Stealthwatch

Kerry Armistead
Director of Product Management
Agenda

• Threat Landscape

• Stealthwatch

• Encrypted Traffic Analytics

• Stealthwatch Cloud

• Cisco Stealthwatch Online Visibility Assessment
Digital business has expanded the attack surface

Enterprise Mobility
- 90% of organizations are not “fully aware” of the devices accessing their network

Cloud
- By 2020, 85% of third-party cloud apps fall in the medium to high-risk category

Acquisitions & Partnerships
- 2/3 By 2020, traffic from wireless and mobile devices that will account for total IP traffic

Internet of Things
- By 2020, 80% of all traffic will be encrypted

Encrypted Traffic
- 21B
  - By 2020, IoT devices that will access the network

Enterprise Mobility
- 101010
  - By 2020, 90% of organizations are not “fully aware” of the devices accessing their network

Enterprise Mobility
- 101010
Network threats are getting smarter

Motivated and targeted adversaries
- State sponsored
- Financial/espionage motives
- $1T cybercrime market

Insider Threats
- Compromised credentials
- Disgruntled employees
- Admin/privileged accounts

Increased attack sophistication
- Advanced persistent threats
- Encrypted malware
- Zero-day exploits

Industry average detection time for a breach: 191 DAYS
Industry average time to contain a breach: 66 DAYS
Average cost of a data breach: $3.62M

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Highly Confidential
Effective security depends on total visibility

- **KNOW** every host
- **SEE** every conversation
- Understand what is **NORMAL**
- Be alerted to **CHANGE**
- Respond to **THREATS** quickly

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Highly Confidential
Cisco Stealthwatch: Scalable visibility and security analytics

Most comprehensive visibility for effective security outcomes

- Advanced Threat Detection
- Accelerated Threat Response
- Simplified Network Segmentation

Using existing network infrastructure

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Highly Confidential
Industry-leading Security Analytics
Behavioral and anomaly detection

**Collect and analyze telemetry**
- Flows

**Create a baseline of normal behavior**
- ~100 Security Events
  - Number of concurrent flows
  - Packet per second
  - Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of SYNs received
- Rate of connection resets
- Duration of the flow

**Alarm on anomalies and behavioral changes**
- Approximate time required to complete baseline
- Exchange Servers

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Highly Confidential
Power of multi-layer machine learning

Increase fidelity of detection using best-in-class security analytics

Requests received
- Anomaly detection
- Trust modeling
- Event classification
- Entity modeling
- Relationship modeling

Global Risk Map
Threat Grid, TALOS

Confirmed Incidents = 0.01% of Requests

Anomalous Traffic
Malicious Events
Threat Incidents

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Highly Confidential
Advanced Threat Detection
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

<table>
<thead>
<tr>
<th>Concern Index</th>
<th>Target Index</th>
<th>Recon</th>
<th>C&amp;C</th>
<th>Exploitation</th>
<th>DDoS Source</th>
<th>DDoS Target</th>
<th>Data Hoarding</th>
<th>Exfiltration</th>
<th>Policy Violation</th>
<th>Anomaly</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Insider threat example: data hoarding

Suspect Data Hoarding
Unusually large amount of data \textit{inbound} from other hosts

Target Data Hoarding
Unusually large amount of data \textit{outbound} from a host to multiple hosts
Insider threat example: data exfiltration

Data Exfiltration
Unusually large amount of data outbound from a host to one or more external hosts
Accelerated Threat Response

Pinpoint the source of the threat through visibility into each host

Conduct forensic investigations into past events by analyzing the network audit trails

Mitigate threats easily without business shutdown by using the network
Investigate threats quickly

- Contextual user and application info
- Top security alarms by hosts
- Drill-down into telemetry associated with security events
- Malware propagation through infected hosts
- Network audit trails for deeper forensics on past/long-running events
Mitigate threats effectively

Investigation

Mitigation

An alarm can have an associated response
- Notify in the alarm table
- Generate an email
- Generate a syslog message to a SIEM

Quarantine identified threats using the network
Detect and respond to advanced threats

Data hoarding and Data Exfiltration

- Alarm triggered
- Device identified
- Additional info determined
  - Name
  - Location
  - MAC address
  - Last seen
  - Policies
  - Host Group
- User identified

- Forensic investigation conducted
- Threat removed from network
- What kind of data was transmitted?
- Where is the data being transmitted?

Reduce incident response time from months to hours
# Stealthwatch is available across all deployment methods

<table>
<thead>
<tr>
<th>Stealthwatch Cloud</th>
<th>Stealthwatch On-Prem</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public</strong> cloud monitoring</td>
<td><strong>On-Prem</strong> network monitoring</td>
</tr>
<tr>
<td>Any business using public cloud infrastructure</td>
<td>Enterprise &amp; commercial customers</td>
</tr>
<tr>
<td>Monitors public cloud via SaaS</td>
<td>Monitor private network via on-premises virtual or hardware appliance</td>
</tr>
<tr>
<td>Complements Cisco Enterprise and Private Network offering</td>
<td>Complements Cisco public cloud offering</td>
</tr>
<tr>
<td>SMB &amp; commercial companies</td>
<td></td>
</tr>
<tr>
<td>Monitors private network via SaaS</td>
<td></td>
</tr>
<tr>
<td>Complements Cisco public cloud offering</td>
<td></td>
</tr>
</tbody>
</table>

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Highly Confidential
Encrypted Traffic Analytics
Encryption is changing the threat landscape

Based on Cisco threat grid analysis, 2017

<table>
<thead>
<tr>
<th>Month</th>
<th>Dec</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>25%</td>
<td>22%</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Gartner predicts that by 2019
80% of all traffic will be encrypted

Straight-line projection

<table>
<thead>
<tr>
<th>Year</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>16%</td>
<td>20%</td>
<td>19%</td>
</tr>
<tr>
<td>19%</td>
<td>22%</td>
<td>23%</td>
</tr>
<tr>
<td>23%</td>
<td>25%</td>
<td>27%</td>
</tr>
<tr>
<td>27%</td>
<td>30%</td>
<td>34%</td>
</tr>
<tr>
<td>34%</td>
<td>41%</td>
<td>60%</td>
</tr>
</tbody>
</table>

% of malware:
- December 2017: 22%
- January 2017: 20%
- February 2017: 19%
- March 2017: 19%
- April 2017: 19%
- May 2017: 25%

Source: Thales and Vormetric
Encrypted Traffic Analytics

Cisco Stealthwatch is the only solution providing visibility and malware detection without decryption

- Detect malware in encrypted traffic
- Ensure cryptographic compliance
### ETA studied Internet encrypted data features

Cisco research

<table>
<thead>
<tr>
<th>TCP/IP</th>
<th>DNS</th>
<th>TLS</th>
<th>SPLT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watchlist address</td>
<td>c15c0.com afb32d75.com</td>
<td>Unusual fingerprint Unusual cert</td>
<td>C2 Message Data Exfiltration Self-Signed Certificate Bestafera</td>
</tr>
<tr>
<td>Prevalent address</td>
<td>cisco.com</td>
<td>Typical fingerprint Typical cert</td>
<td>Google search</td>
</tr>
</tbody>
</table>

Malware traffic

Benign traffic
Detect malware in encrypted traffic

Initial data packet

Sequence of packet lengths and times

Global Risk Map

Make the most of the unencrypted fields

Identify the content type through the size and timing of packets

Know who’s who of the Internet’s dark side
What is Mobile World Congress?

More than 107,000 visitors from 205 countries and territories

Over 55% of attendees held senior-level positions, including more than 7,700 CEOs

Stealthwatch monitored all the wireless traffic to and from the Internet with Encrypted Traffic Analytics
We enabled ETA on an ASR1001-X with the MWC’s Internet bound traffic SPAN’ed from a distribution Cat6K switch to the ASR1001-X on a GigE port.
Summary of the traffic

Sustained flow consumption at ~20k/FlowsPerSecond
More than 55 million flows captured
  More than 29 million TCP Sessions
  More than 23 million UDP Sessions
  More than 1.8 million ICMP Sessions
Over a million streaming audio/video application
Over 850,000 flows of P2P file transfer

82% of all the web traffic was encrypted!
(19.5 million HTTPS flows, 3.5 million HTTP flows)
Over 30 applications detected to be using TLS1.0!
Detection on 2/26 and 2/27

Global Threat Analytics raised 350 events

- Cryptomining
- Android Trojans (Android.spy, Boqx, infected firmware)
- SALITY malware
- SMB Service discovery malware
- OSX Malware Genieo
- Conficker
- RevMob
- Phishing
- AdInjectors

Several Android mobile devices were identified to have an infected firmware

Malware Trojans were identified that were using **PowerShell** to communicate to the C&C servers through HTTPS.

Several malwares / potentially unwanted applications that used **Encrypted traffic**

* Over 13,500 alarms in Stealthwatch on 2/26
* Over 18,500 alarms on 2/27
What is needed for ETA?
Licensing, packaging…

<table>
<thead>
<tr>
<th>Solution Element</th>
<th>Software Version</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise switches</td>
<td>C9300: Cisco IOS® XE 16.6.1</td>
<td>Included in Cisco DNA™ Advantage license</td>
</tr>
<tr>
<td>(Cisco® Catalyst® 9000 Series)*</td>
<td>C9400: Cisco IOS® XE 16.6.2 (Oct)</td>
<td>Cisco ONE™ Advantage</td>
</tr>
<tr>
<td>Branch routers</td>
<td>Cisco IOS® XE 16.6.2 (Oct)</td>
<td>Included in SEC/k9 license</td>
</tr>
<tr>
<td>(ASR 1000 Series, 4000 Series ISR,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSR, ISRv)**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stealthwatch® On-prem</td>
<td>v6.9.2 (Available now)</td>
<td>Management Console, Flow Collector, Flow</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rate License</td>
</tr>
<tr>
<td>Stealthwatch® On-prem</td>
<td>v6.9.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptographic compliance (Q3CY17)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malware Detection (Q4CY17)</td>
<td></td>
</tr>
</tbody>
</table>

*Software support for C9500 is current on roadmap.

**Available for Proof of Concept (PoC) with 16.6.1, General availability in 16.6.2 (Oct)
Cisco Stealthwatch Cloud

Technical Decision Maker
# Stealthwatch Cloud

<table>
<thead>
<tr>
<th>Public cloud monitoring</th>
<th>Private network monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any business using public cloud infrastructure</td>
<td>SMB &amp; commercial companies</td>
</tr>
<tr>
<td>Monitors public cloud via SaaS</td>
<td>Monitors private network via SaaS</td>
</tr>
<tr>
<td>Complements Cisco Enterprise and Private Network offering</td>
<td>Complements Cisco public cloud offering</td>
</tr>
</tbody>
</table>
Quick and easy security for dynamic environments

Stealthwatch Cloud

- VPC Flow Logs
- Other data sources

Public Cloud

- NetFlow
- Mirror port
- Other data sources
Cover your *entire* cloud attack surface with ease

*AWS Flow Logs*

- AWS
  - VPC Flow Logs
- Stealthwatch Cloud
- Additional AWS Data Sources
  - Cloud Trail
  - Cloud Watch
  - Inspector
  - IAM
  - Config
  - Lambda
Detect threats and see network activity using existing telemetry sources

*Virtual Sensors*

Use DNS Lookups to link dynamics IPs to a host name

Collect from all these sources:
- NetFlow
- DNS
- SIEM
- Active Directory
- IPFIX
- Gigamon
- Any Mirror/SPAN

Stealthwatch Cloud

DNS Lookup

IP Traffic Data

Other Security Data

Switches

Firewalls

Mirror/Span Ports

Load Balancers

Application Servers

Threat Detection

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Using modeling to detect security events

**Dynamic Entity Modeling**

- **Collect Input**
  - IP Meta Data
  - System Logs
  - Security Events
  - Passive DNS
  - External Intel
  - Vulnerability Scans
  - Config Changes

- **Perform Analysis**
  - Role
    - What is the role of the device?
  - Group
    - What ports/protocols does the device continually access?
  - Consistency
    - What connections does it continually make?
  - Rules
    - Does it communicate internally only?
      - What countries does it talk to?
  - Forecast
    - How much data does the device normally send/receive?

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Get the full benefit of the cloud

SaaS-based security

- Easy to use and deploy
- Centrally managed
- Flexible pricing
- Secure data storage
- Automatically scale
Manage everything from a simple SaaS portal

SaaS Management Portal

- Unlimited users
- No patching necessary
- Available anywhere
- New features added monthly
- Support available
Start today with a free 60-day trial

Schedule consultation with a security specialist

See results within hours

Learn more: cisco.com/go/stealthwatch-cloud
Security Online Visibility Assessment
Are you compromised today?

• What are your risk areas?
Common areas of risk

- Largest risk areas are often things you think are already covered
- Lack of visibility allows risky activity to continue

Can you see...

- Threats in encrypted traffic
- Server message block (SMB) traffic
- Risky DNS traffic
- Remote access breaches
- Unclassified and unknown internal servers
- Internal and external telnet activity
- Traffic to high risk countries
Cisco Security Online Visibility Assessment

A free, 14-day risk assessment

Focused on common areas of security risk

Provides an immediately actionable, detailed report
The Report

- Detailed results
- Can identify areas of risk and active threats
- Provide actionable intelligence to help you adjust security policies and guide purchase decisions

The Report

DNS Risk

Overview

DNS servers are critical to normal network function as they translate URLs to IP addresses. Many organizations utilize specific DNS servers to safeguard their network and enforce policies. When a host is found to be using an unauthorized DNS server, it could indicate malicious activity or policy violation. Malware may change a host’s DNS server to forward request to sites used for phishing or exploit delivery. Likewise, network users may utilize unauthorized DNS servers to access web resources forbidden by internal policies.

Unauthorized DNS servers can:
- Direct hosts to bad websites to download malware or exploitation tools
- Prevent monitoring of DNS traffic for data loss, command and control activity and exploitation
- Control or block access to software updates from vendors

Notes

Deploying Cisco Umbrella will allow for better protecting DNS traffic and preventing DNS hijacking.

<table>
<thead>
<tr>
<th>DNS SERVER</th>
<th>BYTES</th>
<th>CLIENTS</th>
<th>FLOWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.6.1.162</td>
<td>719.1 MB</td>
<td>3</td>
<td>42887</td>
</tr>
<tr>
<td>192.175.48.6</td>
<td>682.6 MB</td>
<td>3</td>
<td>40060</td>
</tr>
<tr>
<td>192.175.48.42</td>
<td>661.6 MB</td>
<td>3</td>
<td>38690</td>
</tr>
<tr>
<td>198.6.1.210</td>
<td>540.8 MB</td>
<td>3</td>
<td>32910</td>
</tr>
<tr>
<td>192.102.198.240</td>
<td>243.4 MB</td>
<td>3</td>
<td>32632</td>
</tr>
</tbody>
</table>

Potential Hosts at Risk of Exposure, DNS Malware, or Data Loss

<table>
<thead>
<tr>
<th>HOST</th>
<th>BYTES</th>
<th>CLIENTS</th>
<th>FLOWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.182.184.2</td>
<td>4.5 GB</td>
<td>14477</td>
<td>4599824</td>
</tr>
<tr>
<td>10.201.0.16</td>
<td>3.5 GB</td>
<td>14432</td>
<td>3618404</td>
</tr>
<tr>
<td>10.10.30.16</td>
<td>1.5 GB</td>
<td>9499</td>
<td>1578488</td>
</tr>
<tr>
<td>10.10.30.15</td>
<td>83.3 MB</td>
<td>4</td>
<td>56878</td>
</tr>
<tr>
<td>209.182.185.222</td>
<td>471.1 kB</td>
<td>4</td>
<td>644</td>
</tr>
</tbody>
</table>
Ready to start?

Schedule consultation with a security specialist

Learn more: cisco.com/go/stealthwatch-free-assessment