



Solving Endpoint Security & Perimeter Blindness with Splunk

Lessons from Cisco's Internal InfoSec Deployment

Scott Pope
Director – Security Product
Management | Cisco Systems

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

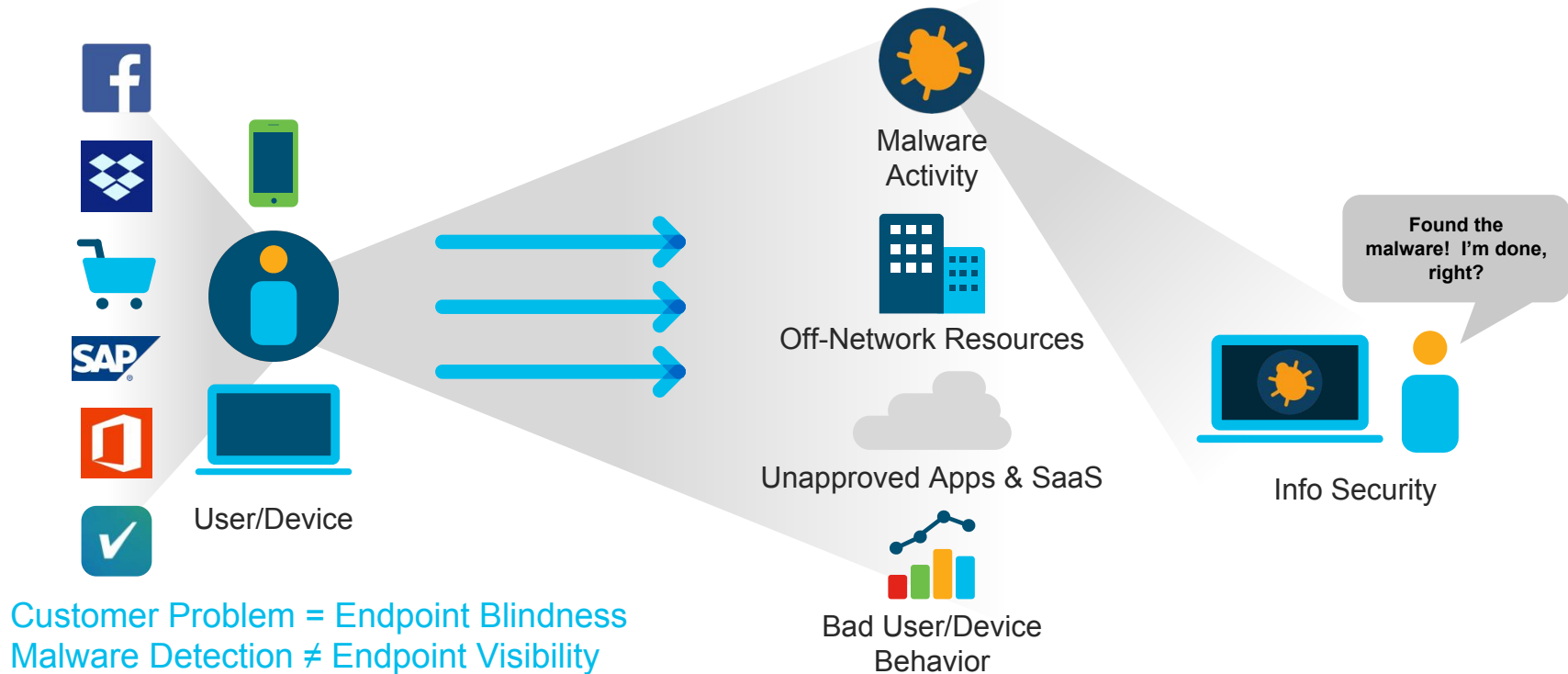
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Agenda

- It's not just malware – many bad things happen on endpoints
- Cisco's endpoint challenges probably look like yours
- Solving endpoint security woes using your existing Splunk & Cisco infrastructure
- Extending those concepts to your perimeter security

The Endpoint Security Gap:

There's lots of bad stuff that happens on endpoints besides malware



Cisco InfoSec Team's Endpoint Visibility Challenges

- Tracking the behavior of users and endpoints
- Getting a real-time view of endpoint assets & footprints
- Detecting insider threats and unknown malware
- Zero-trust – how to monitor endpoints off the network

□ *Doing all of this at scale*

□ *Doing all of this without duct-taping 7 different IT systems together*

You can try to improvise a system, but
results may vary...

You can try to improvise a system, but results may vary...



Step 1: Generate Comprehensive & Consistent Endpoint Telemetry

Cisco AnyConnect Network Visibility Module (NVM)

- 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

Cisco's VPN client, AnyConnect, also provides deep endpoint telemetry



AnyConnect – The Endpoint Visibility it Provides...

Netflow/IPFIX

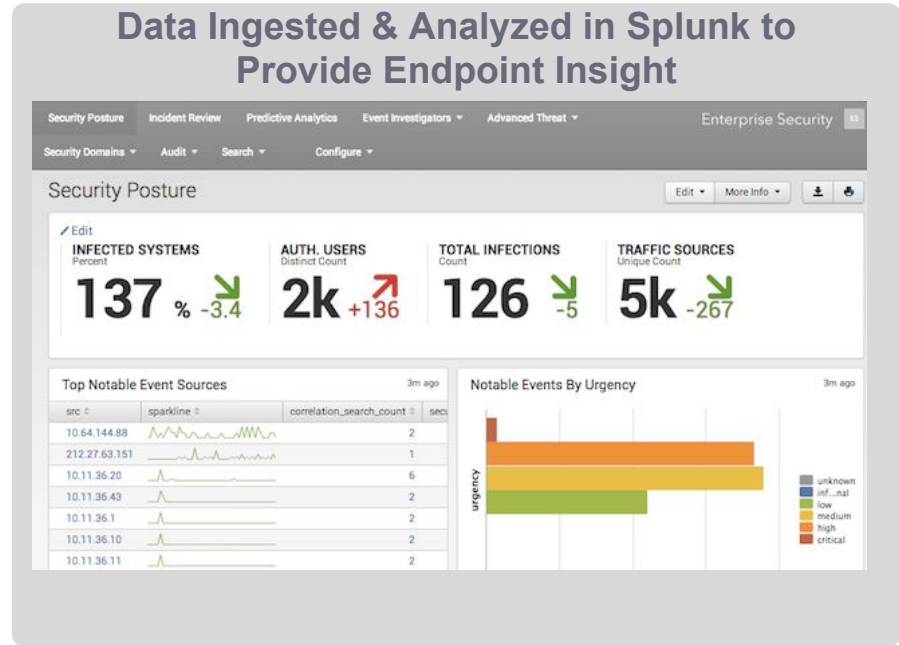
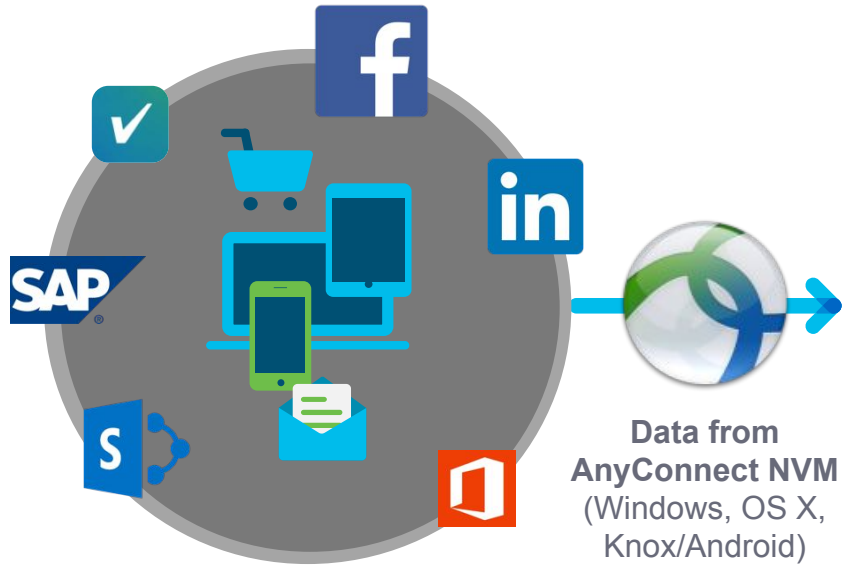
Source IP	Source IP
Destination IP	Destination IP
Source Port	Source Port
Destination Port	Destination Port
Bytes Sent	Bytes Sent
Bytes Received	Bytes Received
	OS Version
	OS Edition
	UDID
	Host Name
	Logged In User
	Process Name
	Process Hash
	Process Account
	Parent Process Name
	Parent Process Hash
	Parent Process Account
	DNS/Destination Hostname
	Module Hash List
	System Manufacturer
	System Type
	MAC Address
	Interface Name / Type / UID

AnyConnect NVM
(IPFIX Formatted)

Deep Endpoint Visibility

User
Traffic Stats
Processes
Applications
SaaS Used
Accounts
Destinations
Machine Details

Step 2: Analyze the AnyConnect Endpoint Telemetry...in Splunk



Step 3: How to Size this in Your Splunk Licensing

Usual Considerations

- How much data will my endpoints produce?
- Aren't endpoints thirsty? How do I size my Splunk license for that?

Introducing Cisco Endpoint Security Analytics Built on Splunk

- Priced per endpoint
- Predictable budget
- Don't need to figure out "how much data will my endpoints produce"
- Affordable – about 25-35% of the cost of typical anti-malware



CESA Built on Splunk – The Product Basics

- Sold through Cisco and Cisco channel
- AnyConnect NVM data is identified by Splunk and priced differently than other data
- Does not utilize Splunk data volume license in any way
- Solution tech support by Cisco and Splunk
- Works with existing Splunk deployments or as stand-alone deployment

Example CESA Detection & Visibility Use Cases

Unapproved Applications & SaaS	• SaaS domains accessed – connections & SaaS use behavior • Application & process visibility – find apps/processes running on devices
Security Evasion & Attribution	• Endpoint security applications – detect if disabled or not installed • CESA – detect if disabled or not installed • Attribute user to network access – user activity down to NIC level
Day-Zero Malware & Threat Hunting	• Unusual app/process behavior – running at root or on non-standard ports • C&C detection – burst of connections to new, unusual or bad domain • Threat detection – application process to host domain correlation
Zero-Trust Monitoring	• Off-net device monitoring – user, device, traffic, app & data behavior • SaaS use behavior – track SaaS services are being used • Untrusted connections – track who is connecting to untrusted networks
Data Loss Detection	• Data hoarding activity – download & upload behavior • Exfiltration – upload to external domains & network shares
Asset Inventory	• Device-type and OS inventory – identify & report by type • Data privacy compliance – confirm removal of personal data from devices

Taking Action on Threats & Compliance Issues Found by CESA

Threats & Compliance Issues
Detected by CESA

Remediation & Response Actions

Data Loss Detection

Unapproved Applications & SaaS

Security Evasion & Attribution

Day-Zero Malware & Threat
Hunting

Zero-Trust Monitoring

Asset Inventory



Cisco ISE

Rapid Threat Containment
from CESA/Splunk Console



User/Device Investigation
and Quarantine



Cisco Umbrella

Enforcement from
CESA/Splunk Console



Blocks Malicious Destinations

COMING
FALL
2019



Cisco AMP

Endpoint Enforcement
from AMP Console



Endpoint File Revocation,
Process Termination

“We had no solution for 80% of these endpoint security use-cases before this solution...”

Imran Islam, Cisco CSIRT (incident response team)

Cisco InfoSec Team's Endpoint Visibility Challenges

Met with CESA Splunk

- ✓ Tracking the behavior of users and endpoints
- ✓ Getting a real-time view of endpoint assets & footprints
- ✓ Detecting insider threats and unknown malware
- ✓ Zero-trust – how to monitor endpoints off the network

- *All done at 100K+ endpoint scale*
- *Single reliable system of consistent data and endpoint visibility*
- *Reduced incident investigation time from days to hours*

Next Steps on CESA Splunk

- Learn more at cisco.com/go/cesa
- Check out the Cisco InfoSec case study at above link
- If you already have Splunk & AnyConnect, try it out:
 - Download & install the Cisco AnyConnect NVM App for Splunk from Splunkbase to create dashboards
 - Download & install the Cisco NVM Technology Add-On for Splunk from Splunkbase to bring NVM data into Splunk
 - Turn on NVM telemetry in your AnyConnect environment as outlined in [tech docs](#)

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

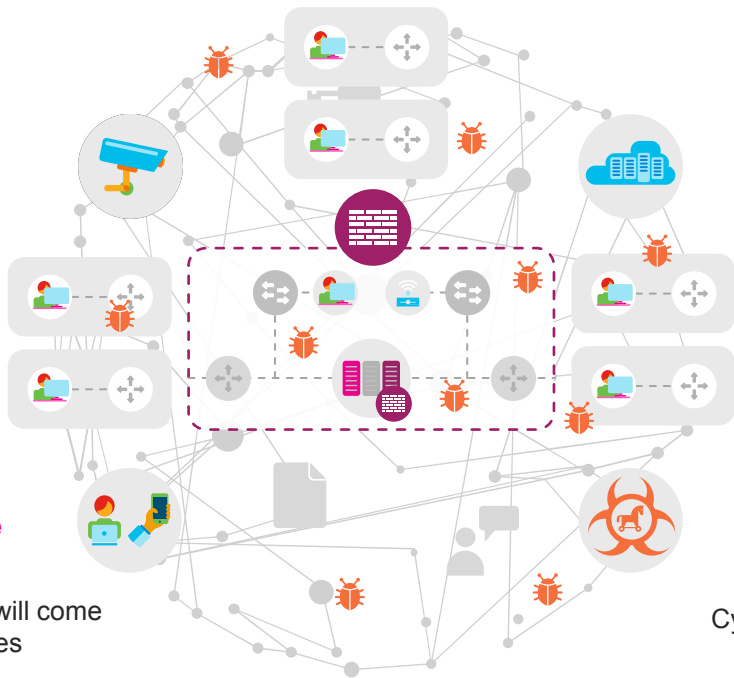
By 2020, >60% of enterprises will have deployed DIA

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

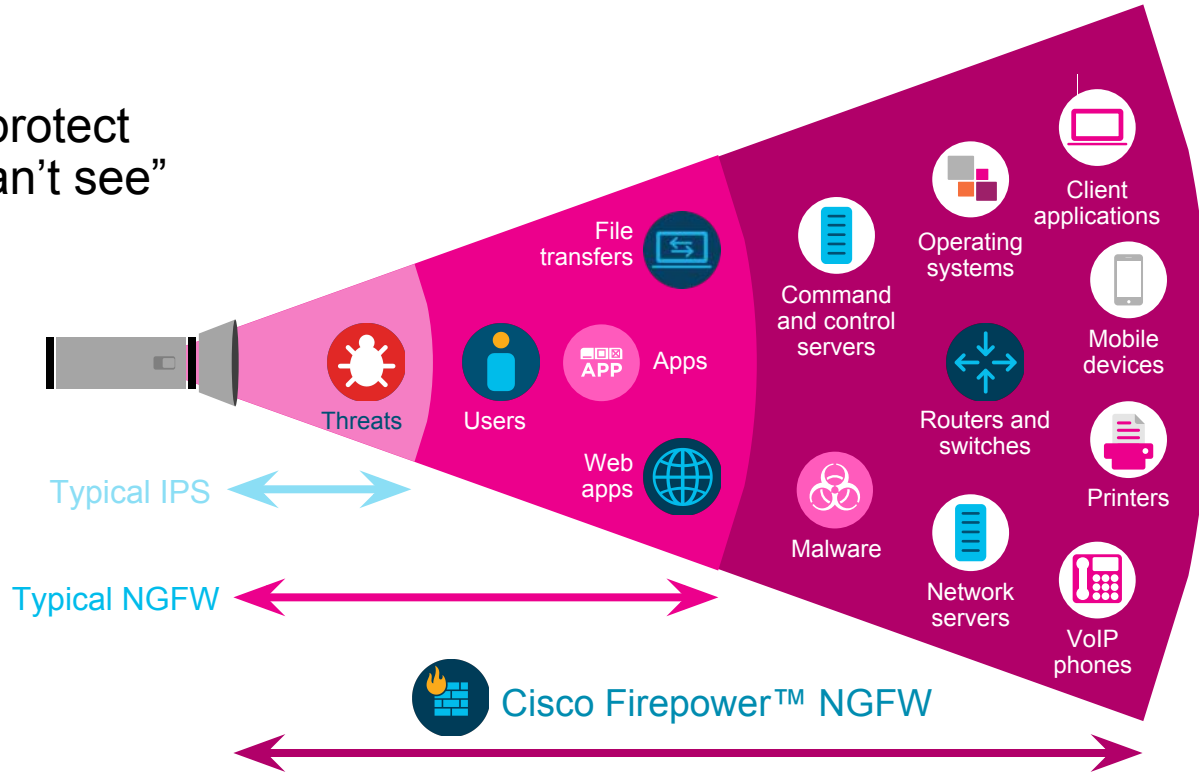


Get control of the extended perimeter by...

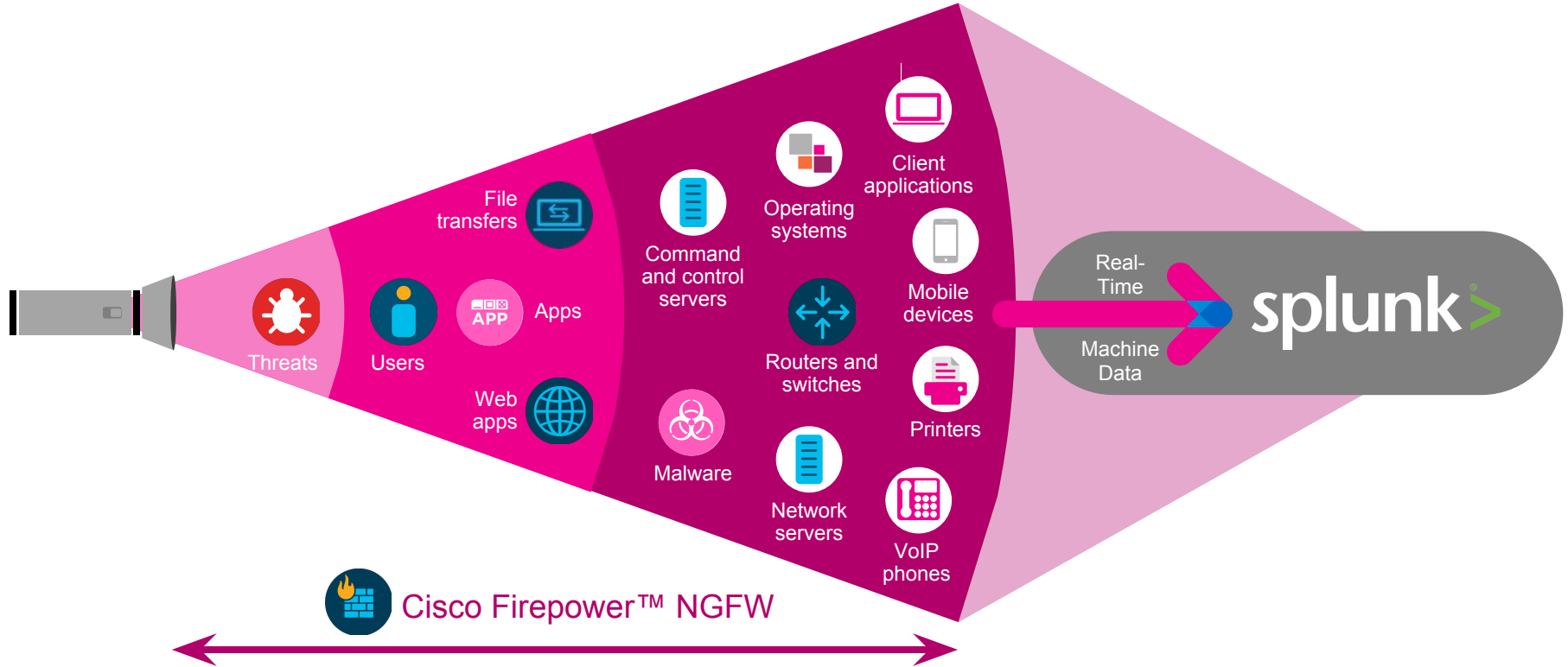
- Making the firewall access control perimeter into a threat control perimeter

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

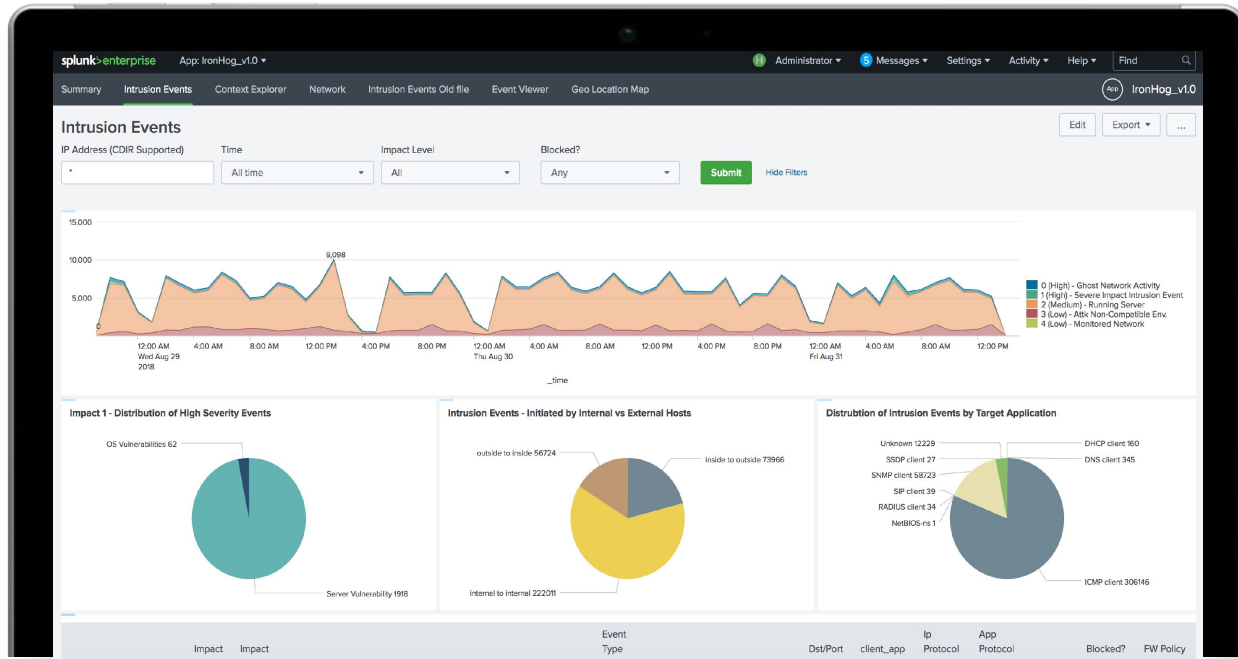
Pat touched ABC malware,
tripped ABC IPS sigs and
was denied access to XYZ
network segments associated
with “Hi Value” FW policy
when using unapproved
application via an allowed
URL. Packet data was
captured for analyzing this
event. Talos and partner
threat intel has been
associated with the event.

Rapid Time-to-Value

Cisco Firepower 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



Splunk Integration Across Cisco Security Platforms

Connect the threat event dots across vendors and manage your Cisco Security events

AMP

NVM

Threat Grid

Umbrella

ISE



splunk>

Enhance Splunk threat visibility with unique Cisco security telemetry



splunk>

Excellent event visibility from your existing Cisco Security infrastructure



Firepower & ASA & CES WSA & CWS Threat Response

Q&A

.conf19
splunk>





**Thank
You!**