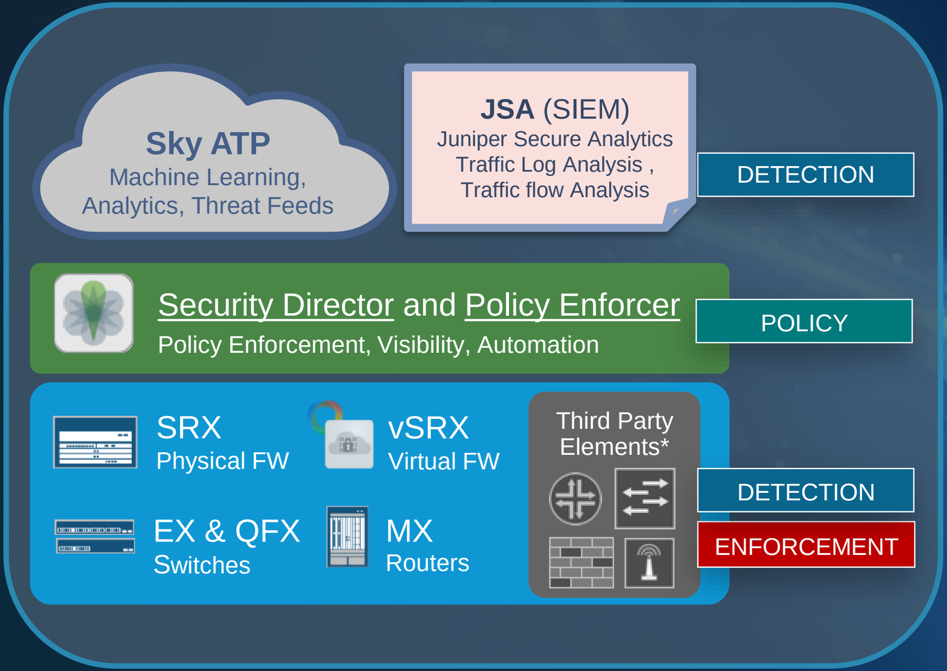
Define Once, Detect and Enforce Everywhere

Pervasive, Automated, Intent-driven



Software Defined Secure Network (SDSN)

Pervasive, Automated, Intent-driven



POLICY

Create and centrally manage policy with an intent-based system

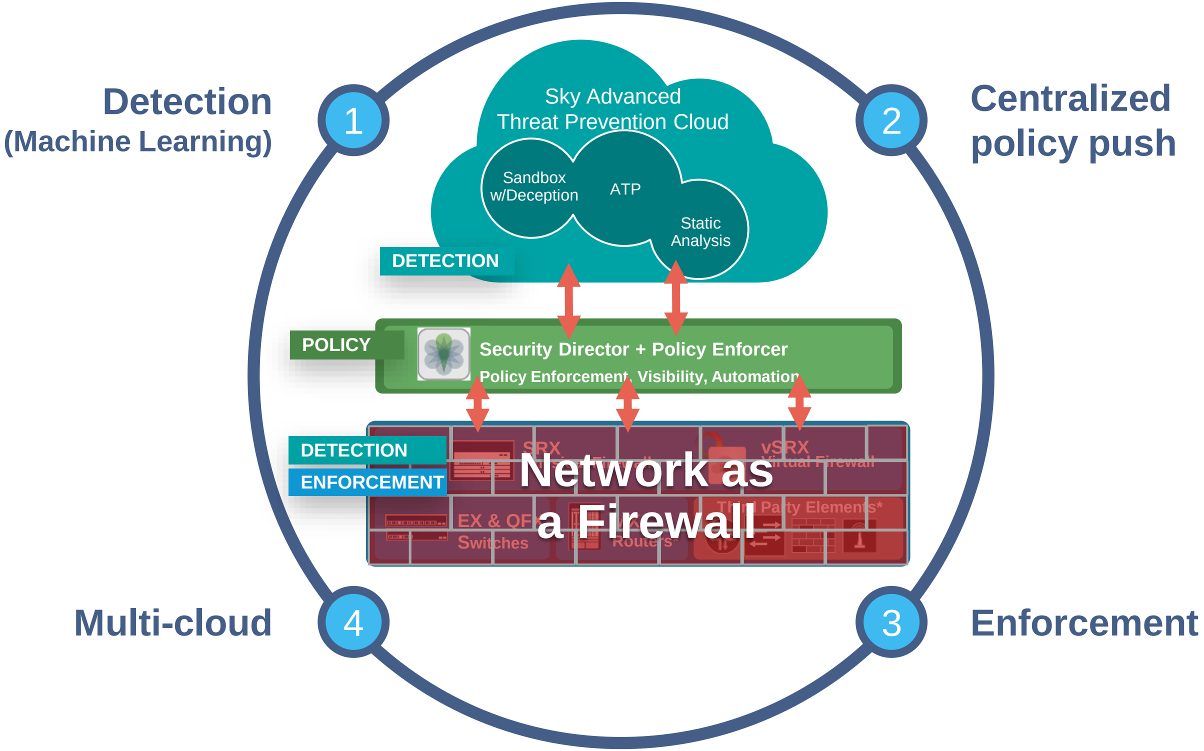
DETECTION

Unify threat intelligence from multiple sources

ENFORCEMENT

Automatically enforce policy across sites and cloud

Software Defined Secure Networks: Network As A Firewall



Detection
(Machine Learning)

1

Centralized
policy push

2

Enforcement

3

Multi-cloud

4

Sky Advanced
Threat Prevention Cloud

Sandbox
w/Deception

ATP

Static
Analysis

DETECTION

POLICY

Security Director + Policy Enforcer

Policy Enforcement, Visibility, Automation

DETECTION

ENFORCEMENT

SRX
Physical Firewall

vSRX
Virtual Firewall

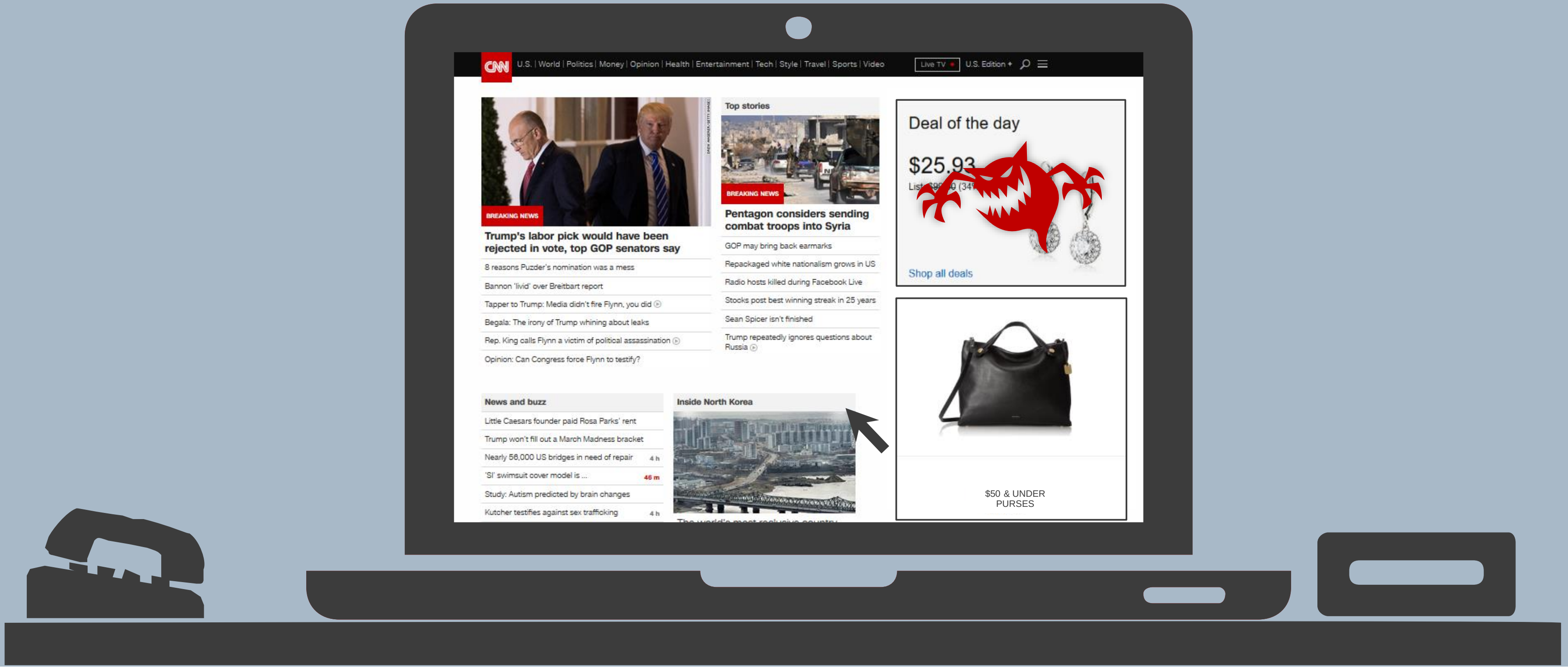
EX & QFX
Switches

MX
Routers*

Third Party Elements*

Network as
a Firewall

Sky Advance Threat Prevention


CNN
U.S. | World | Politics | Money | Opinion | Health | Entertainment | Tech | Style | Travel | Sports | Video
Live TV
U.S. Edition +
BREAKING NEWS
BREAKING NEWS

Trump's labor pick would have been rejected in vote, top GOP senators say

- 8 reasons Puzder's nomination was a mess
- Bannon 'livid' over Breitbart report
- Tapper to Trump: Media didn't fire Flynn, you did
- Begala: The irony of Trump whining about leaks
- Rep. King calls Flynn a victim of political assassination
- Opinion: Can Congress force Flynn to testify?

Top stories

Pentagon considers sending combat troops into Syria

- GOP may bring back earmarks
- Repackaged white nationalism grows in US
- Radio hosts killed during Facebook Live
- Stocks post best winning streak in 25 years
- Sean Spicer isn't finished
- Trump repeatedly ignores questions about Russia

Deal of the day

$25.93

List $99.90 (34

Shop all deals

News and buzz

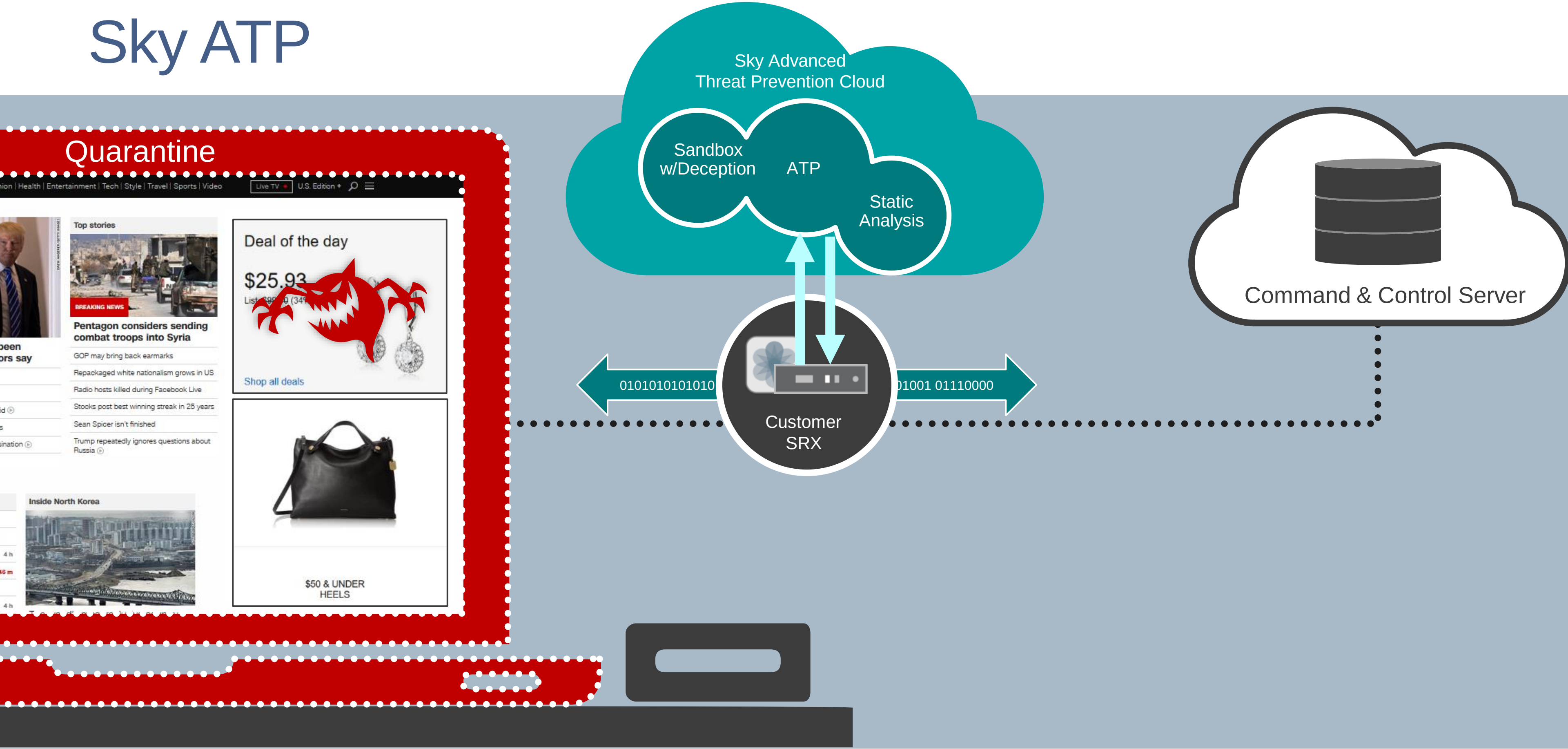
- Little Caesars founder paid Rosa Parks' rent
- Trump won't fill out a March Madness bracket
- Nearly 56,000 US bridges in need of repair 4 h
- 'SI' swimsuit cover model is ... 46 m
- Study: Autism predicted by brain changes
- Kutcher testifies against sex trafficking 4 h

Inside North Korea

The world's most reclusive country

$50 & UNDER
PURSES

Sky ATP



ion | Health | Entertainment | Tech | Style | Travel | Sports | Video   Live TV   U.S. Edition +

Top stories

BREAKING NEWS

Pentagon considers sending combat troops into Syria

GOP may bring back earmarks

Repackaged white nationalism grows in US

Radio hosts killed during Facebook Live

Stocks post best winning streak in 25 years

Sean Spicer isn't finished

Trump repeatedly ignores questions about Russia

een
ors say

Inside North Korea

Deal of the day

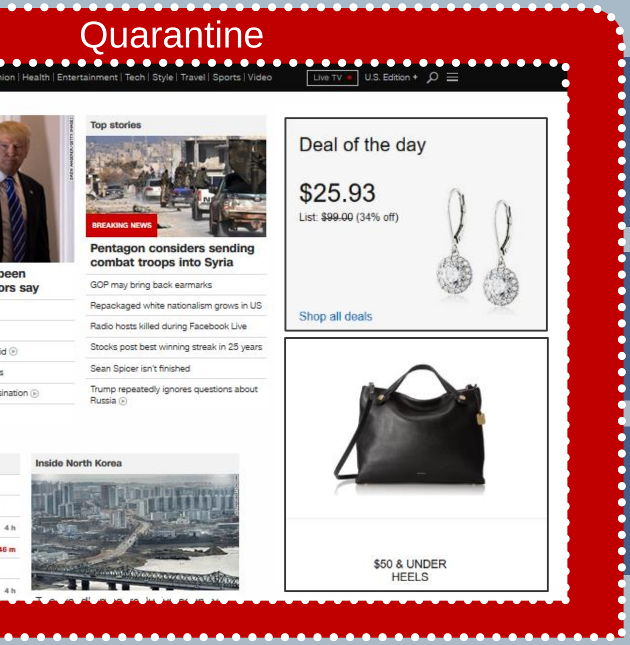
$25.93

List $99.99 (34%

Shop all deals

$50 & UNDER
HEELS

Sky ATP



Quarantine

ion | Health | Entertainment | Tech | Style | Travel | Sports | Video

Live TV

U.S. Edition +

been
ors say

id

s

sination

Top stories

BREAKING NEWS

Pentagon considers sending combat troops into Syria

GOP may bring back earmarks

Repackaged white nationalism grows in US

Radio hosts killed during Facebook Live

Stocks post best winning streak in 25 years

Sean Spicer isn't finished

Trump repeatedly ignores questions about Russia

Inside North Korea

4 h

46 m

4 h

Deal of the day

$25.93

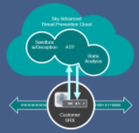
List: ~~$99.00~~ (34% off)

Shop all deals

$50 & UNDER
HEELS

Threat vector bypasses IT desktop/server based AV,
While Juniper Sky ATP immediately detects the malware and quarantines the user

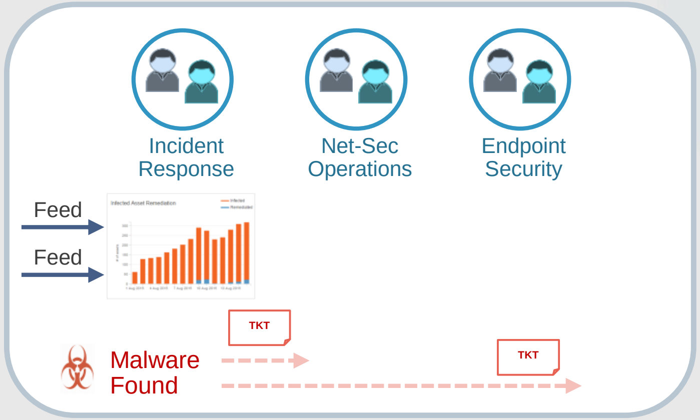
You cannot trust websites. Active threats cannot be managed with reactive security solutions



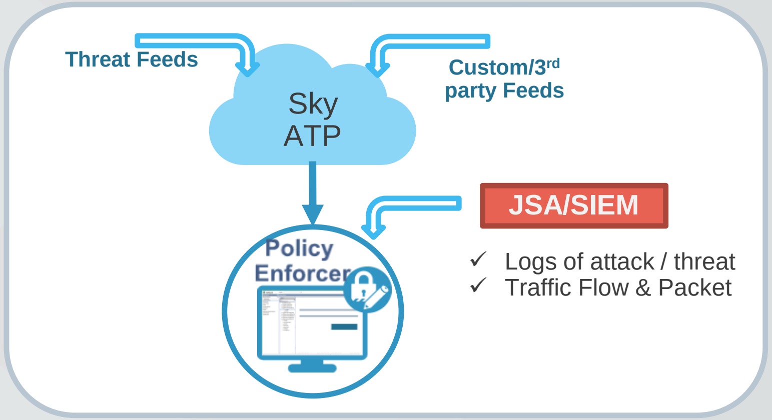
Solution: Deploy security policies which incorporates active & dynamic threat prevention with Sky ATP

SDSN – Threat Management

Manual Threat Workflows



Threat Management Automation



- ✓ Logs of attack / threat
- ✓ Traffic Flow & Packet

- 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

SDSN Security Alliances

CASB

netskope

CipherCloud
Trust in the Cloud™

Cloud App Security

Access Security

ForeScout

aruba
a Hewlett Packard
Enterprise company

Access Security

Endpoint Security

CARBON BLACK
ARM YOUR ENDPOINTS

Endpoint Protection

Micro-segmentation

Micro-segmentation

vmware NSX

SDSN for the SDDC

Ready to Deploy Comprehensive Security Solutions

Every THING on Your Network is a Potential Threat

Normal behavior: call home beacons, energy utilization

Anomalous behavior: bursting traffic, abnormal high data download rate

Is this normal? How do we mitigate risk?

Build More than Network Security

Align your security to your business imperatives
Create and centrally orchestrate policy

Stop sophisticated cyber crime
Gather and distribute threat intelligence across your network

Identify risk sooner
Leverage cloud economics for real-time analysis

Automatically apply enforcement in real time – secure the network in real time

THANK YOU