Say hello to the future.

Cisco Connect 2019
Malaysia, Kuala Lumpur · 18 April 2019
#CiscoConnectMY
Security and Visibility for the Modern Networks

Ross Traynor, Cybersecurity Specialist, Cisco
Eric Rennie, Systems Engineer, Cybersecurity, Cisco
Threats are more numerous and complex. Companies experienced a 27.4% average increase in security breaches in 2019. Threats are using encryption to evade detection. Over 20B connected “things” will be in use by 2020. By 2020, 2/3rds of all IP traffic will come from wireless and mobile devices. More IoT devices connect everyday. Users work anywhere across many devices. 3X increase in encrypted communication from malware in a 12-month period.
The vendor buffet is not a strategy
Adding point solutions adds complexity & can make you less secure

55% Of customers rely on more than 5 vendors to secure their network\(^1\)

54% Of legitimate security alerts are not remediated due to lack of integrated defense systems\(^2\)

100 days Industry average to detect a common threats\(^3\)

\(^1\) Cisco 2019 Annual Cybersecurity Report
\(^2\) Cisco 2019 Annual Cybersecurity Report
\(^3\) Cisco 2019 Mid-Year Cybersecurity Report
The Solution: Network + Security
Activate your network for more holistic security

Understand behavior
Identify host role and monitor behavior without endpoint agents

See everything
Transform the network into a powerful security sensor for complete visibility

Contain and isolate threats
Dynamically enforce software-defined segmentation based on business roles

Detect encrypted threats
Use advanced analytics to automatically detect encrypted threats without decryption
Cisco Stealthwatch
Gain confidence in your security effectiveness

Contextual network-wide visibility

Predictive threat analytics
- Behavioral modeling
- Machine learning
- Global threat intelligence

Automated detection and response
- Unknown threats
- Insider threat
- Encrypted malware
- Policy violations

Using existing network infrastructure
Stealthwatch Use Cases

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 Use Cases:
Key features

Visibility everywhere
Analyses enterprise telemetry from any source (NetFlow, IPFIX, sFlow, other Layer 7 protocols) across the extended network

Encrypted Traffic Analytics
Only product that can analyze encrypted traffic to detect malware and ensure policy compliance without decryption

Rapid Threat Containment
Quarantine infected hosts easily using the Identity Services Engine (ISE) integration, collect and store network audit trails for deeper forensic investigations

Unique threat detection
Combination of multi-layer machine learning and behavioral modeling provides the ability to detect inside as well as outside threats

Smart segmentation
Create logical user groups that make sense for your business, monitor the effectiveness of segmentation policies through contextual alarms
Collecting and optimizing telemetry
Scaling and Optimization: stitching

### Unidirectional Telemetry Records

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Interface</th>
<th>Src IP</th>
<th>Src Port</th>
<th>Dest IP</th>
<th>Dest Port</th>
<th>Proto</th>
<th>Pkts Sent</th>
<th>Bytes Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:20:12.221</td>
<td>eth0/1</td>
<td>10.2.2.2</td>
<td>1024</td>
<td>10.1.1.1</td>
<td>80</td>
<td>TCP</td>
<td>5</td>
<td>1025</td>
</tr>
<tr>
<td>10:20:12.871</td>
<td>eth0/2</td>
<td>10.1.1.1</td>
<td>80</td>
<td>10.2.2.2</td>
<td>1024</td>
<td>TCP</td>
<td>17</td>
<td>28712</td>
</tr>
</tbody>
</table>

### Bidirectional Telemetry Record

**Conversation record**

**Easy visualization and analysis**

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Client IP</th>
<th>Client Port</th>
<th>Server IP</th>
<th>Server Port</th>
<th>Proto</th>
<th>Client Bytes</th>
<th>Client Pkts</th>
<th>Server Bytes</th>
<th>Server Pkts</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:20:12.221</td>
<td>10.2.2.2</td>
<td>1024</td>
<td>10.1.1.1</td>
<td>80</td>
<td>TCP</td>
<td>1025</td>
<td>5</td>
<td>28712</td>
<td>17</td>
<td>eth0/1/eth0/2</td>
</tr>
</tbody>
</table>
Scaling and Optimization: deduplication

Deduplication

- Avoid false positives and misreported traffic volume
- Enable efficient storage of telemetry data
- Necessary for accurate host-level reporting
- No data is discarded
Industry-leading Security Analytics
Anomaly detection using behavioral modeling

Collect and analyze telemetry
- Comprehensive data set optimized to remove redundancies

Create a baseline of normal behavior
- Security events to detect anomalies and known bad behavior
- Analysis of multiple threat behaviors
  - Number of concurrent flows
  - Packet per second
  - Bits per second
  - New flows created
  - Number of SYN sent
  - Time of day
  - Duration of the flow
  - Number of SYN received
  - Rate of connection resets

Alarm on anomalies and behavioral changes
- Alarm categories for high-risk, low-noise alerts for faster response
Behavioral & Anomaly Detection Model
Behavioral Algorithms are Applied to Build “Security Events”

Collect and Analyze Flows

Security Events
- Addr_Scan
- Bad_Flag_ACK
- Beaconing Host
- Bot Infected Host - Successful Brute Force Login
- Fake Application
- Flow_Denied
- ICMP Flood
- Max Flows Initiated
- Max Flows Served
- Suspect Data Hoarding
- Suspect Data Loss
- Suspect Long Flow
- UDP Received

Alarm Category
- Concern
- Recon
- C&C
- Exploitation
- Data hoarding
- Exfiltration
- DDoS target

Response
- Alarm table
- Host snapshot
- Email
- Syslog / SIEM
- Mitigation
Logical alarms based on suspicious events

- Source or target of malicious behavior
  - Scanning, excessive network activity such as file copying or transfer, policy violation, etc.

- Reconnaissance
  - Port scanning for vulnerabilities or running services

- Command and Control
  - Communication back to an external remote controlling server through malware

- DDoS Activity
  - Sending or receiving SYN flood and other types of data floods

- Insider threats
  - Data hoarding and data exfiltration

Concern Index: 4  Target Index: 0  Recon: 6  C&C: 0  Exploitation: 3  DDoS Source: 0  DDoS Target: 1  Data Hoarding: 4  Exfiltration: 3  Policy Violation: 1  Anomaly: 0
Quick snapshot of malicious activity

Suspicious behavior linked to logical alarms

Risks prioritized to take immediate action

Alarms tied to specific entities
Investigating a host

Host Summary

User Name: 
Device Name: 
Device Type: 
Host Group: 
Location: 
Last Active Status: 
Session Information: 
Policies: 
Quarantine: 
Unquarantine: 

Traffic by Peer Host Group

10.201.3.149

Within organization

Outside organization

Alarms by Type

Data Hoarding
Packet Flood
High Traffic
Data Exfiltration

Summary of aggregated host information
Observed communication patterns
Historical alarming behavior
Encrypted Traffic Analytics
Encrypted Traffic Analytics (ETA)
Visibility and malware detection with decryption

Malware in Encrypted Traffic

Is the payload within the TLS session malicious?
- End to end confidentiality
- Channel integrity during inspection
- Adapts with encryption standards

Cryptographic compliance

How much of my digital business uses strong encryption?
- Audit for TLS policy violations
- Passive detection of Ciphersuite vulnerabilities
- Continuous monitoring of network opacity
Detect malware in encrypted traffic

Initial data packet
Make the most of the unencrypted fields

Sequence of packet lengths and times
Identify the content type through the size and timing of packets

Global Risk Map
Know who’s who of the Internet’s dark side
Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic
Accelerated Threat Response
Cisco Identity Services Engine (ISE)

Network and User Context
- Who
- What
- Where
- When
- How

Stealthwatch Security Analytics

Send contextual data collected from users, devices, and network to Stealthwatch Enterprise for advanced insight
Rapid Threat Containment
Without any business disruption

Context

Quarantine or Unquarantine infected host

Information shared with other network and security products

Mitigation

Cisco® Identity Services Engine

Stealthwatch Management Console
Stealthwatch Enterprise Architecture and integrations
Stealthwatch Management Console (SMC)
- A physical or virtual appliance that aggregates, organizes, and presents analysis from Flow Collectors, Identity Services Engine (ISE), and other sources
- User interface to Stealthwatch
- Maximum 2 per deployment

Flow Collector (FC)
- A physical or virtual appliance that aggregates and normalizes NetFlow and application data collected from exporters such as routers, switches, and firewalls
- High performance NetFlow / SFlow / IPFIX Collector
- Maximum 25 per deployment

Flow Rate License
- Collection, management, and analysis of telemetry by Stealthwatch Enterprise
- The Flow Rate License is simply determined by the number/type of switches, routers, firewalls and probes present on the network
Comprehensive visibility and security analytics

Stealthwatch Enterprise architecture

- **ISE**
- **Threat Intelligence License**
- **Cognitive Intelligence**
- **Management Console**
- **Flow Collector**
- **Flow Sensor**
- **Stealthwatch Cloud**
- **Hypervisor with Flow Sensor VE**
- **UDP Director**
- **NetFlow**
- **Telemetry for Encrypted Traffic Analytics**
- **NetFlow enabled routers, switches, firewalls**
- **Endpoint License**
- **Proxy Data**
- **Non-NetFlow enabled equipment**
- **Other Traffic Analysis Software**

NetFlow enabled routers, switches, firewalls

Stealthwatch Cloud with Flow Sensor VE

Hypervisor with Flow Sensor VE

Flow Collector
Solution lifecycle for Cisco Stealthwatch Enterprise and Stealthwatch Customer Experience

Visibility
- Error free deployment
- Highest performance flow collection
- Train your staff
- 24x7 Customer Support

Detection
- Adopt and improve threats detection fidelity
- Reduce time to detection and response of threats
- Tactical workshops for use cases

Utilization
- Integrate with your incident response plan
- Integrate with your telemetry stack
- Virtual labs and e-learning courses
- 24x7 Customer Support
How Stealthwatch CX has helped

Provide network visibility across IT network

Challenges

• SIEM integration with Stealthwatch Enterprise is extremely difficult to do on your own
• Many SOC teams place strong emphasis on working out of a SIEM
• SIEM is viewed as the “single pane of glass” for their security workflow

Results

• Through an extended set of REST API capabilities that are installed for the customer, Professional Services works directly with the customer to understand their investigation workflow
• Integrate these API capabilities into their SIEM through either apps, add-ons, or right-click pivot capabilities
• Reduce the mean time to resolution for customers by enriching the data they use for investigation with Cisco Stealthwatch data
• Provide a clearer picture as to the nature and behaviour of the suspicious host in question, giving them a higher degree of accuracy in securing their networks faster.
Demo
Say hello to the future.

Cisco Connect 2019
Malaysia, Kuala Lumpur · 18 April 2019
#CiscoConnectMY