인텔리전트 글로벌 위협정보를 활용한 컨텐츠 보안 소개
Cisco Security Intelligence Operations
Defense in Depth

Michael J. Covington, Ph.D.

Product Manager, Security Intelligence Operations (SIO)

March 28, 2013

Agenda

- Threat Evolution
- Cisco Security Framework
- SIO Overview
- Breadth and Context
- SIO Defense
- Threat Example

Threat Landscape Evolution

Response

Threats

Host-based (Anti-Virus) 2000

Network Perimeter (IDS/IPS) 2005

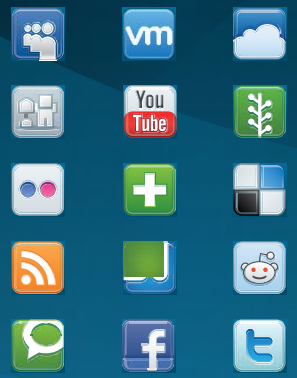
Global Reputation & Sandboxing 2010

Intelligence & Analytics Tomorrow

WORMS

SPYWARE / ROOTKITS

APTs CYBERWARE



INCREASED ATTACK SURFACE (MOBILITY & CLOUD)

Cisco 2013 Annual Security Report

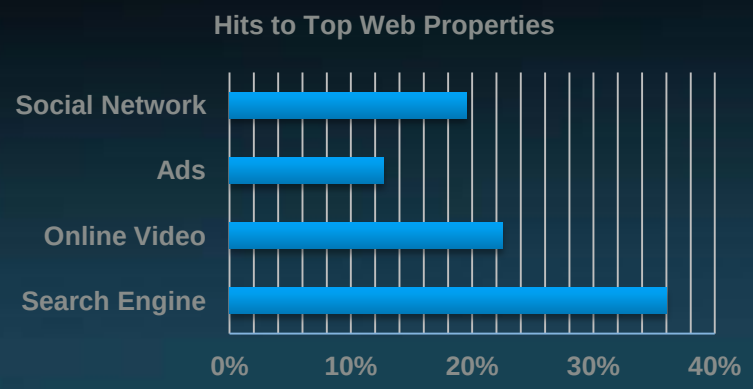
Where You Visit Online…

36%
search engines

22%
Online video

20%
Social networks

13%
Advertisements



Cisco 2013 Annual Security Report

…Is Where The Threats Are

Search Engines vs. Counterfeit Software

27x more likely to deliver malicious content

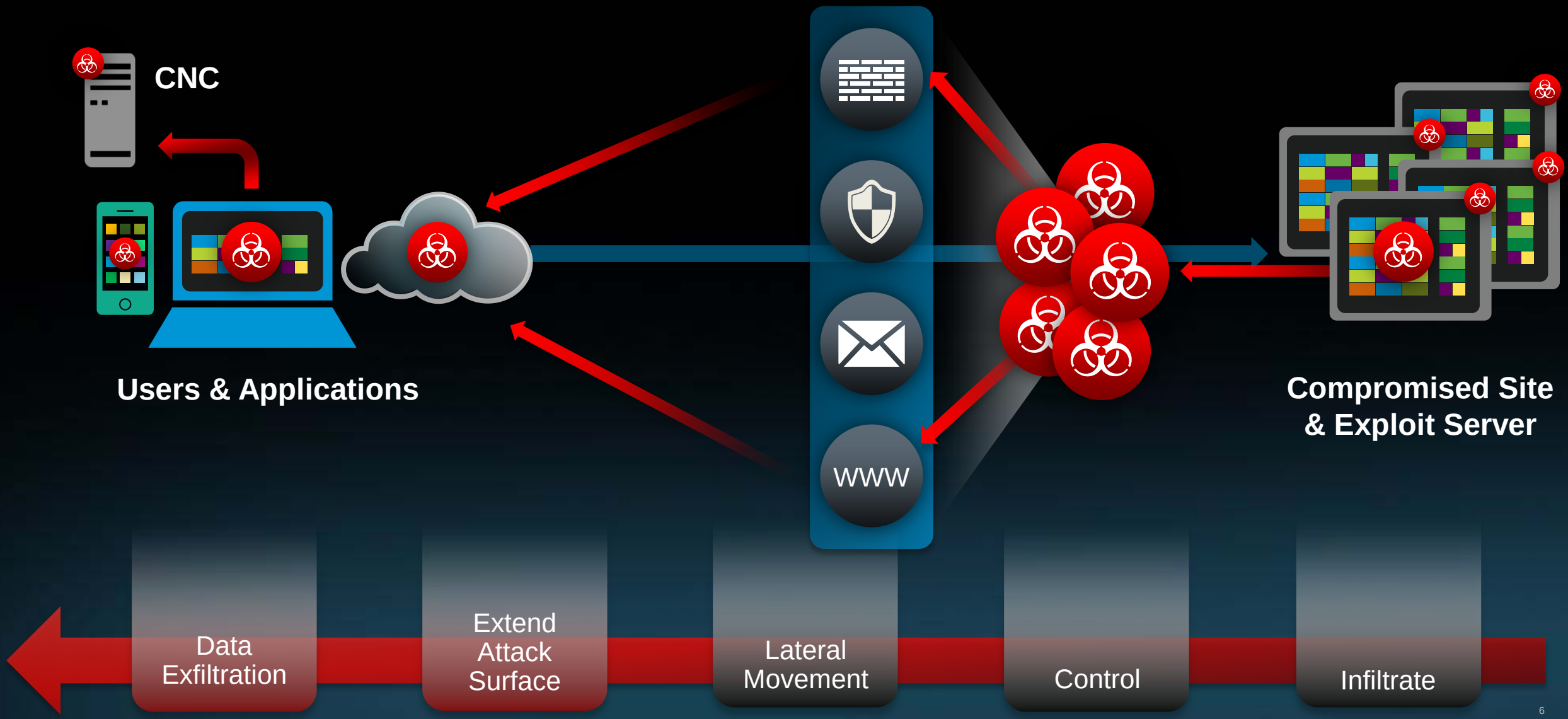
Online Advertisements vs. Pornography

182x more likely to deliver malicious content

Online Shopping vs. Counterfeit Software

21x more likely to deliver malicious content

Advanced Cyber Threats



Implications for Security

Functions need to work as a system

Defend

Policy & Access Control

Blocking

Quarantine

Re-routing Traffic

Discover

Increased Content Inspection

Behavior Anomaly Detection

Advanced Threats

Inside the Network

Remediate

Assess Environment & Threat

Advanced Forensics

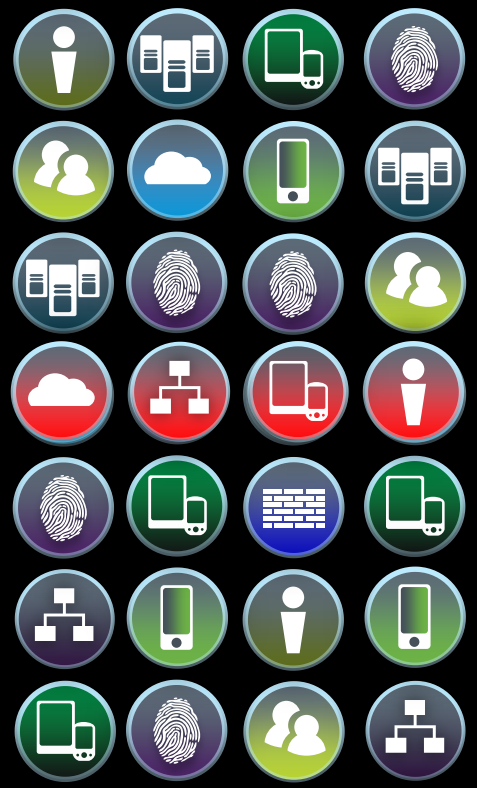
Contain

Fix

Cisco E-Mail Security Portfolio

Cisco Web Security Portfolio

Threat Discovery through Local Intelligence



Detected

IDENTIFY ADVANCED CYBER THREATS
behavioral analysis artificial intelligence

- **THREAT BEHAVIOR ANALYSIS**
  leveraging network, web, and identity context
- **MODERN DETECTION ALGORITHMS**
  behavioral analysis artificial intelligence
- **SELF-LEARNING AND EVASION RESISTANCE**
  game theoretic self optimization

CLOUD-BASED THREAT INTEL & DEFENSE

ATTACKS | 3rd PARTY FEEDS | REPUTATION & RULES | MALWARE ANALYSIS

GLOBAL | LOCAL

COMMON POLICY, MANAGEMENT & CONTEXT

COMMON MANAGEMENT | SHARED POLICY | ANALYTICS | COMPLIANCE | PARTNER API

IDENTITY | APPLICATION | DEVICE | LOCATION | TIME

NETWORK ENFORCED POLICY

ACCESS | FW | IPS | VPN | WEB | EMAIL

APPLIANCES | ROUTERS | SWITCHES | WIRELESS | VIRTUAL

Infrastructure

public

Apps / Services

hybrid

tenants

Workloads

private

A MORE INTEGRATED APPROACH

Threat Defense with Global Intelligence

Discovery with Breadth

100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks

Security Intelligence Operations

Broadest Visibility

Global Footprint

Defense in Depth

Daily Security Intelligence

Discovery with Breadth

100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks

Security Intelligence Operations

Broadest Visibility
Global Footprint
Defense in Depth

Deployed Security Devices

Discovery with Breadth

100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks

Security Intelligence Operations

Broadest Visibility

Global Footprint

Defense in Depth

Daily Web Requests

Discovery with Breadth

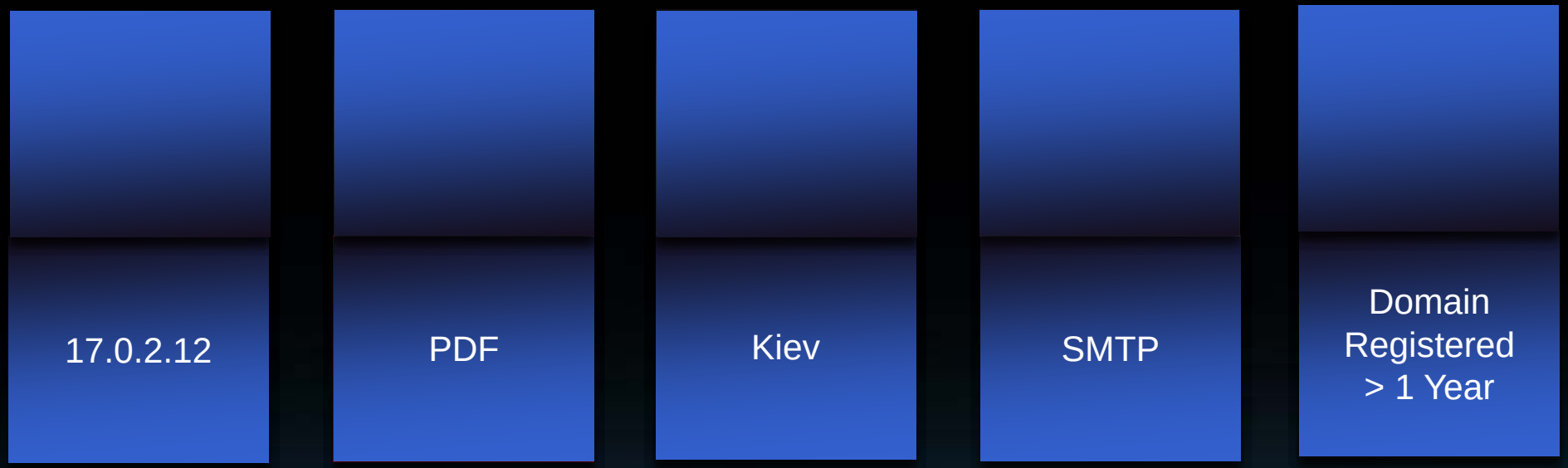
100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks

Security Intelligence Operations

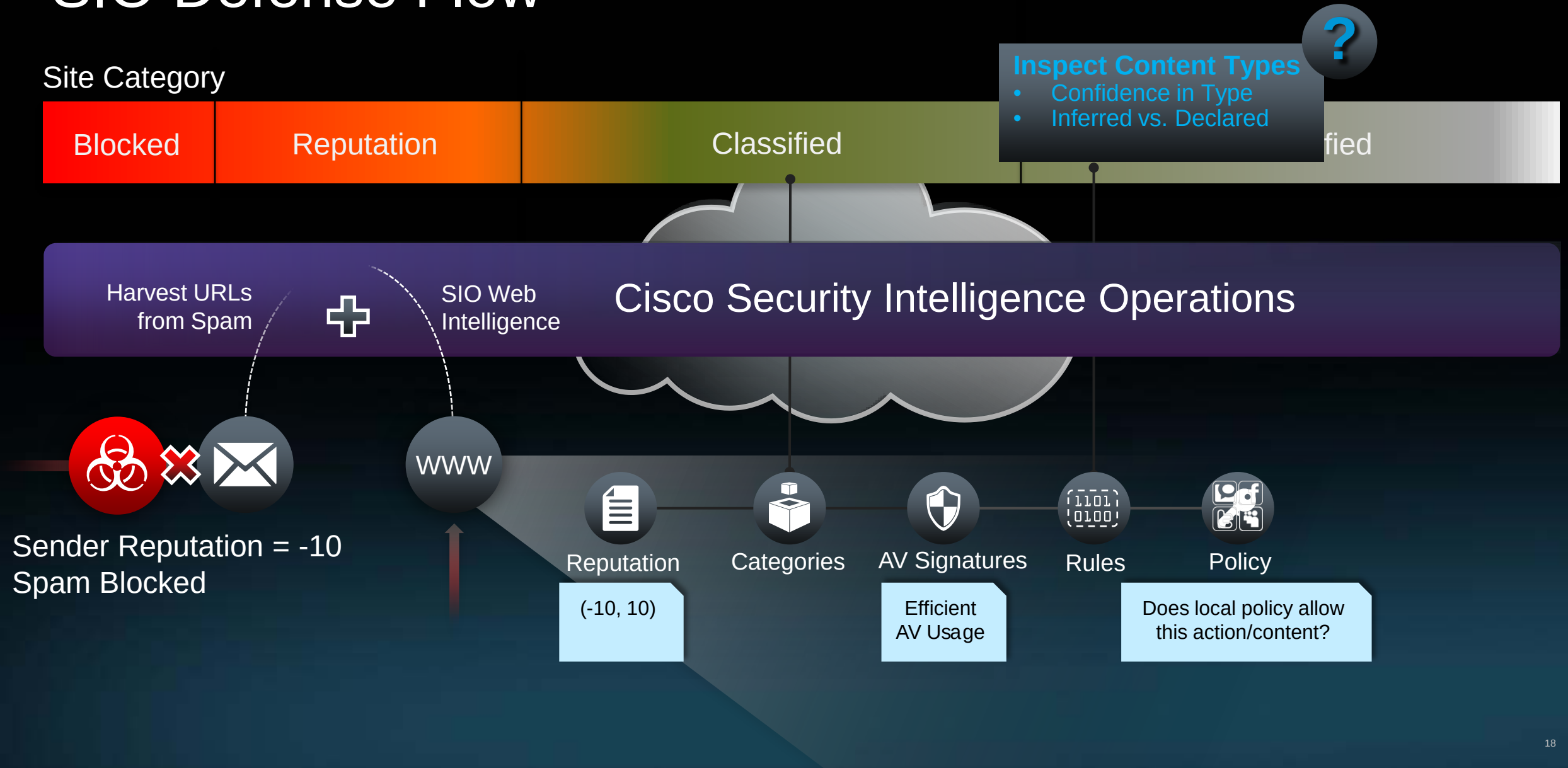
Broadest Visibility
Global Footprint
Defense in Depth

Applications
& Micro-Applications

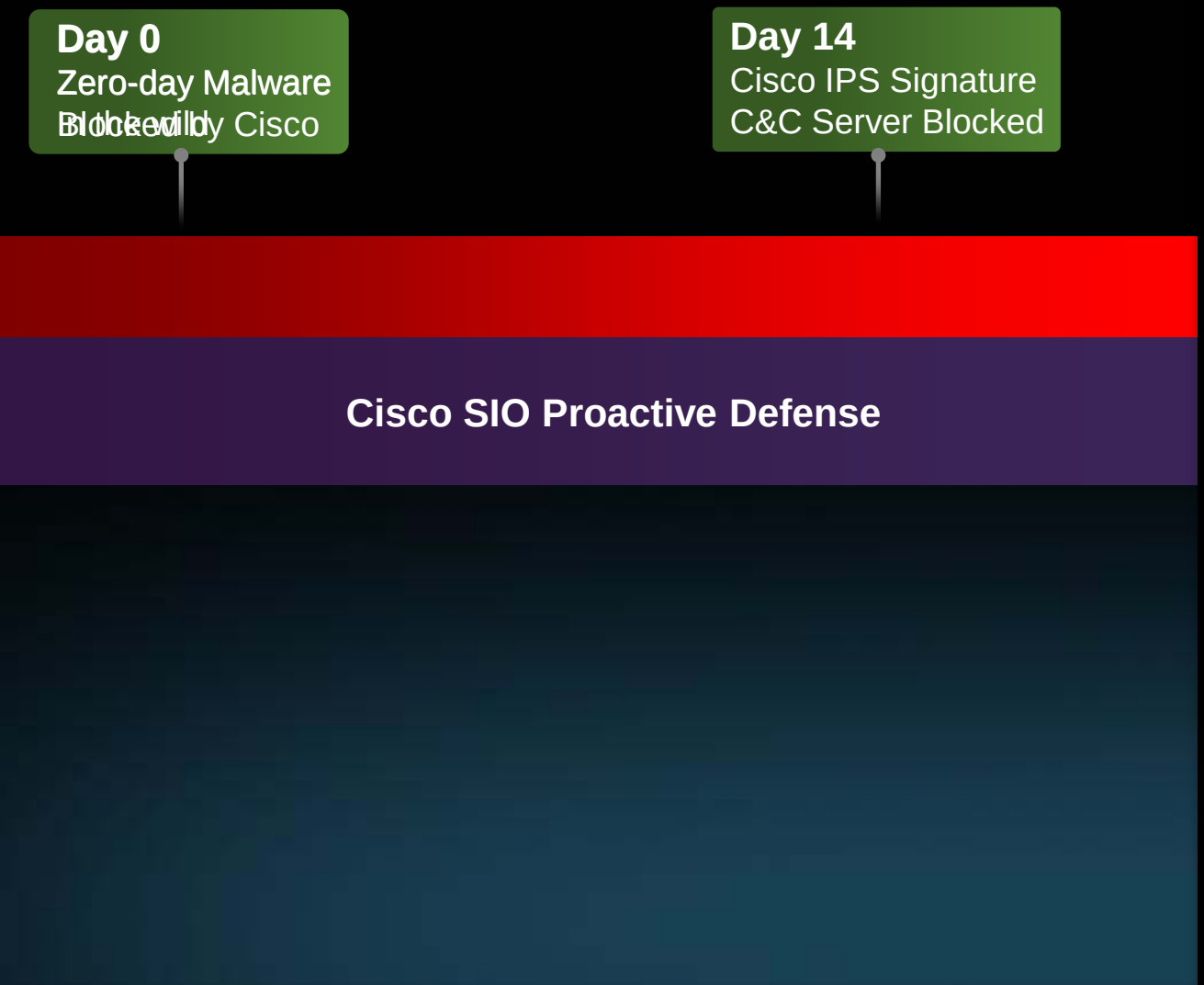
Discovery with Context



SIO Defense Flow



Internet Explorer (IE) Zero-Day Vulnerability



Multiple Attack Vectors, Multiple Layers of Defense

- **SIO cross-platform** intelligence
- **Blocked** zero-day threat
- **Blocked** 40+ “parked” domains
- **Blocked** exploit server & CNC
- **18 day** lead time

SIO: Defense in Depth


CISCO