Gain Full Visibility and Security Across Your Network

Candice Griswold
Security Account Manager NVE-AJC

May 2017
Enterprise Network Security Trends

- **1M new devices** will go online every hour by 2020.
- Malicious breaches take **80 days** to discover.
- **76%** of IT professionals say a lack of visibility is their biggest challenge in addressing network threats.
- **The average total cost** of a single data breach is **$4M**.

Complexity of attacks is increasing but our capabilities are not and we have a security gap between the two. We need to reduce the security gap by providing better visibility of network threats.
Challenges

I want to know what is going on with my network at all times – across all applications, users, and devices.

I want to defend my network against increasingly complex and persistent network threats – now and in the future.

I want a single solution to be able to streamline my organization’s response to and containment of threats.
All Threats Are Insider Threats

One out of four breaches are caused by malicious insiders

95% of all cybercrime is user-triggered by disguised malicious links

Two out of three breaches exploit weak or stolen passwords

With lateral movement of advanced persistent threats, even external attacks eventually become internal threats
Enterprise Network Security Should Provide…

- Detailed network traffic visibility for threat detection
- Intelligent real-time protection against known and unknown threats
- Unified security that reduces risk and complexity
Cisco Enterprise Network Security

Network as a Sensor
Visibility and analytics across the extended enterprise, industry-leading threat intelligence

Network as an Enforcer
Consistent threat protection and remediation across the network

Threat Mitigation
Security embedded into hardware and software by design

Secure your digital network in real-time, all the time, everywhere
Cisco Network as a Sensor (NaaS)

- Detect: Anomalous Traffic Flows, Malware
- Identify: User Access Policy Violations
- Obtain: Broad Visibility into All Network Traffic
See and detect more in your network with Stealthwatch

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Detect</th>
<th>Analyze</th>
<th>Respond</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Obtain comprehensive, scalable enterprise visibility and security context</td>
<td>• Detect and analyze network behavior anomalies</td>
<td>• Collect and analyze holistic network audit trails</td>
<td>• Accelerate network troubleshooting and threat mitigation</td>
</tr>
<tr>
<td>• Gain real-time situational awareness of traffic</td>
<td>• Easily detect behaviors linked to advanced persistent threats (APTs), insider threats, distributed denial-of-service (DDoS) attacks, and malware</td>
<td>• Achieve faster root cause analysis</td>
<td>• Respond quickly to threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Conduct thorough forensic investigations</td>
<td>• Continuously improve enterprise security posture</td>
</tr>
</tbody>
</table>

- Collect and analyze holistic network audit trails
- Achieve faster root cause analysis
- Conduct thorough forensic investigations
- Accelerate network troubleshooting and threat mitigation
- Respond quickly to threats
- Continuously improve enterprise security posture
Behavioral and Anomaly Detection
Behavioral Algorithms Are Applied to Build “Security Events”

SECURITY EVENTS (94 +)

- Addr_Scan/tcp
- Addr_Scan/udp
- Bad_Flag_ACK
- Beaconing Host
- Bot Command Control Server
- Bot Infected Host - Attempted
- Bot Infected Host - Successful
- Flow_Denied
- ICMP Flood
- Max Flows Initiated
- Max Flows Served
- Suspect Long Flow
- Suspect UDP Activity
- SYN Flood

ALARM CATEGORY

- Concern
- Recon
- C&C
- Exploitation
- Data Hoarding
- Exfiltration
- DDoS Target

RESPONSE

- Alarm Table
- Host Snapshot
- Email
- Syslog / SIEM
- Mitigation
NaaS use cases with Stealthwatch

**Context-Aware Visibility**
- Network, application, and user activity
- Monitor lateral movement using the network as a sensor

**Threat Detection**
- Advanced persistent threats
- Insider threat
- DDoS
- Data exfiltration

**Incident Response**
- In-depth, flow-based forensic analysis of suspicious incidents
- Scalable repository of security information

**Network Planning & Diagnostics**
- Network segmentation to profile application / device traffic
- Capacity planning
- Performance monitoring
- Application awareness

**User Monitoring**
- Cisco ISE
- Monitor privileged access
- Policy enforcement
Customer Case Study - Network as a Sensor

**Industry:** Retail
**Company:** Large Known Global Retailer

**Existing Environment:**
- Large Cisco Switch & Router Footprint
- ASA & ISE

**Customer Challenges:**
- Limited visibility & intelligence across their highly-distributed retail footprint
- Lack of ability to correlate numerous data sets

**Results:**
- After deploying Cisco Netflow, Stealthwatch and Cisco ISE
- Gains Retail Point-of-Presence Visibility
- Deeper Understanding into Network Application Usage
Analysis with Stealthwatch Provides

Discovery
Identifies business-critical applications and services across the network

Identification of Additional IOCs
Policy and segmentation
Network behavior anomaly detection (NBAD)

Better Understanding of how to Respond to an IOC
Audit trail of all host-to-host communication
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 Identity Services Engine (ISE)

Adding Visibility and Context to NetFlow

- **NETWORK / USER CONTEXT**
  - Who
  - What
  - When
  - Where
  - How

- **INTEGRATED PARTNER CONTEXT**

Send Contextual Data Collected From Users, Devices, And Networks To Stealthwatch For Advanced Insights And NetFlow Analytics
Network as an Enforcer: Cisco TrustSec Software-Defined Segmentation
Provide Role-Based Segmentation to Control Access and Contain Threats

Segmentation Policy Enforced Across the Extended Network
Customer Case Study - Network as an Enforcer

Industry: Banking
Company: Large Known Global Bank

Existing Environment:
• Large Cisco Switch & Router Footprint

Customer Challenges:
• Visibility into the network and rogue devices
• Policy enforcement of user to data center policies
• Meeting compliance audits

Results:
• After deploying StealthWatch, Cisco ISE and Cisco TrustSec
• Gain Deep Visibility into Network Access and Devices
• Segment Network Access and Assets using Business Role Based Policies
• Accelerated time to Compliance Audits
Architecting a Secure Network
Combining Network as a Sensor / Network as an Enforcer

Network Sensors
- Cisco Collective Security Intelligence
- Network Sensor (Stealthwatch)

Threat
- pxGRID

TrustSec Software-Defined Segmentation

Policy & Context Sharing
- pxGRID

Network Enforcers
- Campus/DC Switches/WLC
- NGFW
- Cisco Routers / 3rd Vendor Devices
- Confidential Data
- NGIPS
- ISE
Integrated Threat Defense (Detection & Containment)

Event: TCP SYN Scan
Source IP: 10.4.51.5
Role: Supplier
Response: Quarantine

Network Fabric

ISE
Stealthwatch
Change Authorization

Employee
Supplier
Quarantine
Shared Server
Server
High Risk Segment
Internet
Employee

Cisco Confidential
Next Steps

Link to
www.cisco.com/go/networksecurity

Link to
www.cisco.com/go/dna