Stop Threats Faster with Rapid Threat Containment Solution

Ross Shehov
Security Systems Engineer

September 2016
One in four breaches are caused by malicious insiders.

95% of all cybercrime is triggered by a user clicking on a malicious link disguised to be legitimate.

Two in three breaches exploit weak or stolen passwords.

With lateral movement of advanced persistent threats, even external attacks eventually become internal threats.
Threats and Attacks Are Growing in...

**Sophistication**
- Organizations often have 40 to 60+ disparate security solutions
- But they don’t – and often can’t – work together

**Stealth**
- 17,000 alerts received on average per week
- 19% prove reliable
- Security teams have time to investigate just 4% of warnings

**Speed**
- The longer threats stay undetected, the greater for damage
- But current industry average detection time: 200 days
- Average cost per data breach: $3.8 million

1. Warning
2. Data source
Threats and Attacks Relies on Dis-Integrated Security Infrastructure

Too Much Information

Too Much Manual Effort

Too Little Time
Core of Rapid Threat Containment - Cisco Identity Service Engine (ISE)

Benefits

Detect Threats Early
Cisco security products publishes events to ISE

Automate Endpoint Containment
ISE alerts the network of suspicious activity according to policy

Integrate Best-of-Breed Security
Growing ecosystem of threat defense partners integrate with ISE
Platform Exchange Grid (pxGrid)

---

**Cisco pxGrid**

**SECURITY THRU INTEGRATION**

- **IAM & SSO**
- **SIEM & Threat Defense**
- **Net/App Performance**
- **IoT Security**
- **Firewall & Access Control**
- **Cisco ISE**
- **Cisco FirePOWER**
- **Cisco WSA**
- **Cloud Access Security**
- **Packet Capture & Forensics**
- **Vulnerability Assessment**
- **Rapid Threat Containment (RTC)**
- **DDI**

---

### pxGrid-Enabled ISE Partners:

- **RTC:** Cisco FirePower, Bayshore, E8, Elastica, Hawk, Huntsman, Infoblox, Invincea, Cisco StealthWatch, LogRhythm, NetIQ, Rapid7, SAINT, Splunk, Tenable
- **Firewall:** Check Point, Infoblox, Bayshore
- **DDI:** Infoblox
- **Cloud:** Elastica, SkyHigh Networks
- **Net/App:** LiveAction, Savvius
- **SIEM/TD:** Splunk, Cisco StealthWatch, NetIQ, LogRhythm, FortScale, Rapid7
- **IAM:** Ping, NetIQ, SecureAuth
- **Vulnerability:** Rapid7, Tenable, SAINT
- **IoT Security:** Bayshore Networks
- **P-Cap/Forensics:** Emulex

### Other ISE Partners:

- **SIEM/TD:** ArcSight, IBM QRadar, Tibco LogLogic, Symantec
- **MDM/EMM:** Cisco Meraki, MobileIron, AirWatch, JAMF, SOTI, Symantec, Citrix, IBM, Good, SAP, Tangoe, Globo, Absolute

---

© 2016 Cisco and/or its affiliates. All rights reserved.
Rapid Threats Containment : Outside Threats
Outside Threats

Advanced Threat Sensors
- Cisco ASA with Firepower Services
- Firepower NGIPS Appliances
- Cisco AMP for Networks
- Firepower on Cisco ISR

Threat Visibility
- Cisco FirePower Management Center
- Automated Contextual Analysis and Threat Qualification
- Continuous Threat Intelligence Updates to Threat Sensors

Automated Enforcement
- Cisco FireSIGHT and Cisco ISE Automate Containment
- Policy Enforcement from Cisco TrustSec, Downloadable ACL, or VLAN
Rapid Threat Containment in Action

Automatically Defend Against Threats with FMC and ISE

Corporate user downloads file, not knowing it’s actually malicious.

Cisco security sensors scan the user activity and downloaded file. FMC aggregates and correlates sensor data.

FMC detects flagrantly suspicious file and alerts ISE. ISE then changes the user’s/device’s access policy to **suspicious**.

Based on the new policy, network enforcers automatically restrict access.

Device is quarantined for remediation or mitigation—access is denied per security policy.
Rapid Threats Containment: Inside Threats
Cisco Stealthwatch & Identity Services Engine (ISE)

Network Reconnaissance Using Dynamic NetFlow Analysis

Monitor

- Understand your network normal
- Gain real-time situational awareness of all traffic

Detect

- Leverage Network Behavior Anomaly detection & analytics
- Detect behaviors linked to APTs, data leakage, DDoS, and users hoarding data

Analyze

- Collect & Analyze holistic network audit trails
- Achieve faster root cause analysis to conduct thorough forensic investigations

Respond

- Accelerate network troubleshooting & threat mitigation
- Respond quickly to threats by taking action to quarantine through Cisco ISE
Stealthwatch – Broad Visibility of Telemetry Via Flow Analysis

EVERYTHING must touch the network

Company Network

Assess

Audit

Posture

Detect

Response

Context

Know every host

RECORD every conversation

Know what is NORMAL

Be alerted to CHANGE

Store for MONTHS

What else can the network tell me?
Inside Threat Detection: Multiple Login example

In one hour, ethel has travelled 1080 miles
(takes 16h by car, 2.5h by flight).
Differentiated Threat Defense with Rapid Threat Containment

Advanced, Automated Threats Detection
Contextual Visibility to Understand and Contain Threats Faster
Continually Updated Threat Intelligence
Pervasive Network Enforcement
Your Cisco Network Infrastructure as Security Sensor and Enforcer