Security Forensics with EndaceProbe and Cisco Security

cisco Solution Partner

Combining EndaceProbes with Cisco Secure Firewall Threat Defense (FTD) streamlines investigation workflows for rapid response to security threats.

Cisco® Security products provide continuous threat protection before, during and after an attack.

The Cisco Firewall Management Center (FMC) is the "nerve center" of the security ecosystem. It correlates attacks with real-time network and user intelligence and centrally manages network security and operational functions, including event monitoring, incident prioritization, forensic analysis and reporting.

When it comes to investigating security incidents, access to an accurate, detailed and complete history of network traffic is an unparalleled resource. Detailed packet history provides definitive evidence of what happened, how it happened and what was compromised. It provides the context behind the security alerts raised by Cisco Firewall Threat Detection (FTD) and lets analysts investigate events quickly and respond with the confidence of knowing exactly what took place.

EndaceProbe™ Analytics Platforms capture, index and store network traffic with 100% accuracy, regardless of network speeds, loads or traffic types. Deploying EndaceProbes alongside FTD appliances or hosting virtual FTD (FTDv) on EndaceProbes in Application Dock™, ensures a complete, hi-fidelity history of network activity is immediately available for security investigations. Packets are timestamped to nanosecond level accuracy, ensuring accurate event reconstruction even for ultra-short-lived events.

Streamlining Security Investigations

The Network History recorded by EndaceProbes can be integrated with FTD using the Pivot-To-Vision™ function of the EndaceProbe's powerful API. Pivot-To-Vision lets security analysts pivot directly from alerts in the FMC dashboard to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

Using the IP address and time range of the trigger, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect and review terabytes of network history down to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

Being able to get directly to the related packets lets security analysts quickly and conclusively establish the root cause of issues and respond appropriately, dramatically reducing the time to investigate and resolve critical incidents.

PRODUCTS

Cisco Firewall Management Center (FMC)

Cisco Firewall Threat Defense (FTD)

EndaceProbe Analytics Platforms

Endace Fusion Connector for Cisco Security

BENEFITS

- Accurate, granular and complete network history provides definitive evidence for security analysts
- Streamlined investigation workflow improves SecOps efficiency and ensures faster investigations
- More effective detection tuning reduces false-positives
- Network packets provide a definitive evidentiary trail

FURTHER INFORMATION

https://www.endace.com/cisco

Access to a 100% accurate record of network history, and a streamlined investigation workflow, enables SecOps analysts to quickly identify, prioritize and respond to real threats and flag false positives for detection tuning.

Increasing Detection Visibility with Application Dock

Cisco FTDv can be hosted in the EndaceProbe's Application Dock built-in hosting environment. Every packet captured and recorded by the EndaceProbe can also be streamed to hosted FTDv instances in real-time.

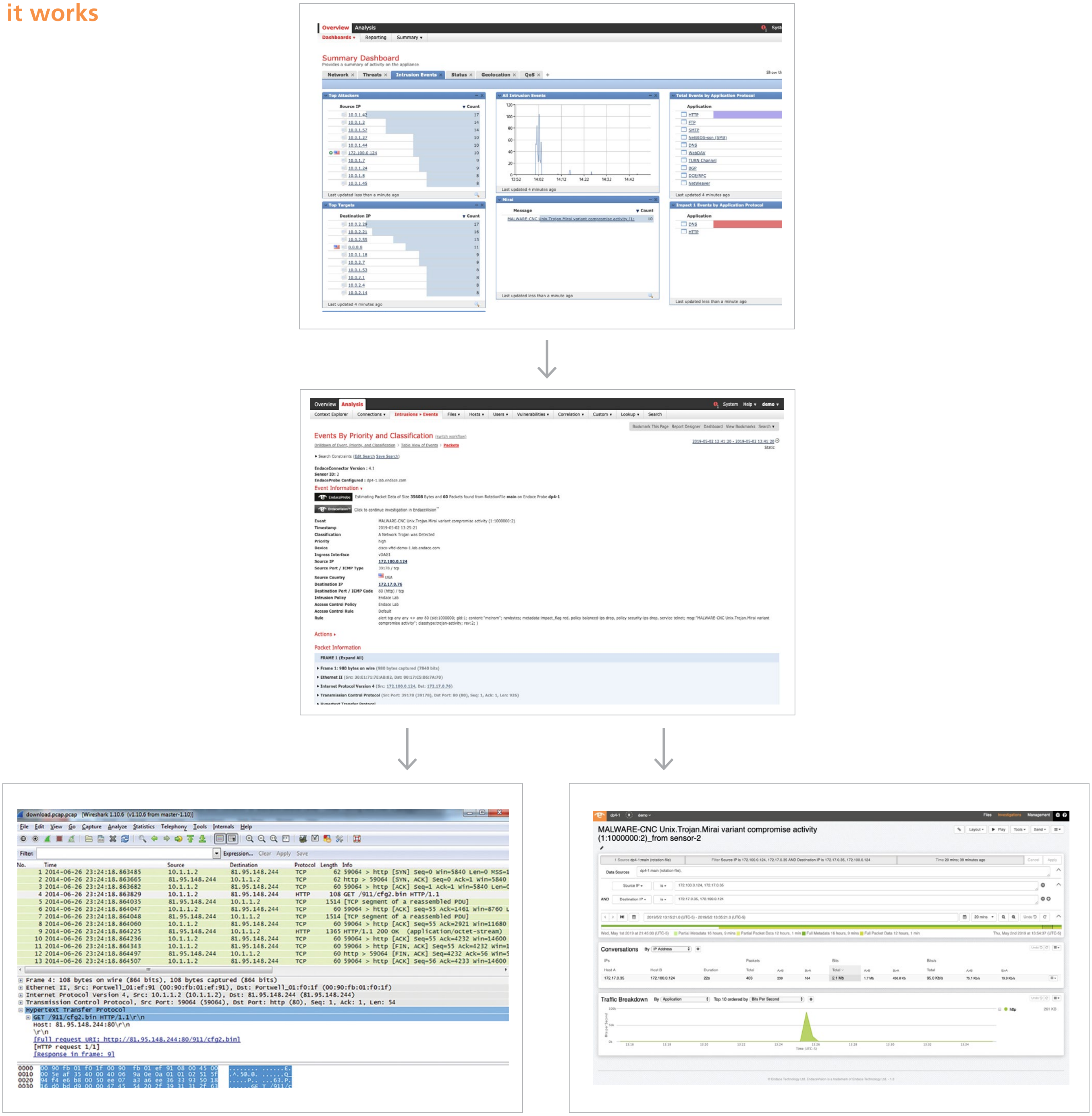
Security Operations teams can dynamically deploy FDTv anywhere on the network that they have EndaceProbe Network Recorders deployed, allowing them to increase their detection footprint without truck rolls or lengthy hardware deployments.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when the hosted FTDv instance is processing heavy traffic loads.

Conclusion

Recorded network history provides the high-fidelity packet-level detail necessary for the conclusive investigation of security incidents. The combination of EndaceProbe Network Recorders and Cisco Security delivers a powerful, end-to-end detection, alerting and investigation solution. It gives SecOps teams industry-leading security monitoring and alerting, with access to the detailed data they need for fast, conclusive threat investigation and response.

How it works



Overview | Analysis
Dashboards ▾ | Reporting | Summary ▾

Summary Dashboard
Provides a summary of activity on the appliance

Network × | Threats × | Intrusion Events × | Status × | Geolocation × | QoS × | +

Top Attackers

Source IP	Count
10.0.1.42	17
10.0.1.2	14
10.0.1.57	14
10.0.1.27	10
10.0.1.44	10
172.100.0.124	10
10.0.1.7	9
10.0.1.24	9
10.0.1.8	8
10.0.1.45	8

Last updated less than a minute ago

Top Targets

Destination IP	Count
10.0.2.29	17
10.0.2.21	16
10.0.2.55	13
8.8.8.8	11
10.0.1.18	9
10.0.2.7	9
10.0.1.53	8
10.0.2.1	8
10.0.2.4	8
10.0.2.14	8

Last updated 4 minutes ago

Last updated 4 minutes ago

Mirai

Message	Count
MALWARE-CNC Unix.Trojan.Mirai variant compromise activity (1:	10

Last updated less than a minute ago

Total Events by Application Protocol

Application: HTTP, FTP, SMTP, NetBIOS-ssn (SMB), DNS, WebDAV, TURN Channel, BGP, DCE/RPC, NetWeaver

Last updated 4 minutes ago

Impact 1 Events by Application Protocol

Application: DNS, HTTP

Last updated less than a minute ago

Overview | Analysis | System | Help ▾ | demo ▾
Context Explorer | Connections ▾ | Intrusions ▸ Events | Files ▾ | Hosts ▾ | Users ▾ | Vulnerabilities ▾ | Correlation ▾ | Custom ▾ | Lookup ▾ | Search
Bookmark This Page | Report Designer | Dashboard | View Bookmarks | Search ▾

Events By Priority and Classification (switch workflow)
Drilldown of Event, Priority, and Classification › Table View of Events › Packets
2019-05-02 12:41:20 - 2019-05-02 13:41:20
Static

▸ Search Constraints (Edit Search Save Search)

EndaceConnector Version : 4.1
Sensor ID: 2
EndaceProbe Configured : dp4-1.lab.endace.com

Event Information ▾

EndaceProbe Estimating Packet Data of Size **35608** Bytes and **60** Packets found from RotationFile **main** on Endace Probe **dp4-1**

EndaceVision™ Click to continue investigation in EndaceVision™

Event	MALWARE-CNC Unix.Trojan.Mirai variant compromise activity (1:1000000:2)
Timestamp	2019-05-02 13:25:21
Classification	A Network Trojan was Detected
Priority	high
Device	cisco-vftd-demo-1.lab.endace.com
Ingress Interface	vDAG1
Source IP	172.100.0.124
Source Port / ICMP Type	39178 / tcp
Source Country	USA
Destination IP	172.17.0.76
Destination Port / ICMP Code	80 (http) / tcp
Intrusion Policy	Endace Lab
Access Control Policy	Endace Lab
Access Control Rule	Default
Rule	alert tcp any any <> any 80 (sid:1000000; gid:1; content:"meinsm"; rawbytes; metadata:impact_flag red, policy balanced-ips drop, policy security-ips drop, service telnet; msg:"MALWARE-CNC Unix.Trojan.Mirai variant compromise activity"; classtype:trojan-activity; rev:2;)

Actions ▸

Packet Information

FRAME 1 (Expand All)

▸ **Frame 1: 980 bytes on wire** (980 bytes captured (7840 bits)
▸ **Ethernet II** (Src: 30:E1:71:7E:AB:82, Dst: 00:17:C5:B6:7A:70)
▸ **Internet Protocol Version 4** (Src: 172.100.0.124, Dst: 172.17.0.76)
▸ **Transmission Control Protocol** (Src Port: 39178 (39178), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 926)
▸ Hypertext Transfer Protocol

download.pcap.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

```
No.   Time                        Source          Destination     Protocol Length Info
    1 2014-06-26 23:24:18.863485  10.1.1.2        81.95.148.244   TCP        62 59064 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1
    2 2014-06-26 23:24:18.863665  81.95.148.244   10.1.1.2        TCP        62 http > 59064 [SYN, ACK] Seq=0 Ack=1 Win=5840
    3 2014-06-26 23:24:18.863682  10.1.1.2        81.95.148.244   TCP        60 59064 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
    4 2014-06-26 23:24:18.863829  10.1.1.2        81.95.148.244   HTTP      108 GET /911/cfg2.bin HTTP/1.1
    5 2014-06-26 23:24:18.864035  81.95.148.244   10.1.1.2        TCP      1514 [TCP segment of a reassembled PDU]
    6 2014-06-26 23:24:18.864047  10.1.1.2        81.95.148.244   TCP        60 59064 > http [ACK] Seq=55 Ack=1461 Win=8760 L
    7 2014-06-26 23:24:18.864048  81.95.148.244   10.1.1.2        TCP      1514 [TCP segment of a reassembled PDU]
    8 2014-06-26 23:24:18.864060  10.1.1.2        81.95.148.244   TCP        60 59064 > http [ACK] Seq=55 Ack=2921 Win=11680
    9 2014-06-26 23:24:18.864225  81.95.148.244   10.1.1.2        HTTP     1365 HTTP/1.1 200 OK  (application/octet-stream)
   10 2014-06-26 23:24:18.864236  10.1.1.2        81.95.148.244   TCP        60 59064 > http [ACK] Seq=55 Ack=4232 Win=14600
   11 2014-06-26 23:24:18.864343  10.1.1.2        81.95.148.244   TCP        60 59064 > http [FIN, ACK] Seq=55 Ack=4232 Win=1
   12 2014-06-26 23:24:18.864497  81.95.148.244   10.1.1.2        TCP        60 http > 59064 [FIN, ACK] Seq=4232 Ack=56 Win=5
   13 2014-06-26 23:24:18.864507  10.1.1.2        81.95.148.244   TCP        60 59064 > http [ACK] Seq=56 Ack=4233 Win=14600

⊞ Frame 4: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
⊞ Ethernet II, Src: Portwell_01:ef:91 (00:90:fb:01:ef:91), Dst: Portwell_01:f0:1f (00:90:fb:01:f0:1f)
⊞ Internet Protocol Version 4, Src: 10.1.1.2 (10.1.1.2), Dst: 81.95.148.244 (81.95.148.244)
⊞ Transmission Control Protocol, Src Port: 59064 (59064), Dst Port: http (80), Seq: 1, Ack: 1, Len: 54
⊟ Hypertext Transfer Protocol
  ⊞ GET /911/cfg2.bin HTTP/1.1\r\n
    Host: 81.95.148.244:80\r\n
    \r\n
    [Full request URI: http://81.95.148.244:80/911/cfg2.bin]
    [HTTP request 1/1]
    [Response in frame: 9]

0000  00 90 fb 01 f0 1f 00 90  fb 01 ef 91 08 00 45 00   ........ ......E.
0010  00 5e af 35 40 00 40 06  9a 0e 0a 01 01 02 51 5f   .^.5@.@. ......Q_
0020  94 f4 e6 b8 00 50 ee 07  a3 a6 ee 36 33 93 50 18   .....P.. ...63.P.
0030  16 d0 bd d9 00 00 47 45  54 20 2f 39 31 31 2f 63   ......GE T /911/c
```

dp4-1 | demo | Files | Investigations | Management

MALWARE-CNC Unix.Trojan.Mirai variant compromise activity (1:1000000:2)_from sensor-2

1 Source dp4-1:main (rotation-file) | Filter Source IP is 172.100.0.124, 172.17.0.35 AND Destination IP is 172.17.0.35, 172.100.0.124 | Time 20 mins; 39 minutes ago

Data Sources: dp4-1:main (rotation-file),
Source IP ▾ is ▾ 172.100.0.124, 172.17.0.35
AND Destination IP ▾ is ▾ 172.17.0.35, 172.100.0.124
2019/5/2 13:15:21.0 (UTC-5) - 2019/5/2 13:35:21.0 (UTC-5) | 20 mins | Undo

Wed, May 1st 2019 at 21:45:00 (UTC-5) Partial Metadata 16 hours, 9 mins Partial Packet Data 12 hours, 1 min Full Metadata 16 hours, 9 mins Full Packet Data 12 hours, 1 min Thu, May 2nd 2019 at 13:54:37 (UTC-5)

Conversations By IP Address

IPs			Packets			Bits			Bits/s		
Host A	Host B	Duration	Total	A>B	B>A	Total	A>B	B>A	Total	A>B	B>A
172.17.0.35	172.100.0.124	22s	403	239	164	2.1 Mb	1.7 Mb	436.8 Kb	95.0 Kb/s	75.1 Kb/s	19.9 Kb/s

Traffic Breakdown By Application Top 10 ordered by Bits Per Second

© Endace Technology Ltd. EndaceVision is a trademark of Endace Technology Ltd. - 1.3

Figure 1 - Streamlined workflow from an alert in the Cisco FMC, to the alert detail, to related packets or network visualizations.

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com