From Endpoint to Firewall – Building Effective Threat Perimeters with Cisco and Splunk

Doug Hurd & Alex Calaoagan

Security Product Management – Cisco Systems

Oct 2018

Agenda:

Make Better Use of What You Already Have

Get control of the new perimeter by:

- Making the firewall access control perimeter into a threat control perimeter
- Getting more from endpoint analytics (it's more than just finding malware!)
- Increasing on and off-network visibility and threat prevention – from data center to cloud

Splunk + Cisco – “Better Together” for Security

Security Breadth, Customer Reach, Infrastructure for Automation

- Largest security footprint in the industry
- Produces broad range of security telemetry across most security technologies
- Ubiquitous network footprint enables threat response automation
- High investment in Splunk apps for serving joint customers

Analytics Efficacy, Ability to Automate

- Voluminous, context-rich Cisco security data sources drive more effective SIEM use cases and new use cases beyond security
- Automated actions in Cisco network environs
- Proven, supported integrations accelerate time to value

Cisco Security is Well Integrated with Splunk

Quality Data Goes In, Network-Wide Mitigation Comes Out

CURATE & CORRELATE | **TAKE IMMEDIATE ACTION**

CISCO Firepower
Highly-enriched NGFW, IPS & malware events

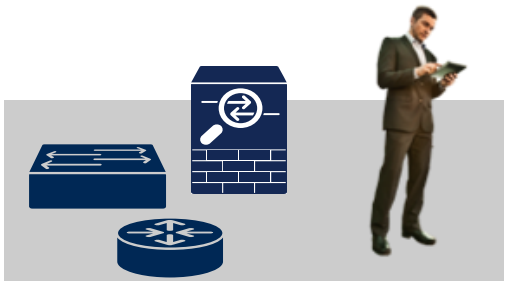
CISCO Umbrella
Context on domains, IPs or file hashes

CISCO AMP
File dispositions & malware context

CISCO ISE
Identity, posture, device-type, network privilege

splunk> Analytics & Action

Cisco ISE Rapid Threat Containment



User/Device Investigation & Quarantine

splunk> .conf18

Cisco Security is Well Integrated with Splunk

Quality Data Goes In, Network-Wide Mitigation Comes Out

AND MORE…

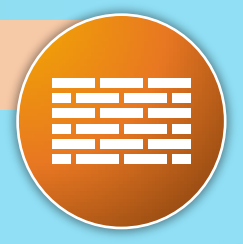
ESA

Threat Grid

WSA

AnyConnect NVM

ASA



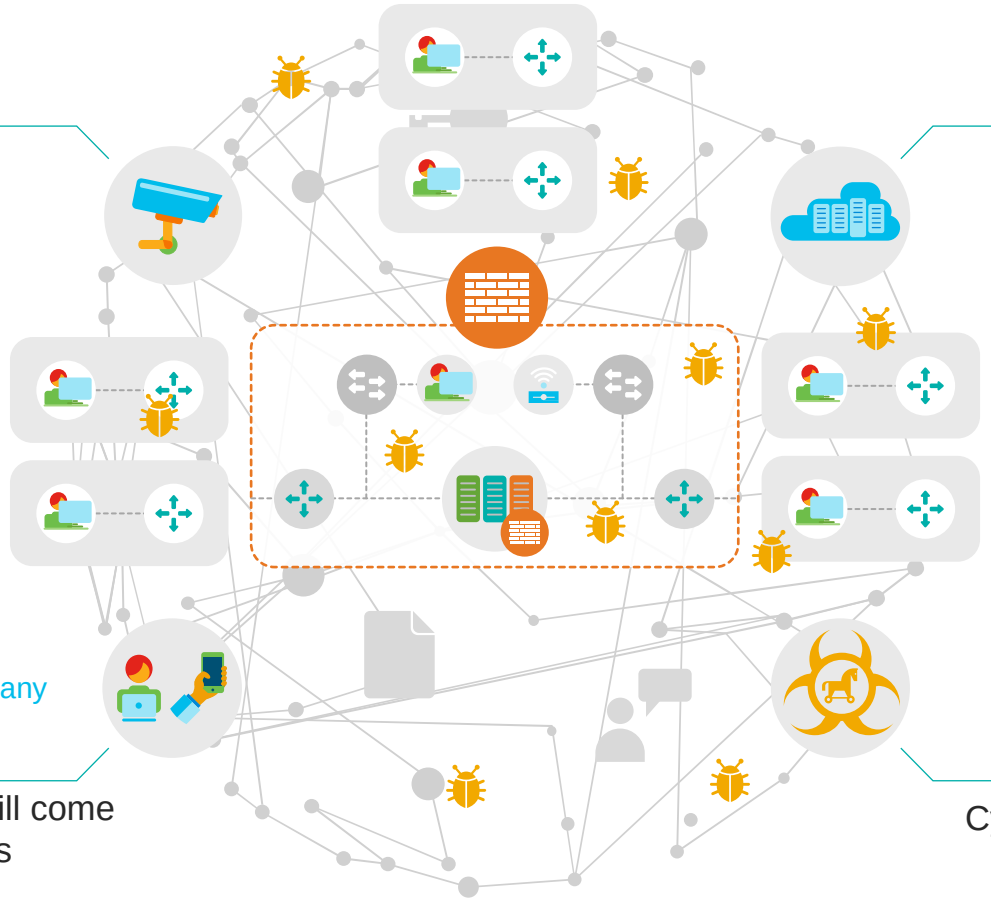
Cloudlock

A New Era for the Security Perimeter

"There is No Perimeter"…aka "The Perimeter is Everywhere"

More devices connect everyday

1 million new devices will go online every hour by 2020



Workloads and apps are shifting **to the cloud**

83% of enterprise workloads will be in the cloud by 2020

Direct internet access at distributed branches

By 2020, >60% of enterprises will have deployed DIA

Users work from anywhere across many devices

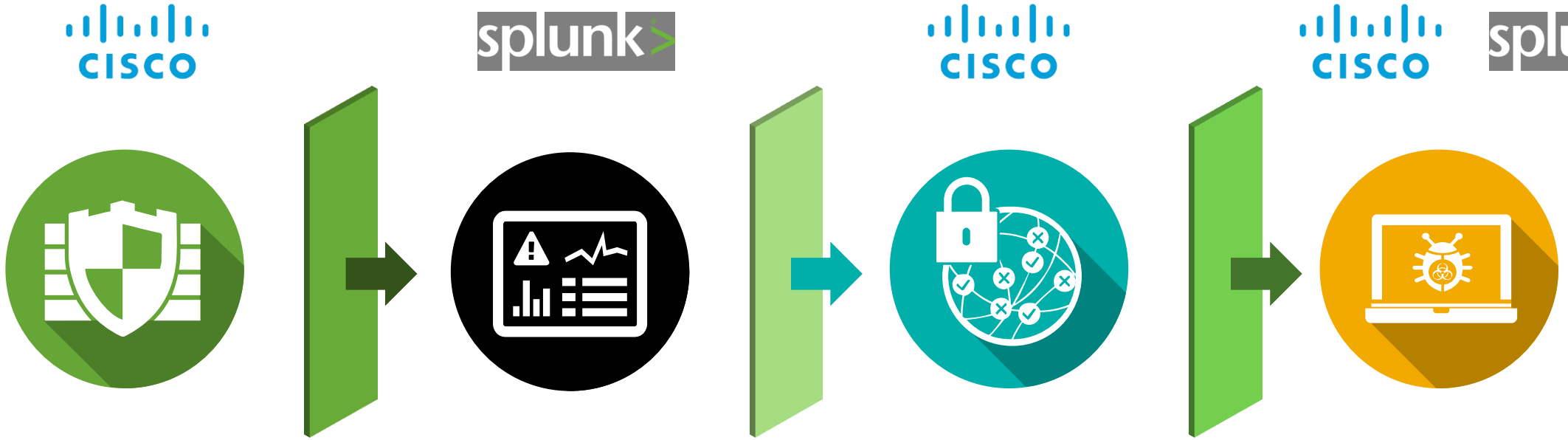
By 2020, 2/3rds of all IP traffic will come from wireless and mobile devices

Threats are more numerous and persistent

Cyber crime damage costs to hit **$6 trillion annually** by 2021

Four-Phase Network Security Rollout

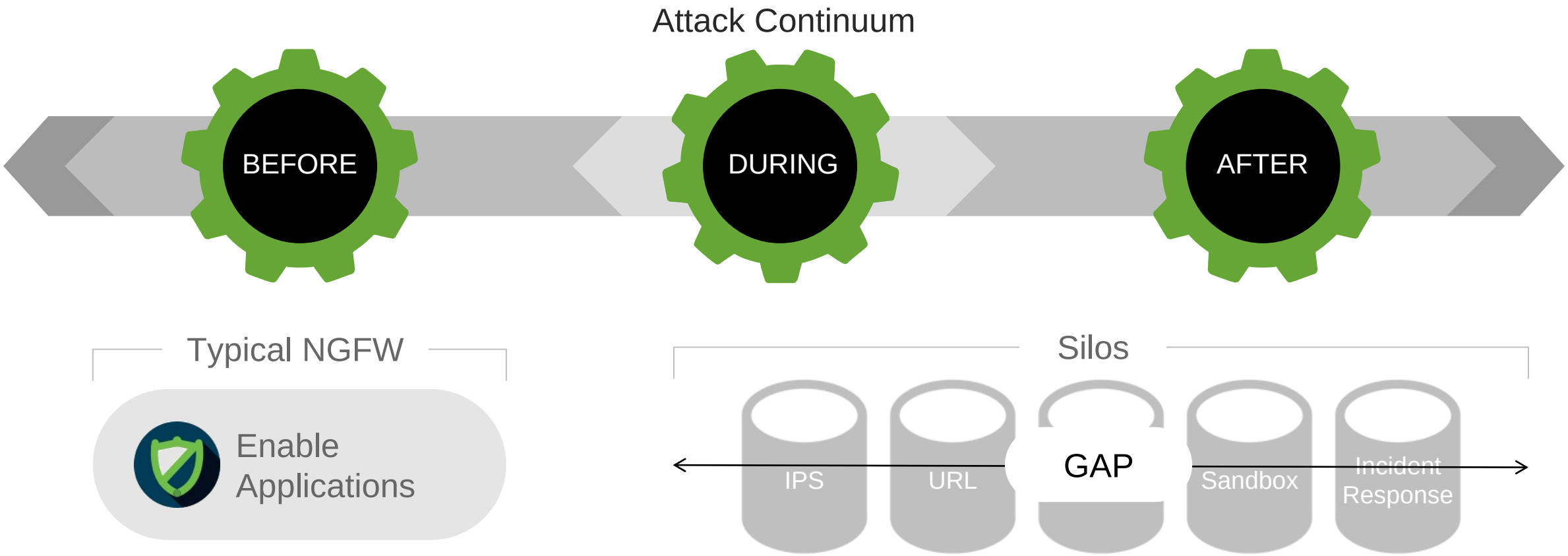
Comprehensive perimeter security is still possible



The Traditional Perimeter – Evolve Firewall Access Control to Threat Control

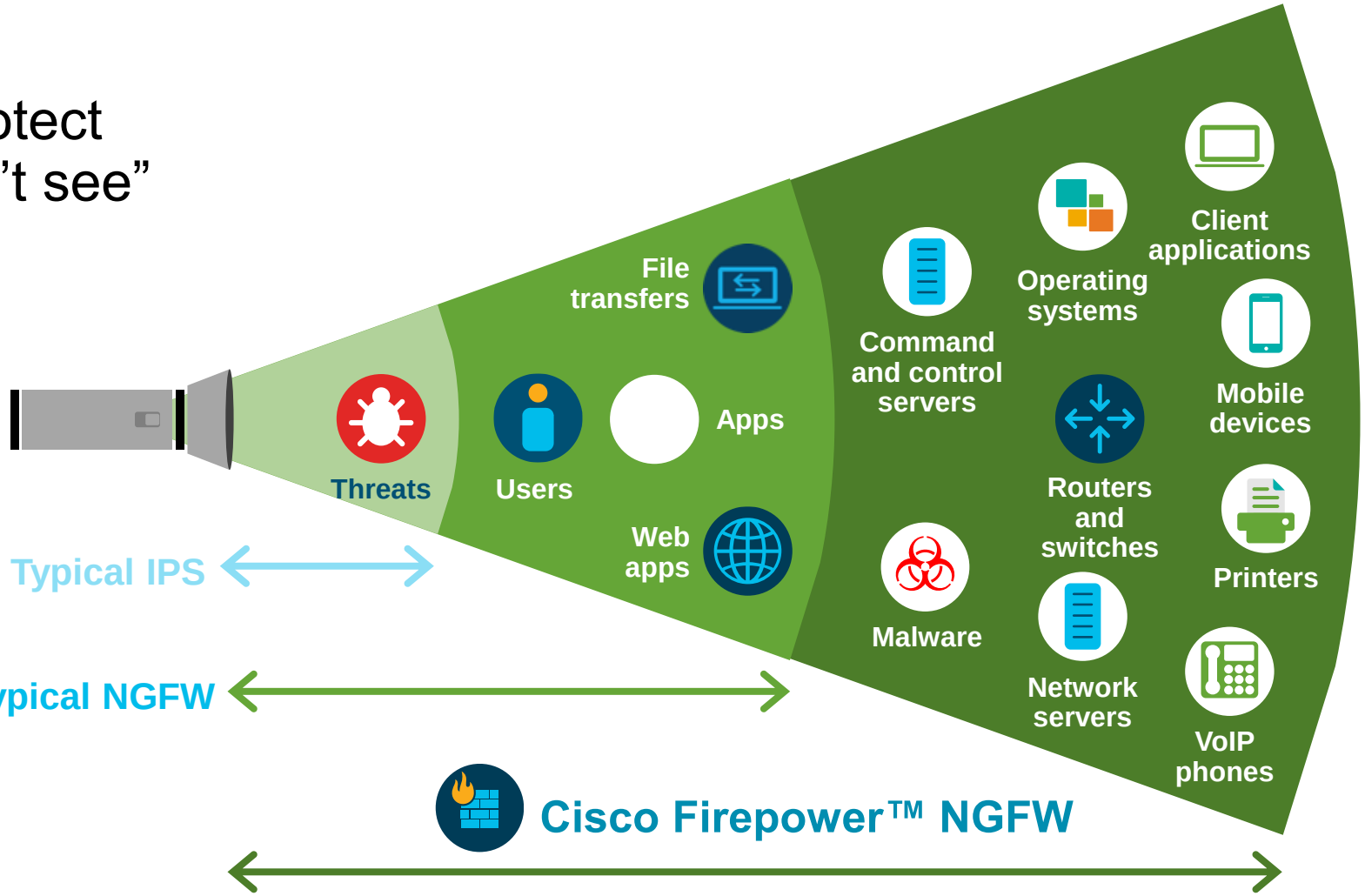
Most NGFW Protect Before an Attack…

But are less effective during or after one

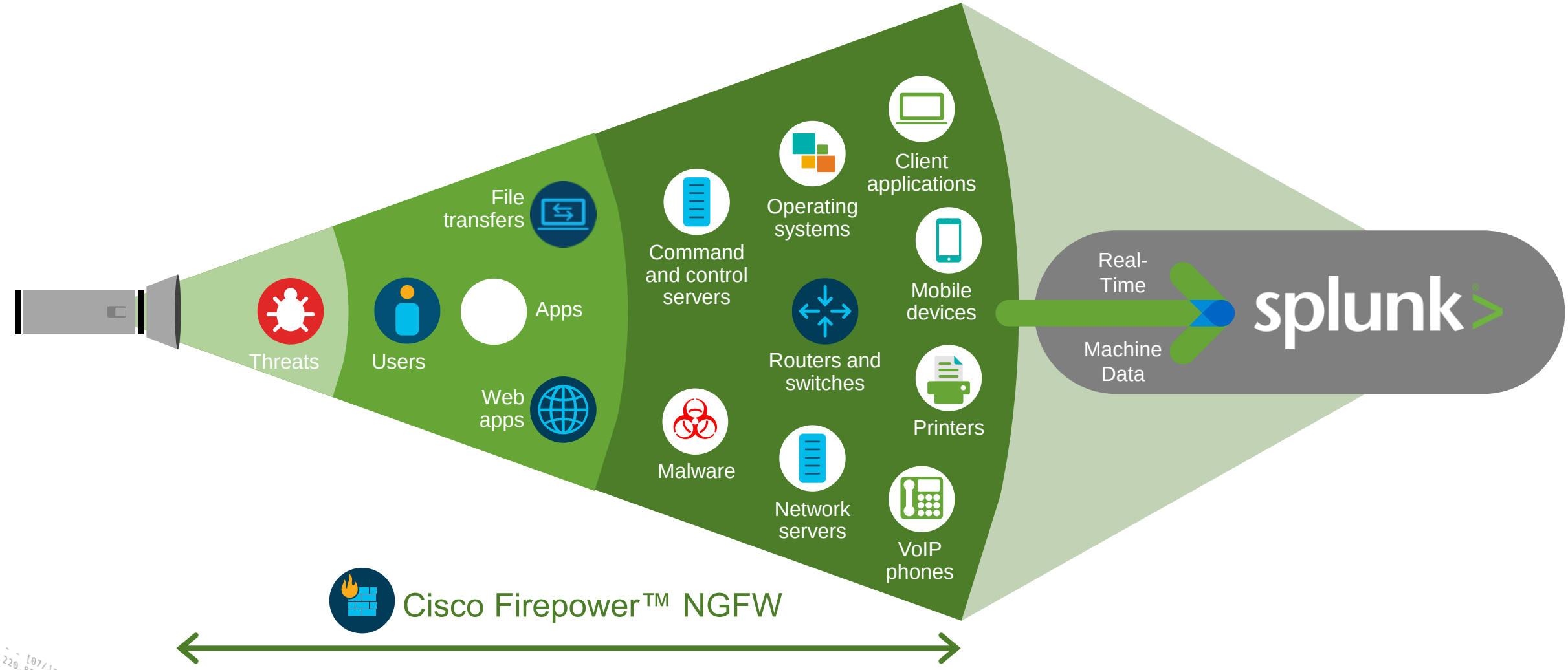


Gain More Insight with Increased Visibility

"You can't protect what you can't see"



Context-Rich Data Accelerates Threat Management in Splunk



Attain Deep Threat Visibility with Splunk & Firepower

Use Case: Tell me about security activity associated with user “Pat”

Traditional Firewall
Limited data

Pat tried to access XYZ network segments and was denied

Firepower Syslog
Uncorrelated events

Pat tried to access XYZ network segments and was denied due to policy ABC

Pat has been using unapproved applications

Pat has triggered IPS alerts

Pat has been associated with ABC malware

Firepower+Splunk
End-to-end correlated view

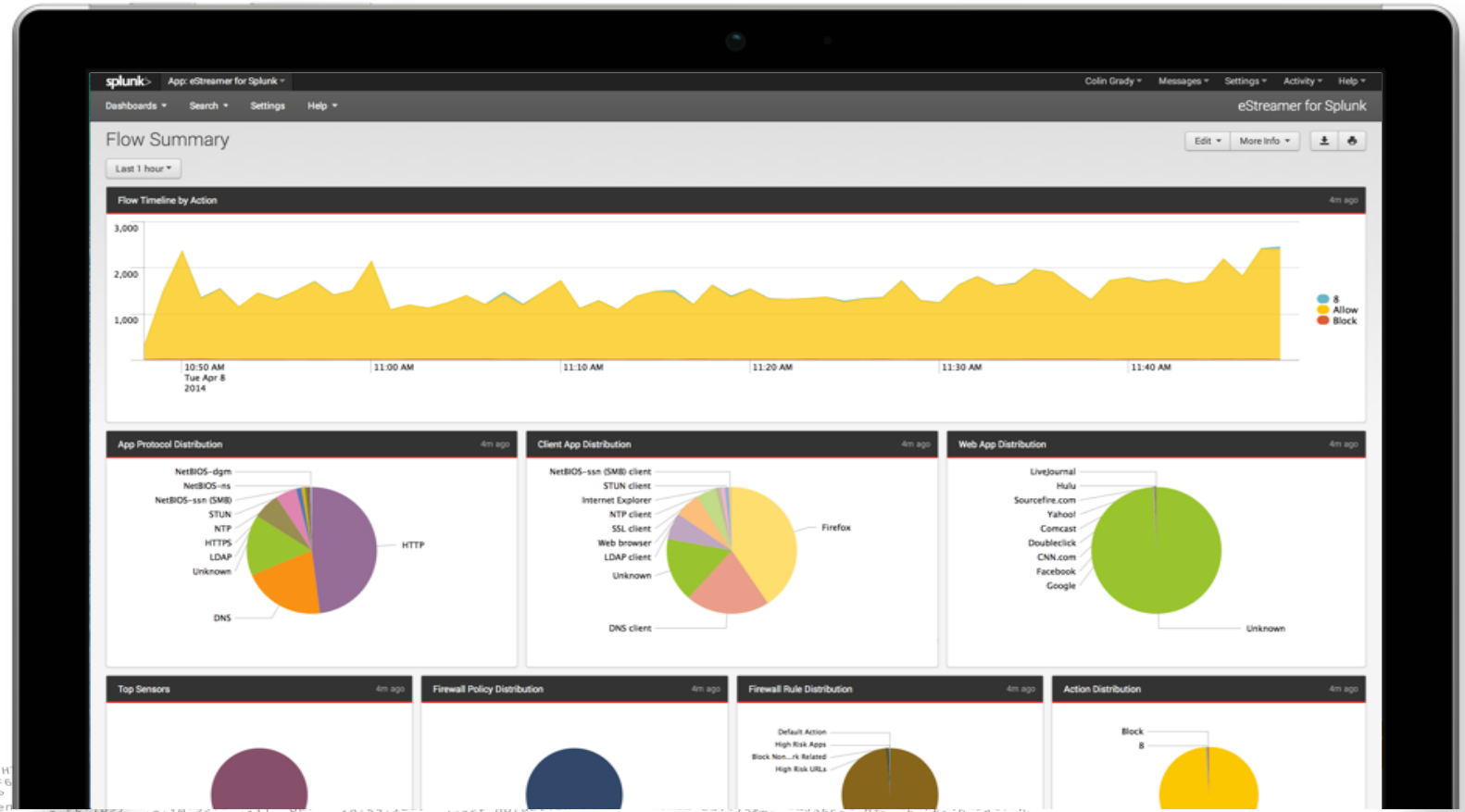
Pat touched ABC malware, tripped ABC IPS sigs and was denied access to XYZ network segments associated with “Hi Value” FW policy when using unapproved application via an allowed URL. Packet data was captured for analyzing this event. Talos and partner threat intel has been associated with the event.

Rapid Time-to-Value

Cisco Firepower eNcore NGFW App & Add-on for Splunk

- Drill into dashboard components to access underlying event source data in complete detail
- Fully conduct comprehensive forensics investigations across historical data
- Compliance reporting across historical data
- Pinpoint trends and set policies based on historical trends
- Easily integrate with existing SOC processes
- Most comprehensive integration across many data sources
- Proven across 100s of deployments
- 24X7 support via Cisco TAC (optional)

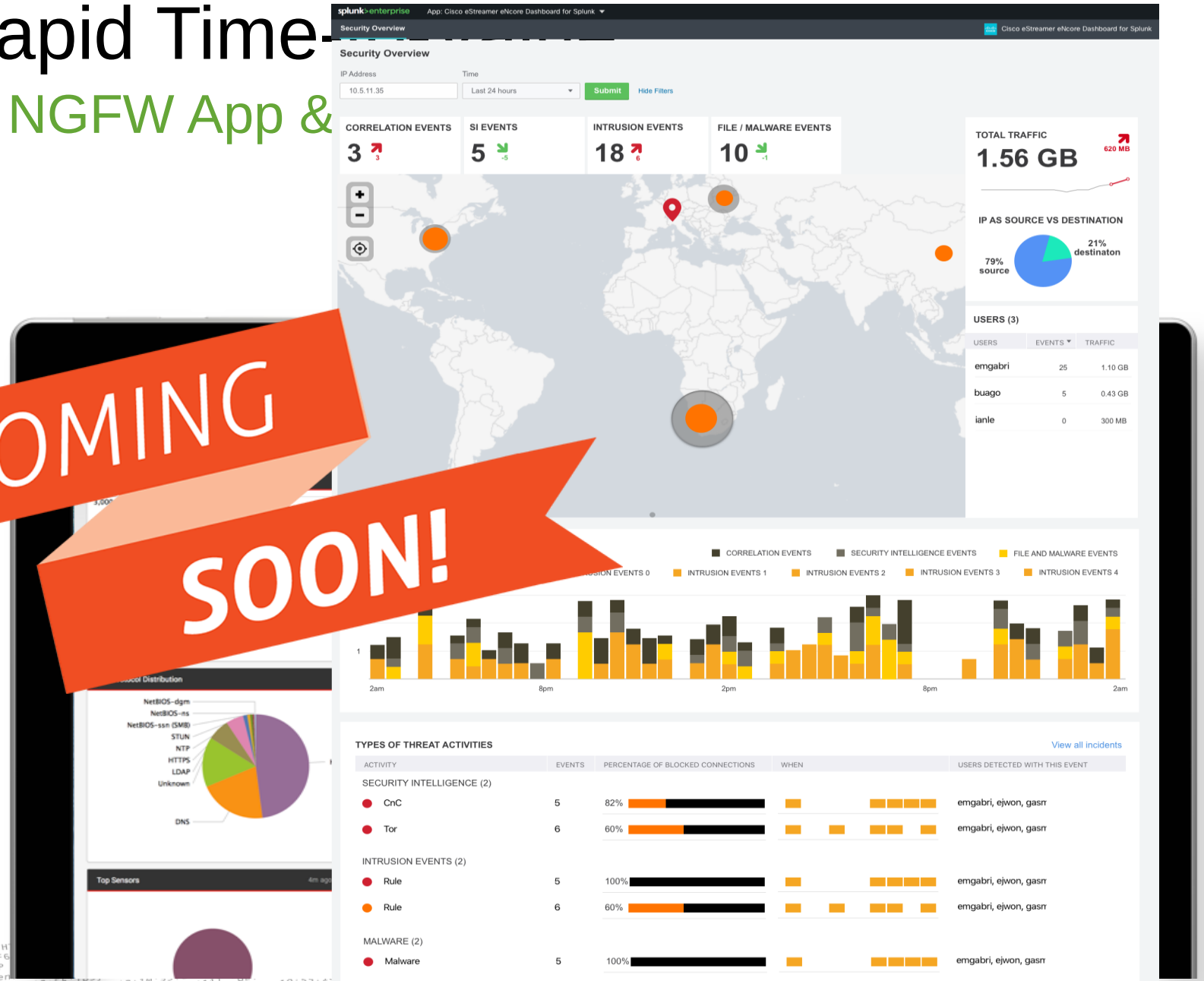
Focus and Speed Investigations



Rapid Time-

Cisco Firepower eNcore NGFW App &

- Drill into dashboard components to access underlying event source data in complete detail
- Fully conduct comprehensive forensics investigations across historical data
- Compliance reporting acros historical data
- Pinpoint trends and set poli based on historical trends
- Easily integrate with existing SOC processes
- Most comprehensive integration across many data sources
- Proven across 100s of deployments
- 24X7 support via Cisco TAC (optional)



ASA and Firepower Data Co-Existence in Splunk

Get all your ASA Firewall data and more into Splunk…eases migration

Access Firewall & System Events

Layer 3 & 4 ACL events
5 tuple, NAT, Routing
System health, HA

Application & Identity Firewall Events

Application inventory, white/blacklist events, URLs
Identity attribution
Discovery events (Host profiles, IOC, port, etc.)

Threat & Correlation Events

IPS events with packet data
Malware disposition, AMP endpoint data
Correlated events and flow data with
Talos & 3rd-party threat intelligence

ASA Splunk Add-On

Firepower Splunk App

Firepower Splunk App

Firepower Splunk App

splunk> .conf18

Cisco Firepower NGFW and Splunk Enable the Business

splunk>

Stop more threats

Gain more insight

Detect earlier, act faster

Reduce complexity

Get more from your network

Continuous Monitoring/ Alerting

Incident Management

CSIRT

Security Compliance

How to get started…

Install Cisco Firepower Add-On & App from Splunkbase:
https://splunkbase.splunk.com/app/3663
https://splunkbase.splunk.com/app/3662

Learn More:

Integration at-a-glance - http://bit.ly/splunk-firepower

Video demo - http://bit.ly/splunk-firepower-demo

See a live demo or theater presentation at the Cisco booth

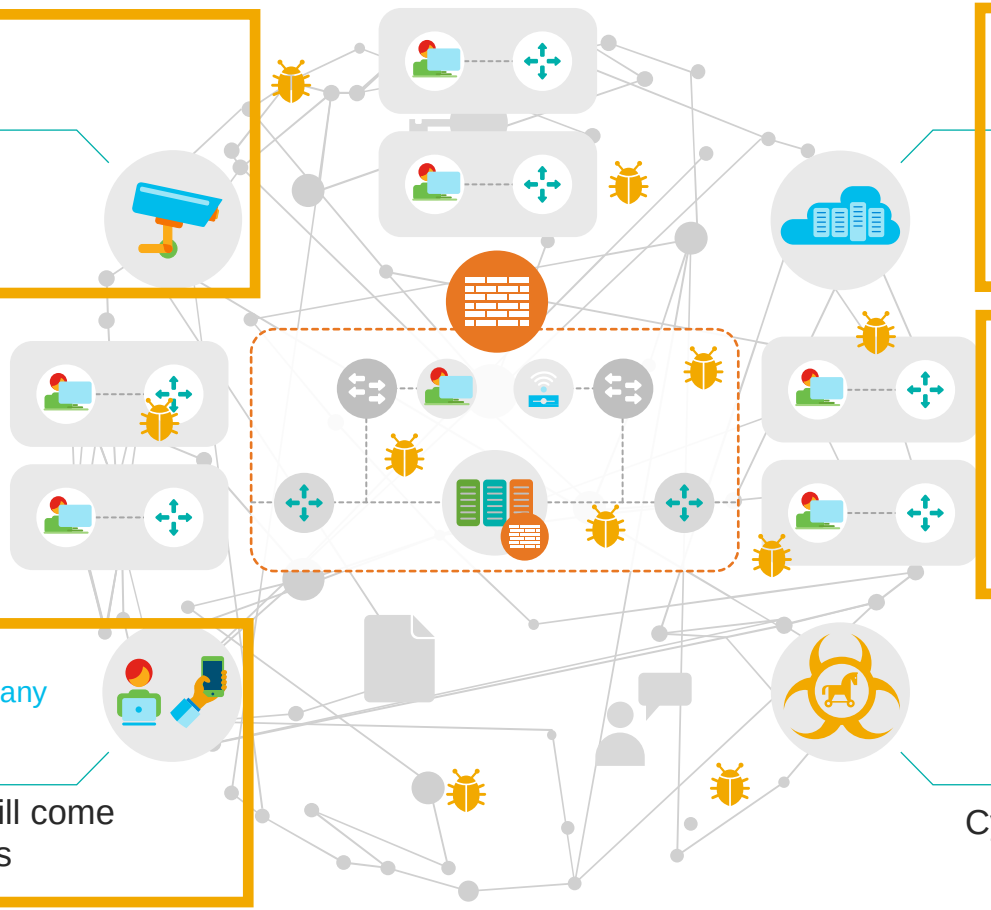
“The Endpoint is the New Perimeter…”

A New Era for the Security Perimeter

"There is No Perimeter"…aka "The Perimeter is Everywhere"

More devices connect everyday

1 million new devices will go online every hour by 2020



Workloads and apps are shifting **to the cloud**

83% of enterprise workloads will be in the cloud by 2020

Direct internet access at distributed branches

By 2020, >60% of enterprises will have deployed DIA

Users work from anywhere across many devices

By 2020, 2/3rds of all IP traffic will come from wireless and mobile devices

Threats are more numerous and persistent

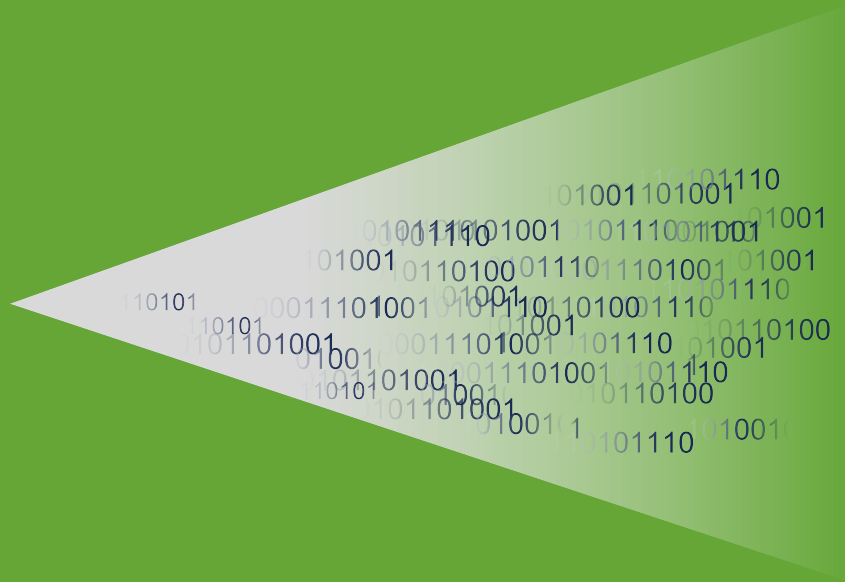
Cyber crime damage costs to hit **$6 trillion annually** by 2021

Endpoint-Related

splunk> .conf18

Customer Problem – Endpoint Blindness
Malware Detection ≠ Endpoint Visibility

User/Device



Malware Activity

Enterprise Resources

SaaS & Shadow IT

Info Security

Traffic/Use Pattern Analysis

AnyConnect Network Visibility Module (NVM)

See your endpoint beyond its malware…and see that too

- Enables extensive behavioral visibility and analytics across users, endpoints, applications and privileges
- Collects, caches, exports IPFIX (NetFlow) from the endpoint when on and off-prem
- Leverages existing AnyConnect VPN client footprint on endpoint
- Excludes select variables to meet privacy requirements

Critical Endpoint Questions NVM Helps Answer...

Data leakage, unapproved apps/SaaS, security evasion…& early malware detection

What endpoints have known bad files, applications, or talking to bad domains?

Has user privilege escalated on any devices?

What apps/processes are running at root (but shouldn't be)?

What SaaS services are in use?

Are endpoint processes uploading/downloading files that match against known hashes?

Why someone is connecting so many times to a destination?

Are unusual processes running on an unusual ports? (eg SMTP on wrong port)

What devices and OSs are on my network?

Where is my endpoint traffic going? Is anything evading the corporate network?

Where are the leak-paths in my network?

Is someone hoarding data to steal or share?

Who is connecting to untrusted networks?

What is making connections to LDAP?

Did any users' behaviors change?

Can I prove that personal data was deleted after processing was done?

<<Waiting on BOTS Slide from Jae Lee at Splunk>>

splunk> .conf18

Network Visibility Module: "How it Works" Example

Application – User – Device – Location – Destination

- IPFIX-Based Record (Source IP, Destination IP, etc)
- Unique Device ID (correlate records from same endpoint device)
- Device Name (bsmith-WIN) and OS Version (Window 7)
- Domain\User Name (AMER\bsmith)
- Local DNS (starbucks.com),Target DNS (-> amceco.box.com)
- Interface (Intel (R) Dual Band Wireless)
- Process/Container Name (iexplorer.exe), Process ID (hash)
- Parent Process Name (foobar.exe) Parent ID (hash)

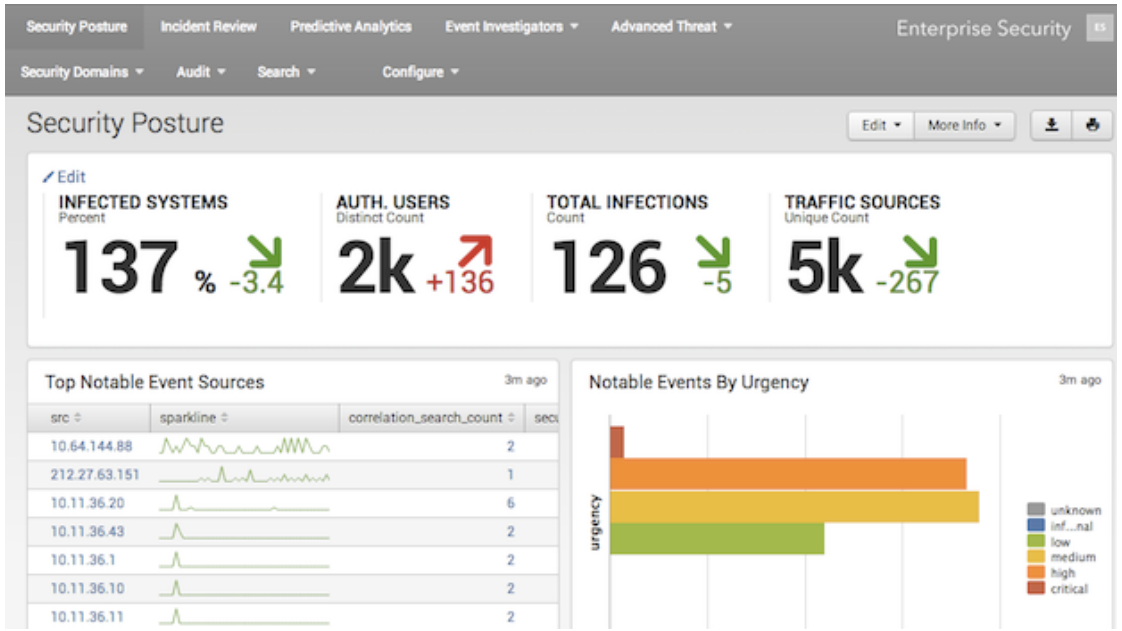
New Cisco Specific Attributes =

splunk> .conf18

Cisco AnyConnect NVM + Splunk Analytics

Drawing Conclusions from Data

Data from AnyConnect NVM (Windows, OS X, Knox/Android)



Data Ingested & Analyzed in Splunk to Provide Insight

splunk> .conf18

How to get started…

Install Cisco AnyConnect NVM App from Splunkbase:

https://splunkbase.splunk.com/app/2992/

Demo video: http://bit.ly/splunk-nvm-demo

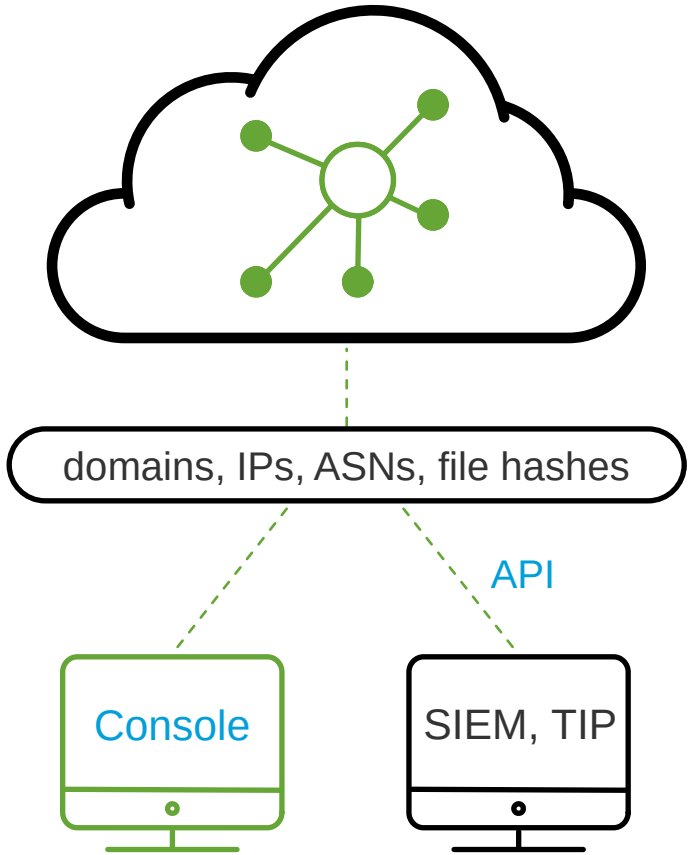
SEC1378 - Splunking the Endpoint IV: A New Hope
Wednesday, Oct 03, 3:15 p.m. - 5:15 p.m.
James Brodsky, Sr. Security Specialist Manager, Splunk

Learn More:

- Check out the Boss of the SOC for AnyConnect NVM content
- Deployment guide - http://bit.ly/splunk-nvm-deploy

Automating On/Off-Network Threat Intelligence to Better Prioritize Threats

Investigate: a Powerful Way to Uncover Threats



Key points

Intelligence about domains, IPs, and malware across the internet

Live graph of DNS requests and other contextual data

Correlated against statistical models

Discover and predict malicious domains and IPs

Enrich security data with global intelligence

Umbrella's View of the Internet

100B
requests per day

85M
daily active users

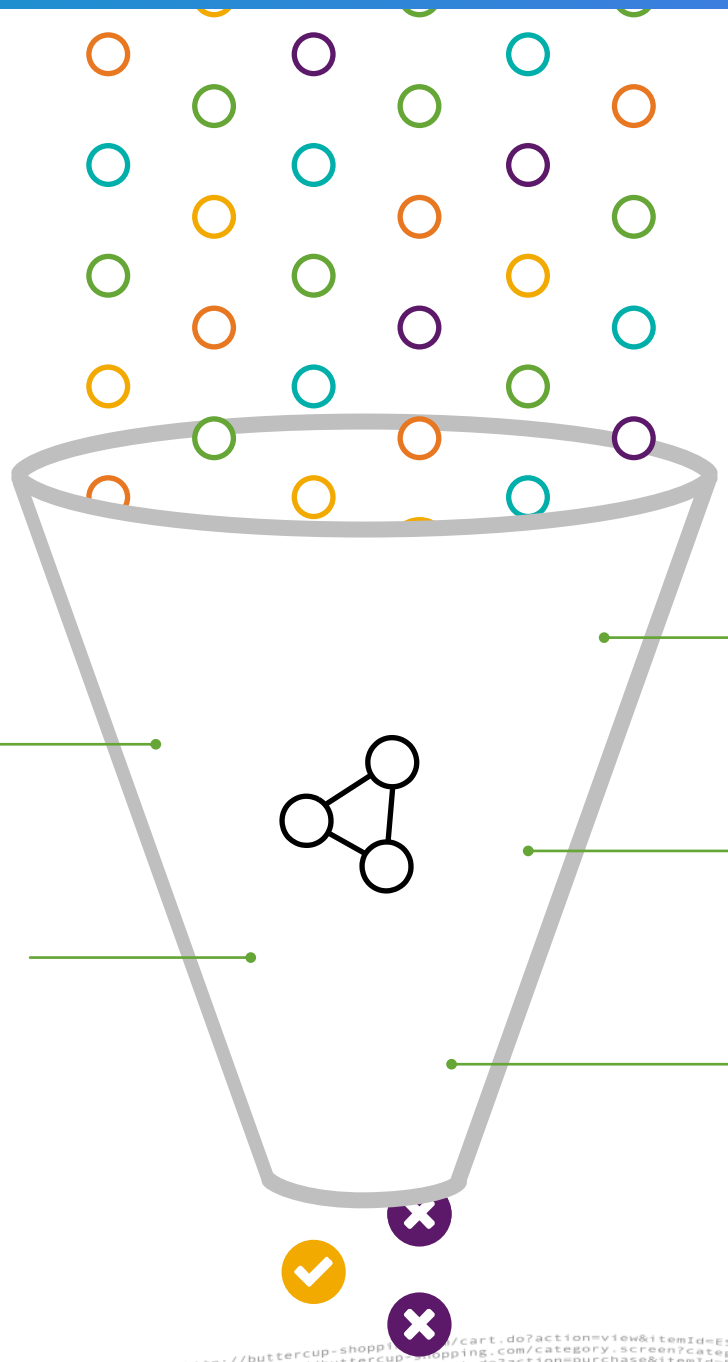
12K
enterprise customers

160+
countries worldwide

splunk> .conf18

Intelligence

Statistical models



2M+ live events per second

11B+ historical events

Co-occurrence model

Identifies other domains looked up in rapid succession of a given domain

Natural language processing model

Detect domain names that spoof terms and brands

Spike rank model

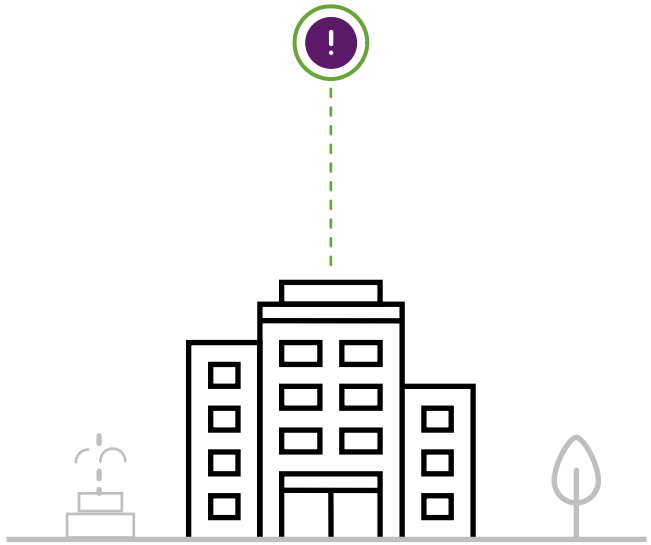
Detect domains with sudden spikes in traffic

Predictive IP space monitoring

Analyzes how servers are hosted to detect future malicious domains

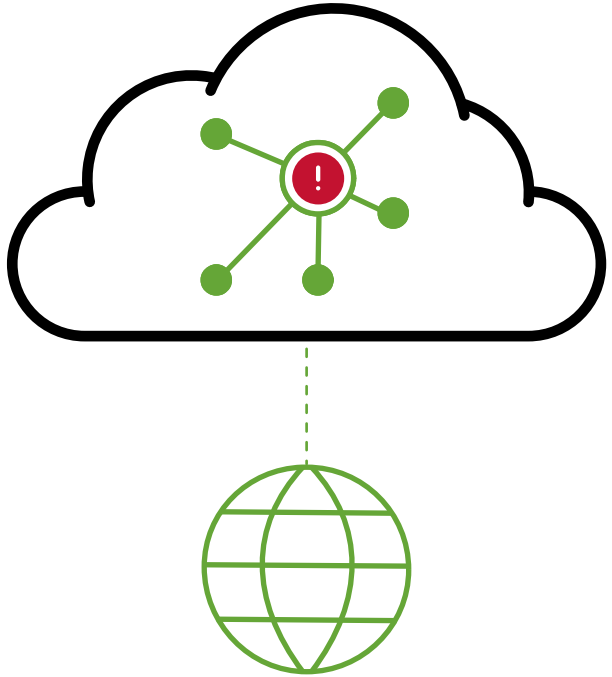
Dozens more models

You know one IOC



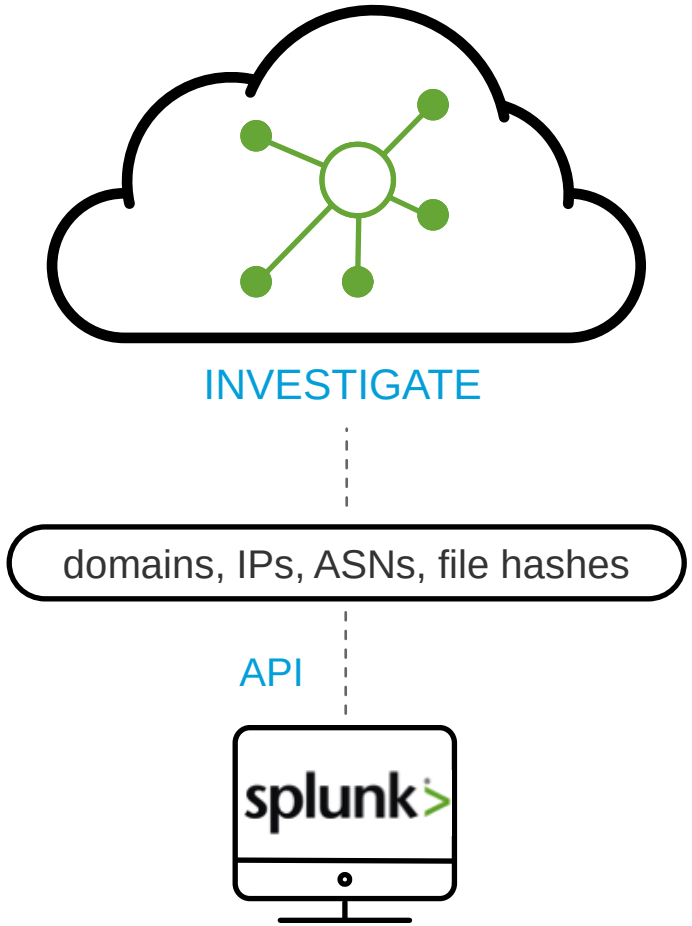
Your local intelligence

We know all its relationships



Our global context

Splunk Add-on for Cisco Umbrella Investigate



Automatically enrich security alerts inside Splunk, allowing analysts to discover the connections between the domains, IPs, and file hashes in an attacker's infrastructure.

Key Benefits of Splunk Add-on for Cisco Umbrella Investigate

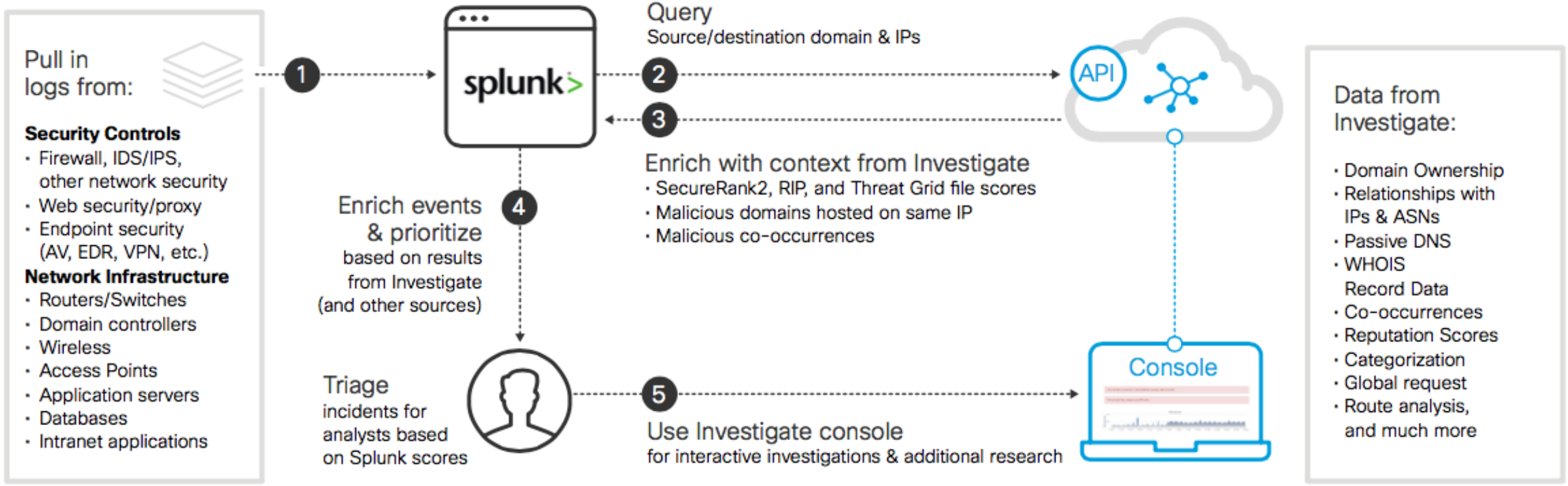
Complete view of an attack

Better prioritize incident response

Uncover missing connections

Speed up investigations

How It Works



splunk> .conf18

How to get started…

Install Cisco Umbrella Investigate Add-On from Splunkbase:
https://splunkbase.splunk.com/app/3324/
See a live demo at the Cisco booth

Come see detailed Umbrella Investigate+Splunk .conf session:
Anatomy of an Attack, and Staying Ahead with Cisco and Splunk
Thursday @ 12:30 pm

Learn More:
Umbrella Investigate at-a-glance - http://bit.ly/splunk-umbrella
Video demo - http://bit.ly/splunk-umbrella-demo

Key Takeaways

1. Perimeter = edge, endpoint, on-net, off-net…everywhere

2. Firewalls need to be threat perimeters, not just access control…and feed that threat telemetry to your Splunk instance

3. With a 130+ million AnyConnect clients installed, chances are many of you have it. Use the built-in NVM telemetry with Splunk for endpoint visibility.

4. Umbrella provides a good dimension for feeding new types of telemetry to your Splunk analysis…helps complete the picture

Thank You

Don't forget to rate this session in the .conf18 mobile app