Pervasive Security for Higher Education

Cisco's Architectural Approach

Justin Malczewski

Regional Manager, Security Solutions

April 26, 2017

Play the Video:
“Anatomy of an Attack”

https://youtu.be/4gR562GW7TI

A New Era in Higher Education Cybersecurity

Cybercriminals exploit the spirit of **trust and openness** inherent in the Higher Education community, targeting its rich troves of **research data**, **intellectual property**, and **personally identifiable information**. Some attacks are highly sophisticated, while others are simple but effective like legitimate-looking emails that link to advanced malware that compromises critical hosts. Today's cybersecurity risks extend well beyond direct information loss into **reputation damage**, **negative press**, and **future revenue loss**.

Important questions higher-ed should be asking:

- What are you trying to protect?
- Who is your adversary?
- Do you have a framework you follow and how do you measure your maturity?
- What is your risk tolerance?
- How mature do we need to be based on our risk profile?

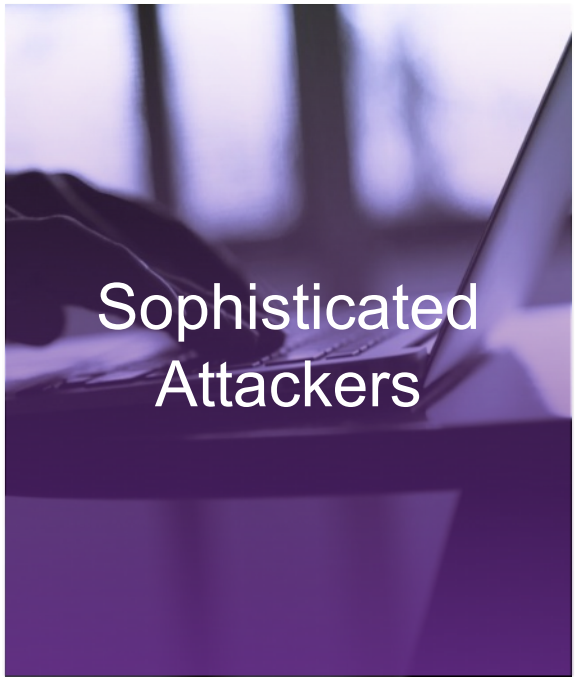
Asymmetric warfare: a conflict between opposing forces which differ greatly in power and that typically involve the use of unconventional weapons and tactics…

The Security Effectiveness Gap

Goal for Effective Security

Any Worthwhile Journey can be a challenge….

Complexity: Are We Secure Yet?

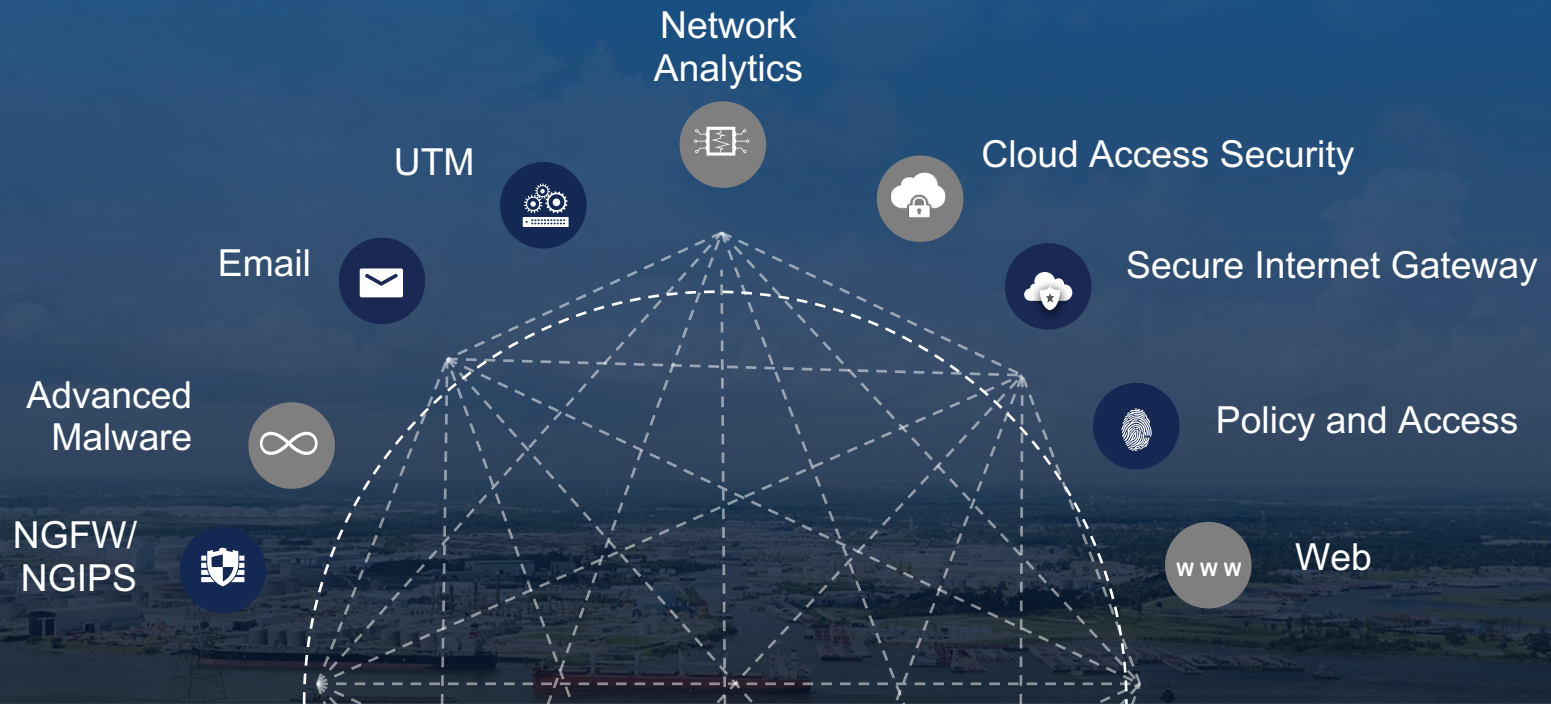


Cisco: Uniquely Positioned to Deliver

Reach: Powering Visibility Everywhere

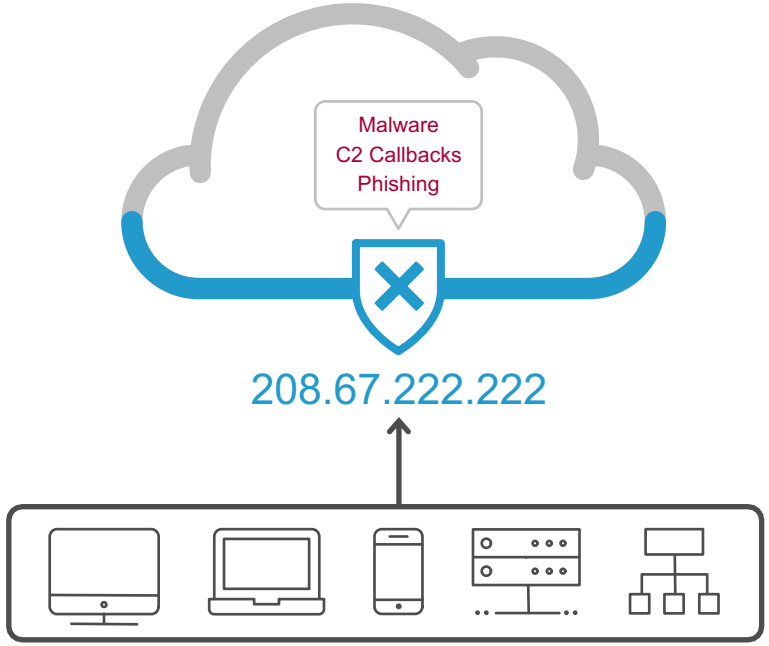
Premiere Portfolio in the Industry

Best of Breed and Integrated Architecture



Umbrella

The fastest and easiest way to block threats

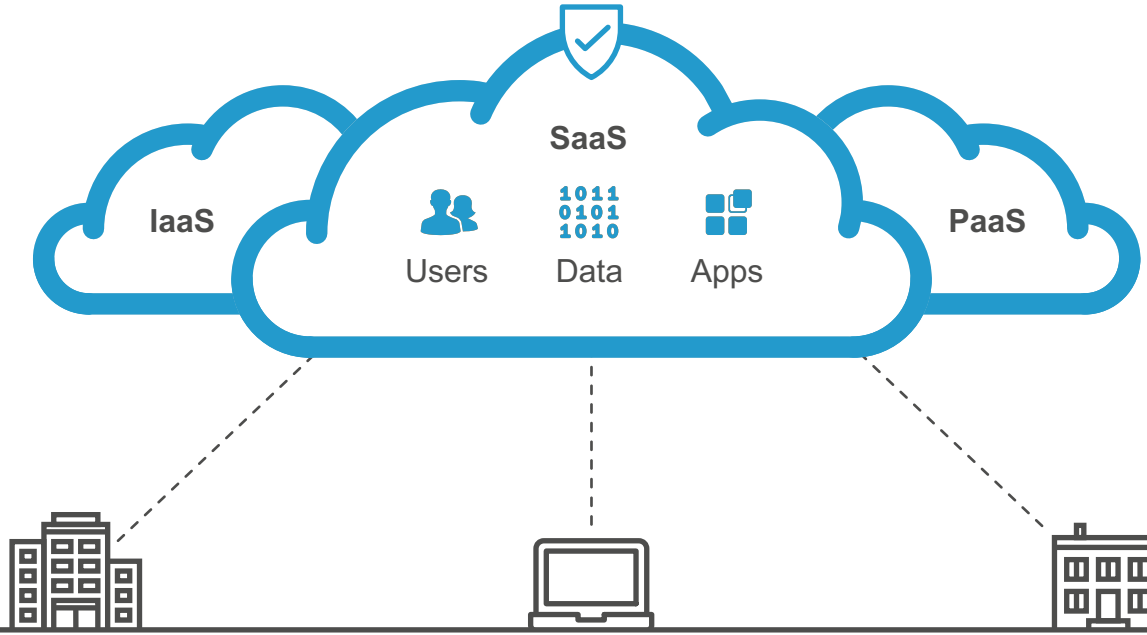


Key points

- First line of defense against threats
- Visibility and protection everywhere
- Enterprise-wide deployment in minutes
- Intelligence to see attacks before they launch
- Integrations to amplify existing investments

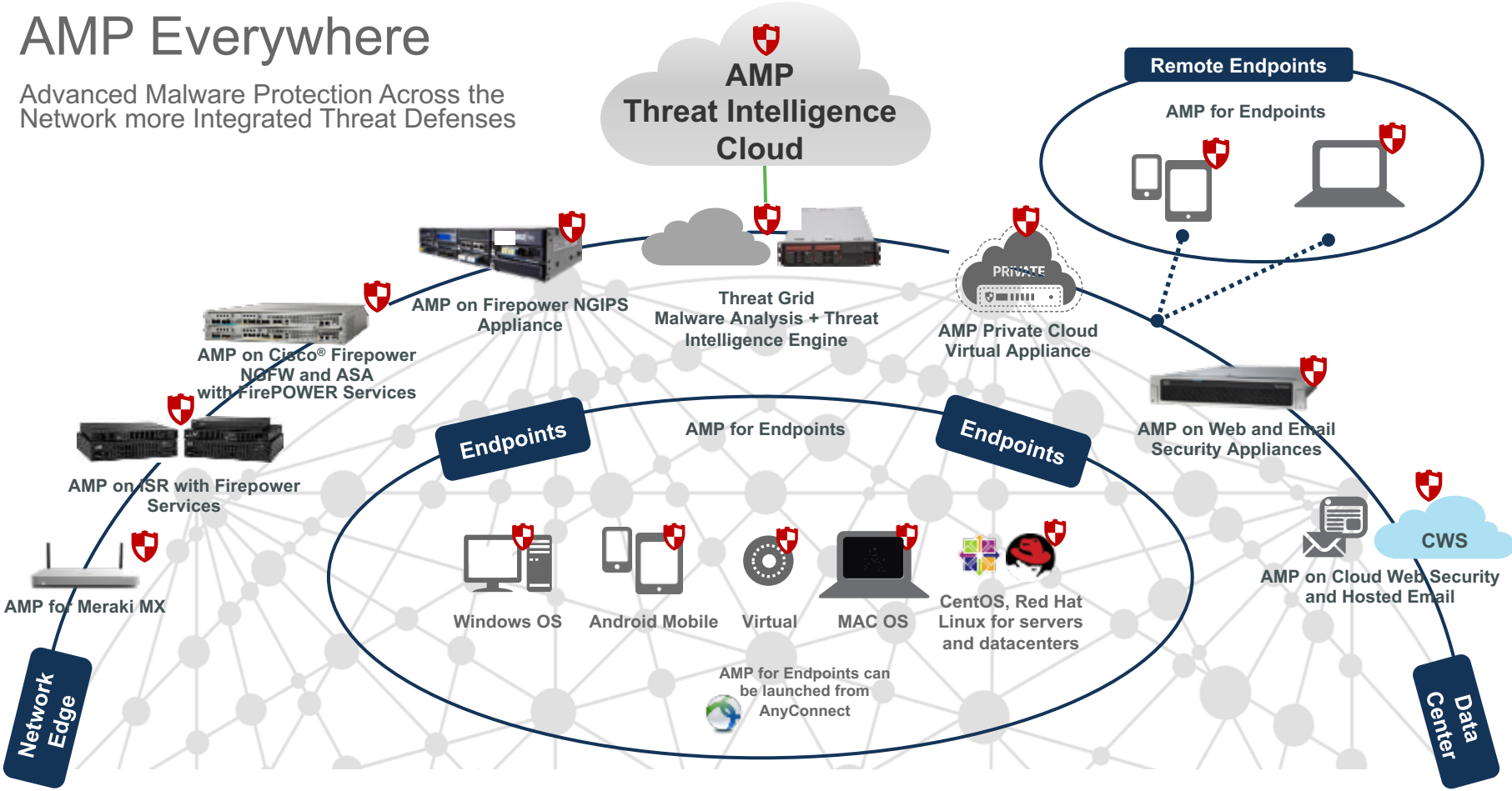
CloudLock

Cloud Access Security Broker (CASB)

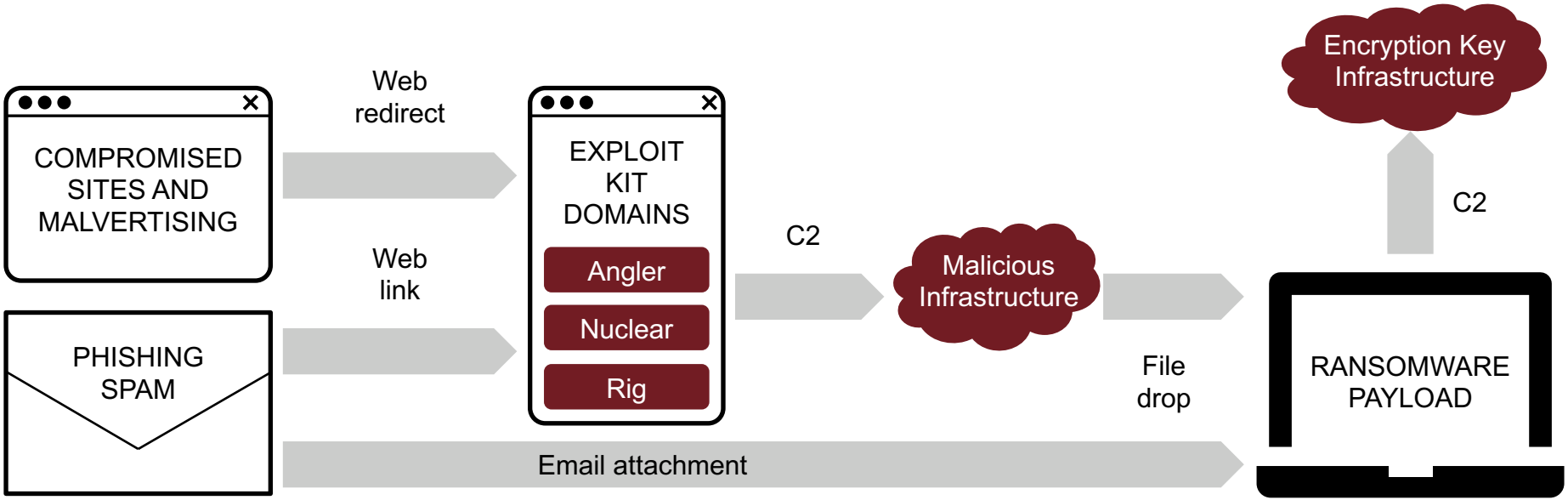


AMP Everywhere

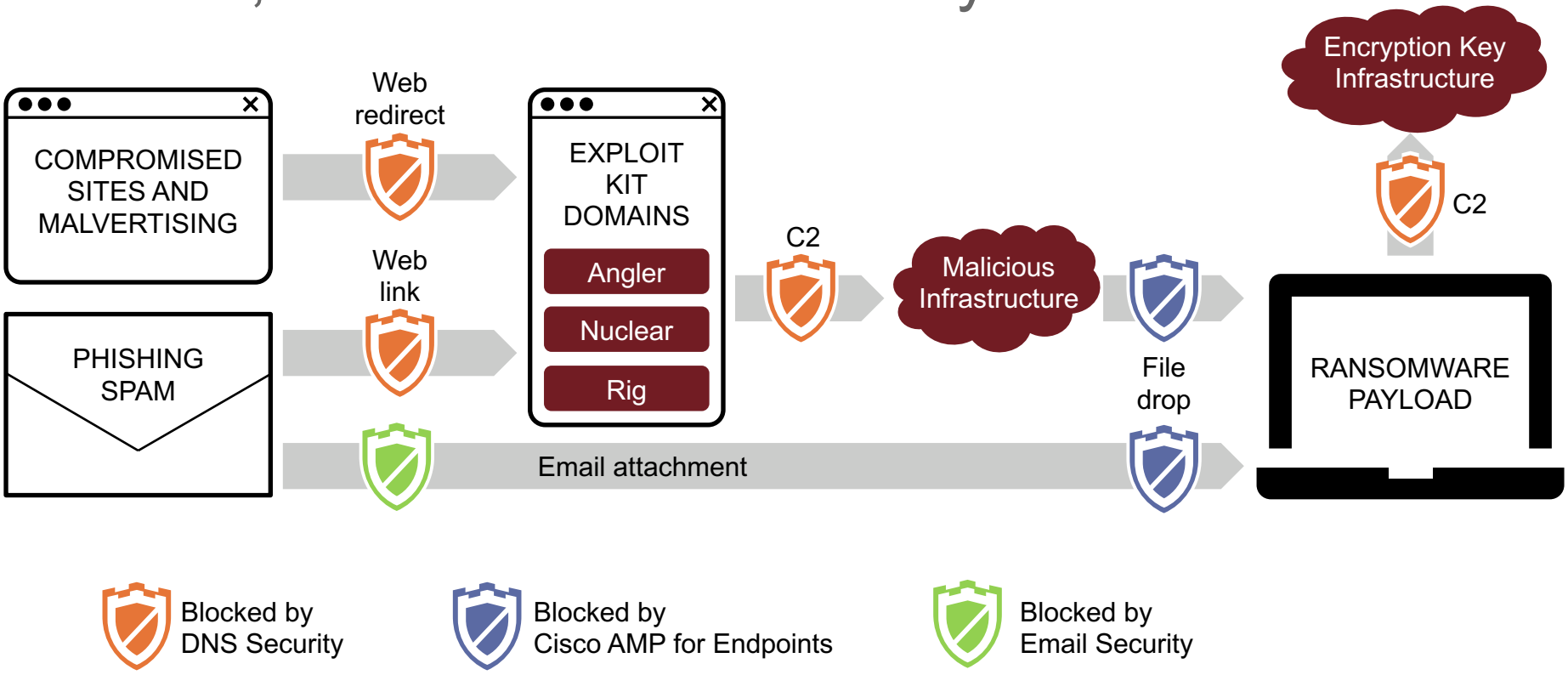
Advanced Malware Protection Across the Network more Integrated Threat Defenses



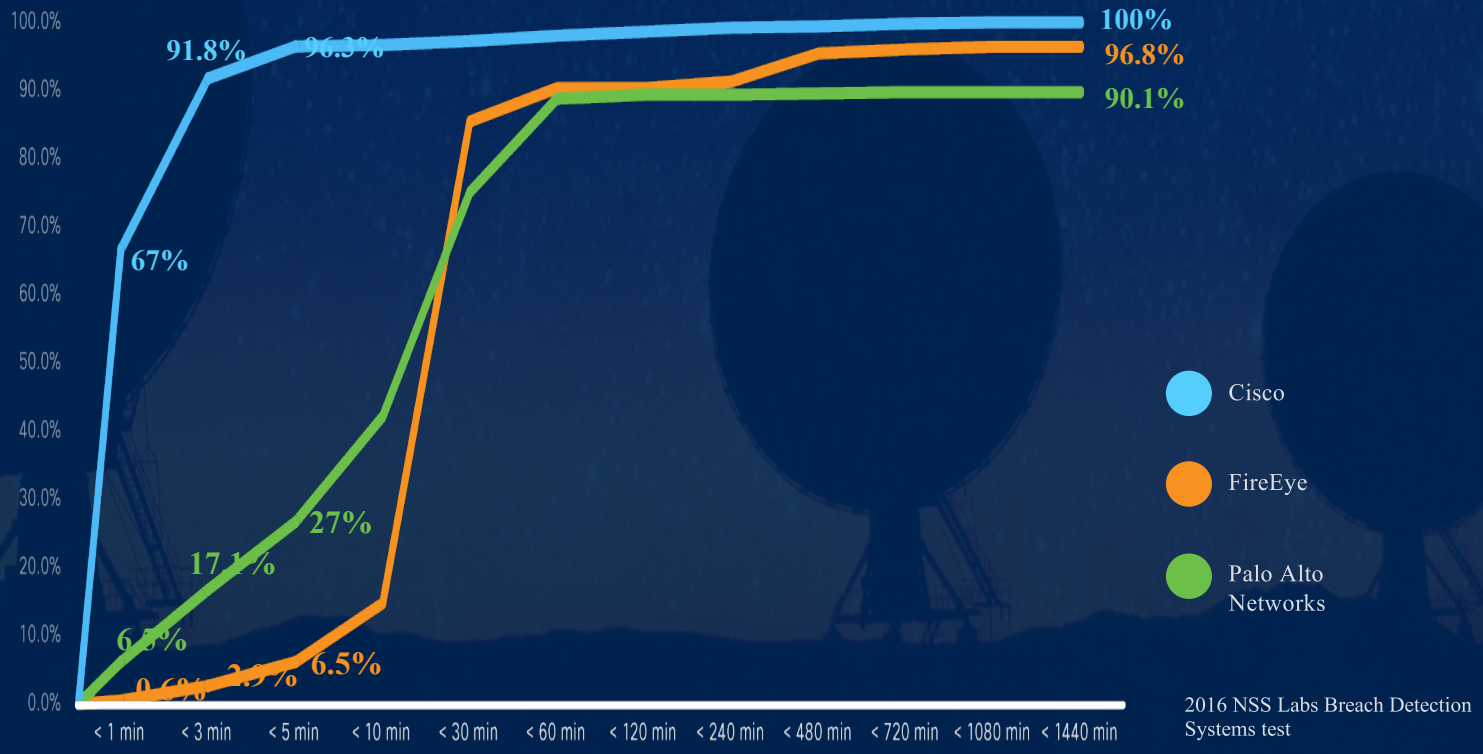
Most Ransomware Relies on C2 Callbacks



Prevent and Contain Ransomware with Umbrella, AMP and Email Security



CISCO LEADS IN BREACH DETECTION



2016 NSS Labs Breach Detection Systems test

Cisco AMP: Leader in Security Effectiveness with Fastest Time to Detection

NSS Breach Detection and Time to Detection Test Results for Cisco

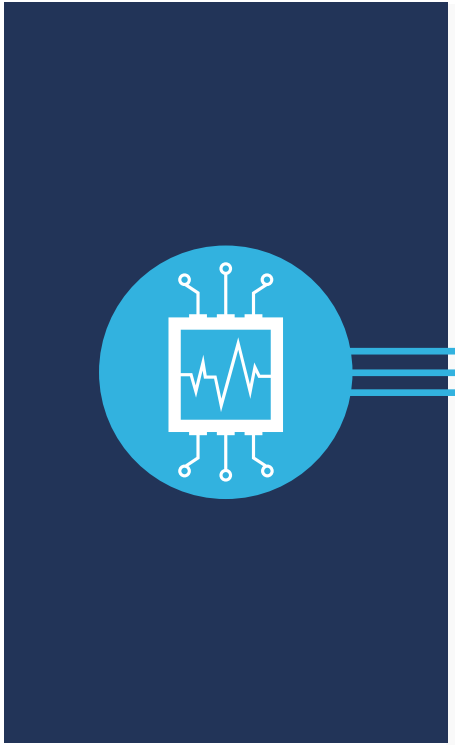
Product				Breach Detection Rate[1]		NSS-Tested Throughput	
Cisco Firepower 8120 with NGIPS v6.0 and Advanced Malware Protection				100.0%		1,000 Mbps	
False Positives	Drive-by Exploits	Social Exploits	HTTP Malware	SMTP Malware	Offline Infections	Evasions	Stability & Reliability
0.33%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	PASS

Detection Time Scoring									
Time to Detect	Product A	Cisco	Product B	Product C	Product D	Product E	Product F	Product G	Product H
<1min	44.40%	67.00%	0.60%	48.90%	46.20%	5.50%	7.30%	6.50%	3.60%
<3min	75.90%	91.80%	2.90%	88.70%	84.20%	31.30%	17.90%	17.10%	26.70%
<5min	86.60%	96.30%	6.50%	91.00%	88.40%	47.80%	27.60%	27.00%	66.20%
<10min	97.40%	96.60%	15.20%	95.60%	91.30%	85.00%	43.10%	42.50%	90.10%
<30min	97.90%	97.10%	85.80%	98.50%	93.10%	96.90%	76.40%	75.40%	94.00%
<60min	98.20%	97.90%	90.80%	98.70%	93.10%	98.20%	97.90%	89.20%	96.30%
<120min	98.50%	98.50%	90.80%	98.90%	94.30%	98.40%	98.50%	89.70%	96.60%
<240min	98.90%	99.20%	91.60%	99.00%	97.60%	98.90%	98.50%	89.70%	96.80%
<480min	99.00%	99.40%	95.80%	99.00%	98.70%	99.40%	98.90%	90.00%	99.70%
<720min	99.20%	99.70%	96.40%	99.40%	98.70%	99.50%	98.90%	90.10%	99.80%
<1080min	99.40%	99.80%	96.80%	99.40%	98.70%	99.80%	98.90%	90.10%	99.80%
<1440min	99.40%	100.00%	96.80%	99.40%	99.00%	100.00%	98.90%	90.10%	99.80%
Overall Detection Score	**99.40%**	**100.00%**	**96.80%**	**99.40%**	**99.00%**	**100.00%**	**98.90%**	**90.10%**	**99.80%**

= > 90%
= 80 - 89%
= 60 - 79%
= 40 - 59%
= < 40%

- The leader for the 3rd year in a row in the BDS test – detecting 100% of malware, exploits & evasions.
- Faster time to detection than any other vendor - blocking 91.8% of attacks in < 3 minutes
- Products with faster detection rates get to green numbers faster moving from top to bottom.
- Products may have the same Overall Detection Score at the bottom, but those with the faster time to detection are more effective – giving attackers less time and space to operate.

Cisco Network as a Sensor (NaaS)

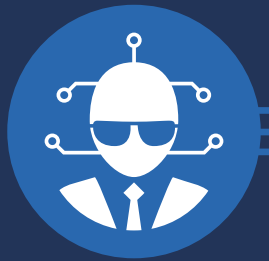


Detect anomalous traffic flows, malware

Identify user access policy violations

Obtain broad visibility into all network traffic

Cisco Network as an Enforcer (NaaE)



- **Implement Access Controls** to Secure Resources
- **Contain the Scope** of an Attack on the Network
- **Quarantine Threats,** Reduce Time-to-Remediation

Cisco Umbrella Proof-of-Value Workshop:

Date: June 2, 2017

Time: 9 am - Noon

Location: Cisco Vancouver Office #2123 – 595 Burrard Street

1. Sign up for Cisco Umbrella Trial using the following link:

http://cs.co/cse-free-trial

2. Email Rob Bleeker to register for the Umbrella PoV workshop:

robleeke@cisco.com

BC AWARE 2018

Date: BC AWARE Day - Jan 30, 2018

Time: 8 am – 5 pm

Location: SFU Downtown Campus

Featuring: A Very Special Guest

ISACA
Trust in, and value from, information systems
Vancouver Chapter

Is your higher-ed institution ready to host a BC AWARE Event?!

If so….

Come see me at Cisco booth!!

Mark Your Calendars!!

www.bcaware.ca