



Industry's First Threat-Focused NGFW

Cisco ASA with FirePOWER Services

Dean Frye
Security Engineering Manager, APJC

Introducing: Cisco ASA with FirePOWER Services

Industry's First Threat-Focused Next-Generation Firewall

Features

- ▶ Cisco® ASA firewalling combined with Sourcefire® Next-Generation IPS
- ▶ Advanced Malware Protection (AMP)
- ▶ Best-in-class security intelligence, application visibility and control (AVC), and URL filtering

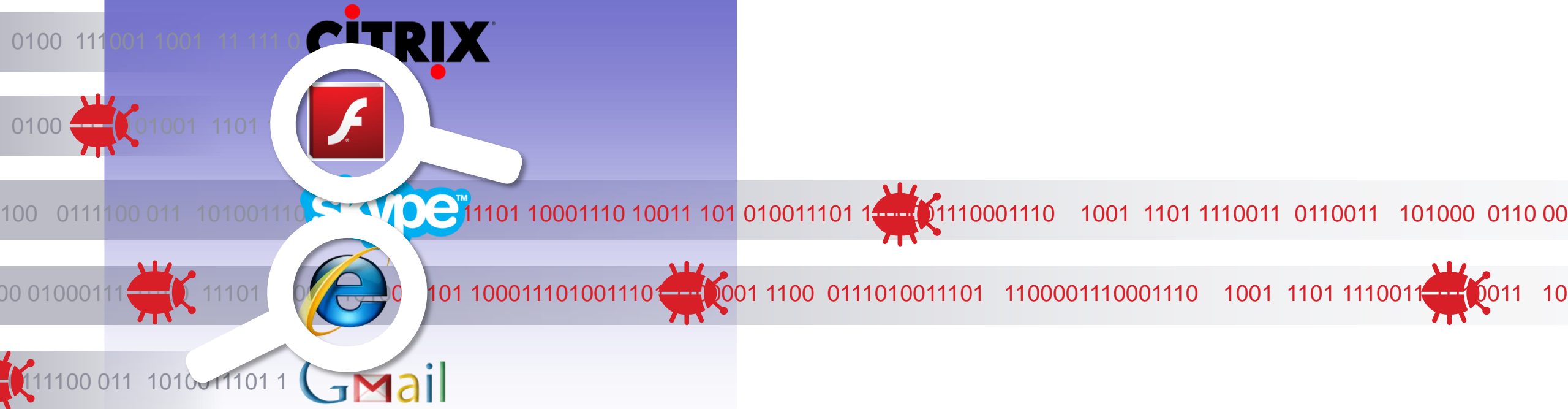
Benefits

- ▶ Superior, multilayered threat protection
- ▶ Unprecedented network visibility
- ▶ Integrated threat defense across the entire attack continuum
- ▶ Reduced cost and complexity



The Problem with Legacy Next-Generation Firewalls

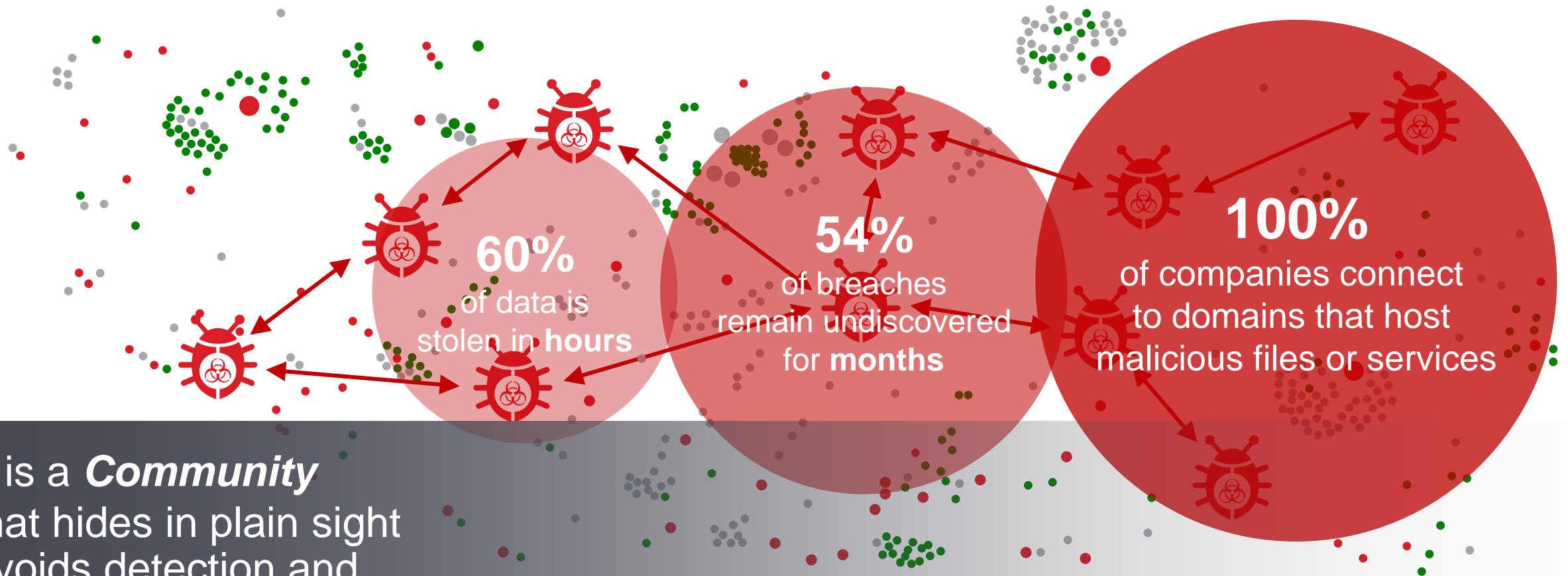
Focus on the Apps



But totally miss the threat...

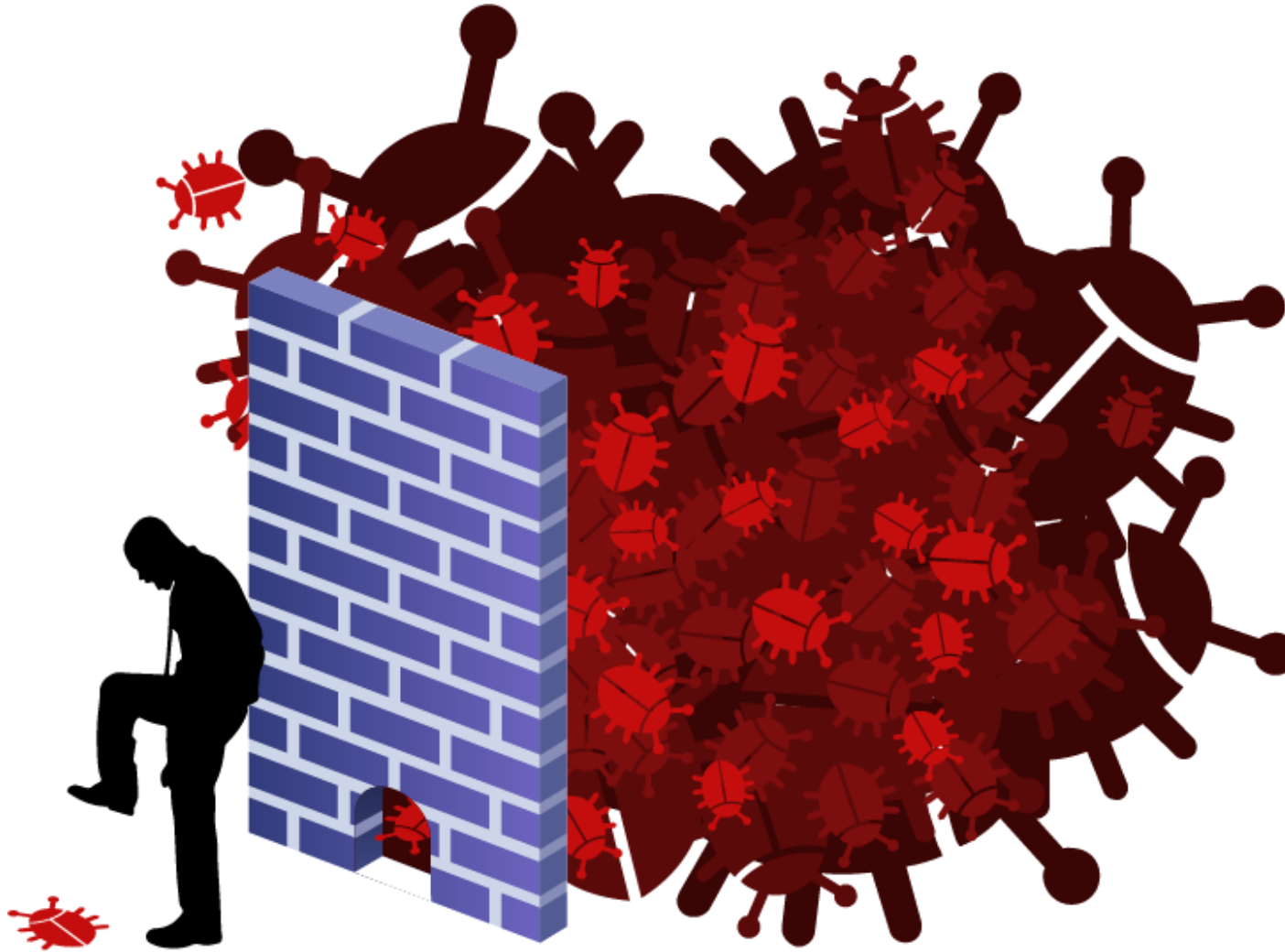
Legacy NGFW can reduce attack surface area but advanced malware often evades security controls.

Threat Landscape Demands more than Application Control



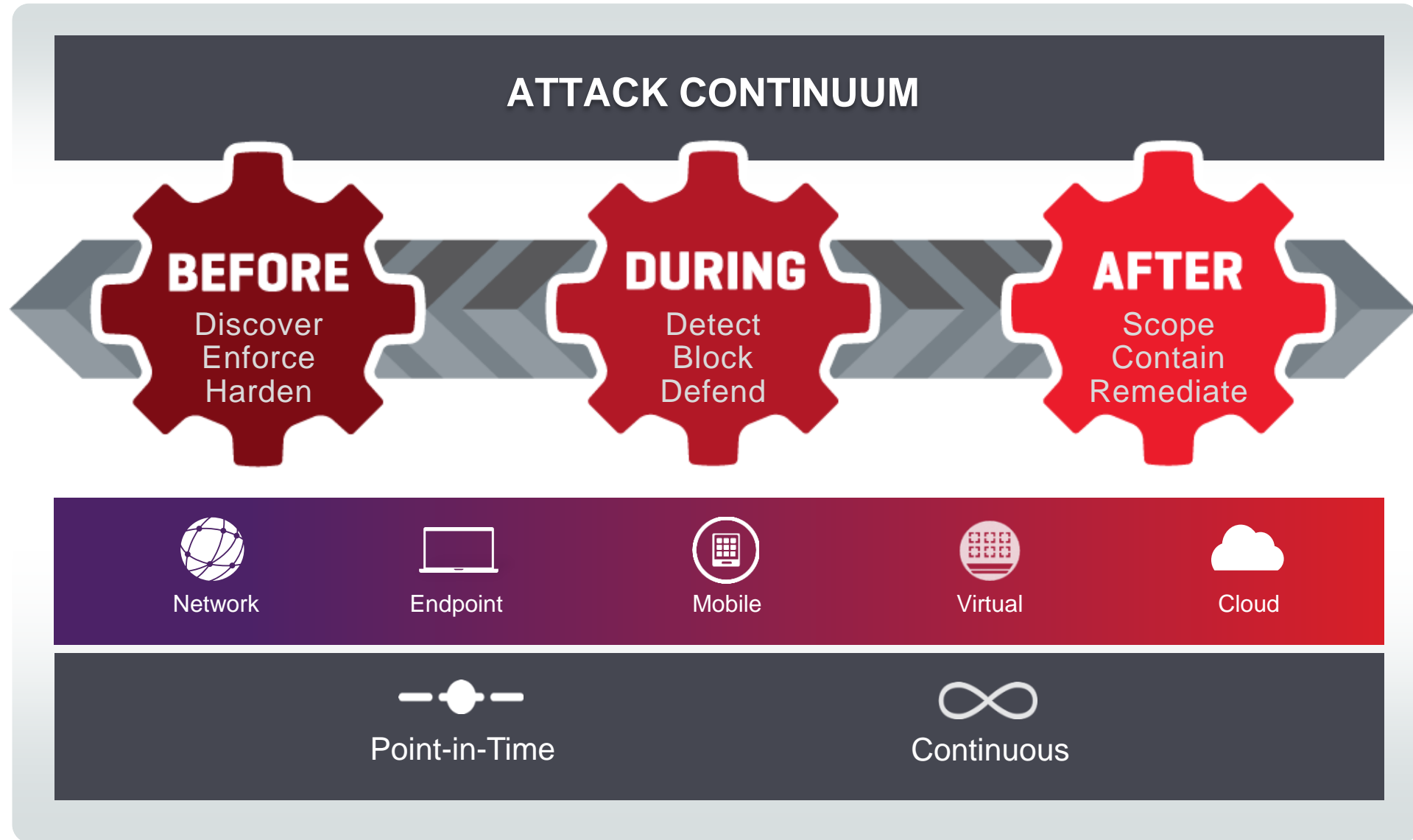
It is a **Community** that hides in plain sight avoids detection and attacks swiftly

Legacy NGFWs Lack Complete Visibility and Control

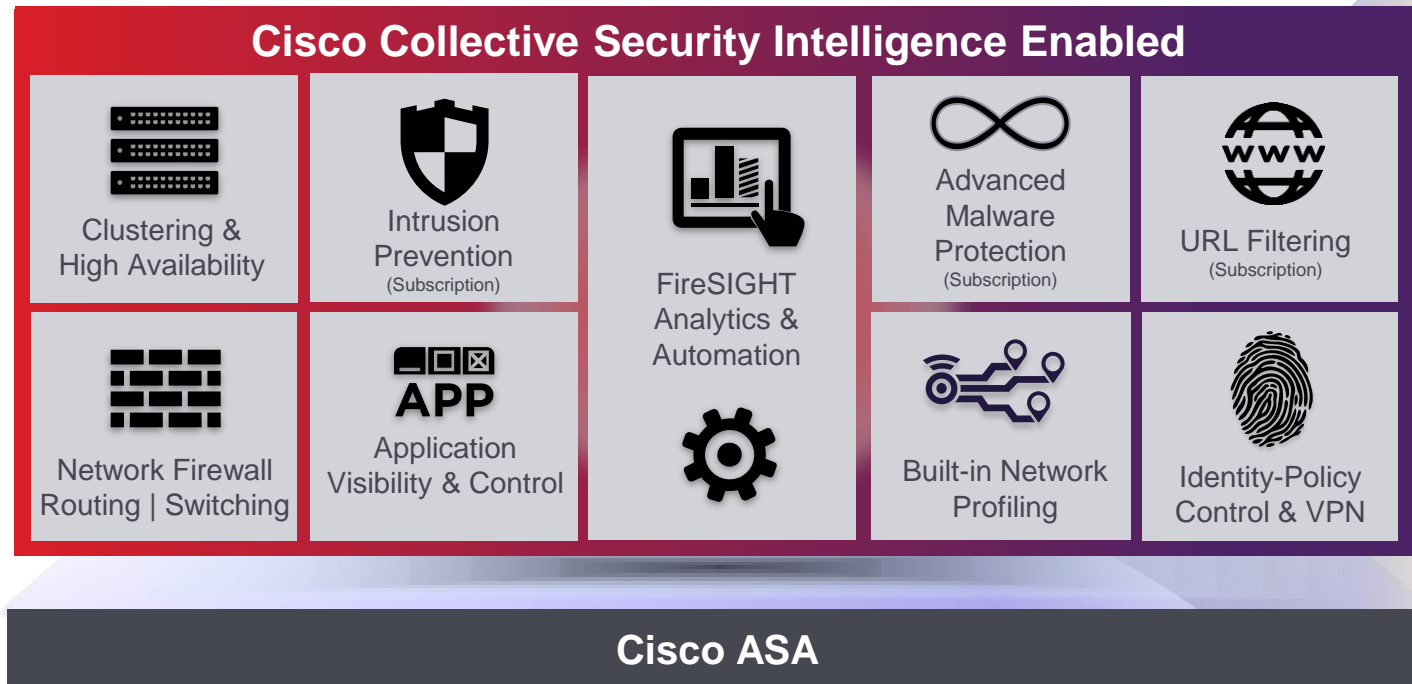


Without Proper Visibility Threat Protection Cannot Be Operationalized

Integrated Threat Defense Across the Attack Continuum



Superior Integrated & Multilayered Protection

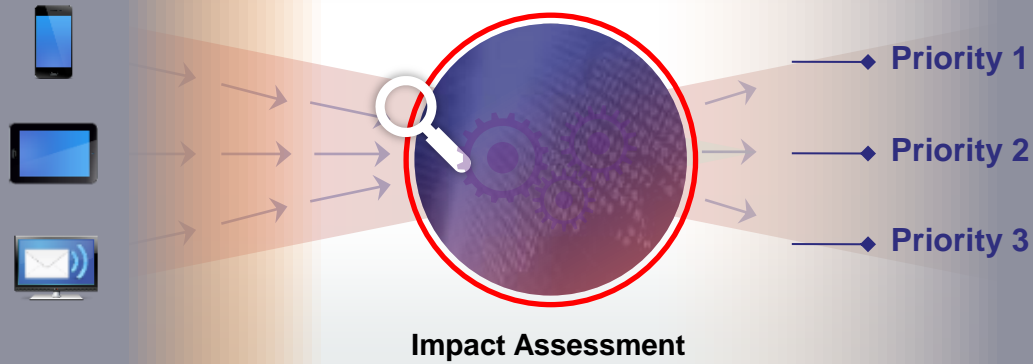


- ▶ World's most widely deployed, enterprise-class ASA stateful firewall
- ▶ Granular Cisco® Application Visibility and Control (AVC)
- ▶ Industry-leading FirePOWER next-generation IPS (NGIPS)
- ▶ Reputation- and category-based URL filtering
- ▶ Advanced Malware Protection with Retrospective Security

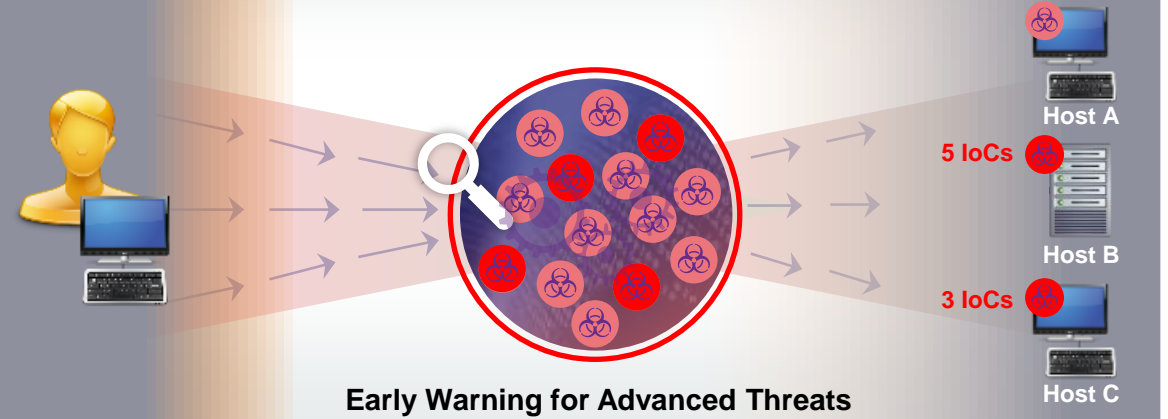
Automated, Integrated Threat Defense

Superior Protection for Entire Attack Continuum

Context and Threat Correlation



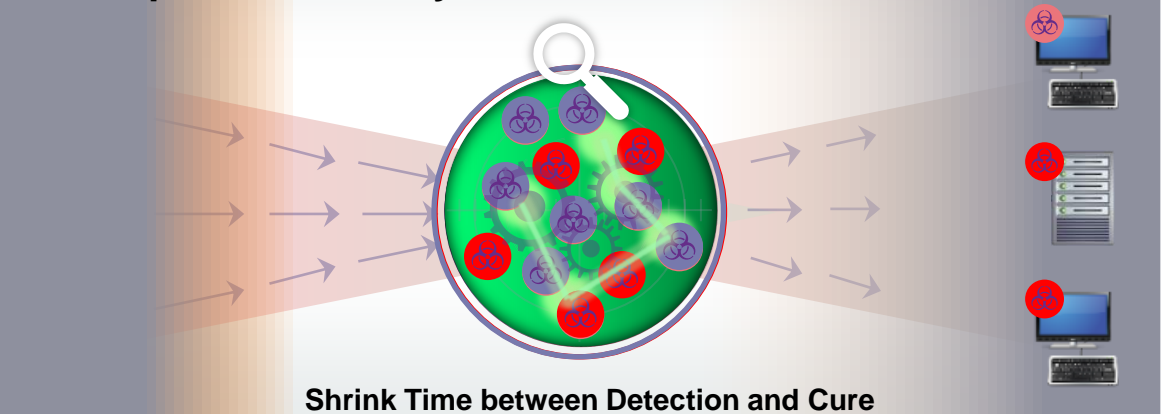
Multi-vector Correlation



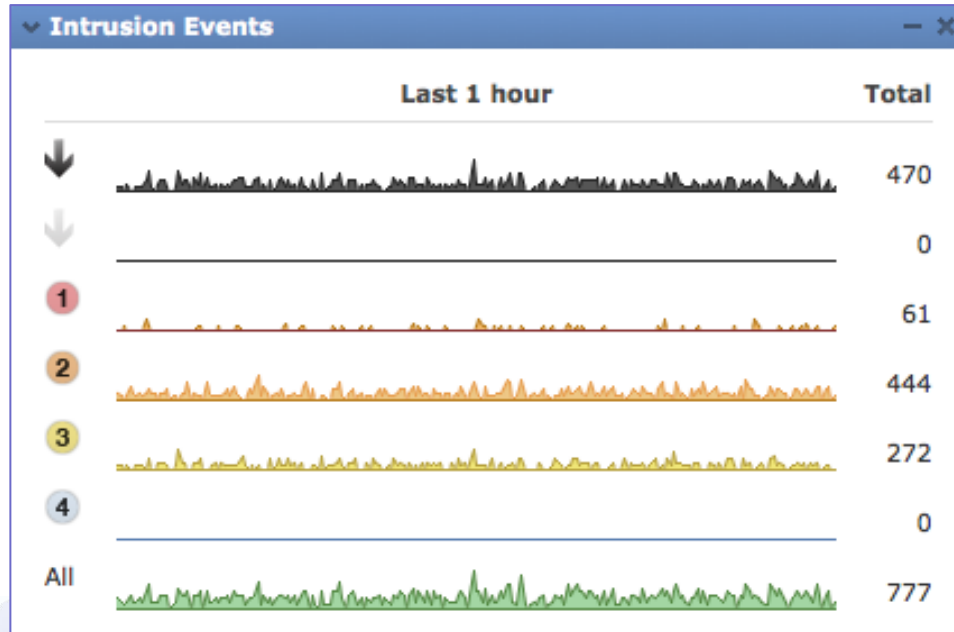
Dynamic Security Control







Retrospective Security



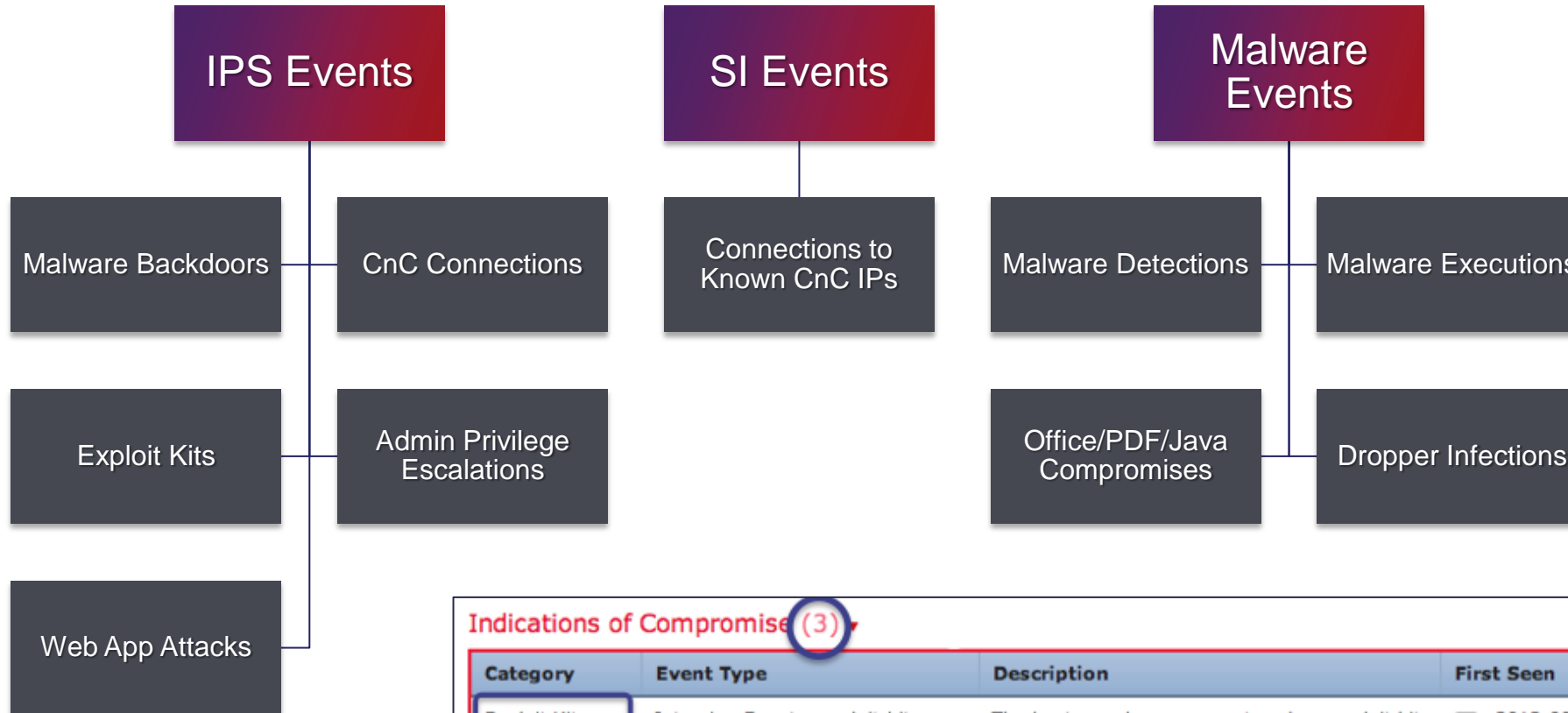
Impact Assessment



Correlates all intrusion events to an impact of the attack against the target

IMPACT FLAG	ADMINISTRATOR ACTION	WHY
 1	Act Immediately, Vulnerable	Event corresponds to vulnerability mapped to host
 2	Investigate, Potentially Vulnerable	Relevant port open or protocol in use, but no vuln mapped
 3	Good to Know, Currently Not Vulnerable	Relevant port not open or protocol not in use
 4	Good to Know, Unknown Target	Monitored network, but unknown host
 0	Good to Know, Unknown Network	Unmonitored network

Indicators of Compromise (IoCs)



Indications of Compromise (3)							Edit Rule States		Mark All Resolved	
Category	Event Type	Description	First Seen	Last Seen						
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31						
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45						
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49						

Cisco ASA with FirePOWER Services vs. Legacy NGFW

Feature	Cisco ASA with FirePOWER Services	Legacy NGFW
Reputation-Based Proactive Protection	Superior	Not Available
Visibility, Context & Intelligent Security Automation	Superior	Not Available
File Reputation, File Trajectory, Retrospective Analysis	Superior	Not Available
IoC's	Superior	Not Available
NGIPS	Superior	Available ¹
Application Visibility and Control	Superior	Available
Acceptable Use/URL Filtering	Superior	Available
Remote Access VPN	Superior	Not Enterprise-Grade
Stateful Firewall, HA, Clustering	Superior	Available ²

1 – Typically 1st generation IPS, 2 -HA Capabilities vary from NGFW vendor



Complete Security Solutions

Cisco ASA with FirePOWER Services

Industry's First Threat-Focused NGFW

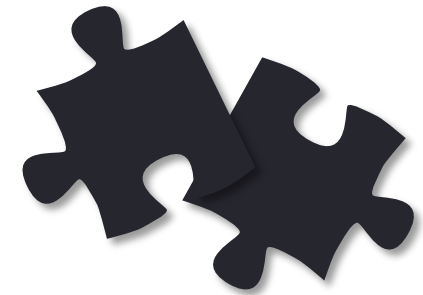
Superior Visibility

- ▶ Full contextual awareness to eliminate gaps



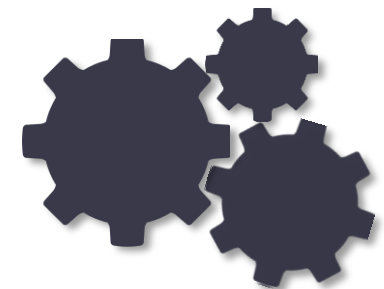
Integrated Threat Defense

- ▶ Best-in-class, multilayered protection in a single device



Automation

- ▶ Simplified operations and dynamic response and remediation



Thank You

