BluVector and Endace

BLUVECTOR®
A COMCAST COMPANY

Combine a next-generation Intrusion Detection System, powered by AI with full network visibility for confident, rapid threat response.

Combining BluVector and Endace gives analysts a platform that detects even the most advanced threats in real time and provides a full understanding of the threat through detailed context and packet-level Network History.

BluVector® Cortex™ is a next-generation Intrusion Detection System that accurately and efficiently detects, triages and responds to threats including ransomware, fileless malware, and zero-day malware in real time.

At the heart of BluVector Cortex are three components:

- A pair of AI-based detection engines that process traffic to detect file-based and fileless threats.
- Intelligent Decision Support that delivers context and visibility to threat security teams and their investigations by pre-correlating and highlighting log entries associated with events prioritized for analysis.
- An extensible Connectors Framework that automates the hunt process, orchestrates response to threats, and enables easy integration of additional security solutions.

EndaceProbe™ Network Analytics Platforms capture, index and store network traffic with 100% accuracy while simultaneously hosting a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment. Customers can extend their security monitoring capability by deploying BluVector Cortex instances anywhere they have EndaceProbes deployed. Hosted instances can analyze recorded traffic in real time at full line-rate or analyze recorded Network History for back-in-time investigation.

Accelerating Security Investigations

The Network History recorded by EndaceProbes can be integrated into BluVector Cortex using the Pivot-to-Vision™ function of the EndaceProbe API. Pivot-to-Vision lets security analysts pivot from threat alerts in BluVector Cortex directly 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 event, Pivot-to-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect, review and extract the relevant traffic from the terabytes of Network History recorded on the network.

It enables analysis to microsecond level with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

PRODUCTS

BluVector Cortex

EndaceProbe with Application Dock

BENEFITS

- Detect file-based and fileless malware on the network in real time
- Extend threat visibility by deploying BluVector Cortex on EndaceProbes on the network
- Neutralize threats quickly and efficiently with streamlined investigation workflows.
- Rapid, conclusive and actionable investigations with one-click drill-down to packet-level detail.
- Reduce threat exposure through improved analyst productivity and faster incident investigation.
- Access a definitive evidence trail with an accurate record of all relevant packets.
- Bridge the gap between NetOps and SecOps by giving both teams the ability to rapidly make critical decisions using a shared source of definitive Network History
- Use investigation results to continuously retrain the supervised Machine Learning Engine

Being able to get directly to the related packets with a single click lets security analysts rapidly establish the root cause of issues. They can respond quickly, dramatically reducing the time to resolve critical incidents and minimizing the risk of security threats escalating to become more serious breaches.

Scaling Deployment with BluVector Cortex and Application Dock

BluVector Cortex can be hosted on EndaceProbes. Every packet captured and recorded by the EndaceProbe can be simultaneously streamed to hosted BluVector Cortex virtual appliances in real time.

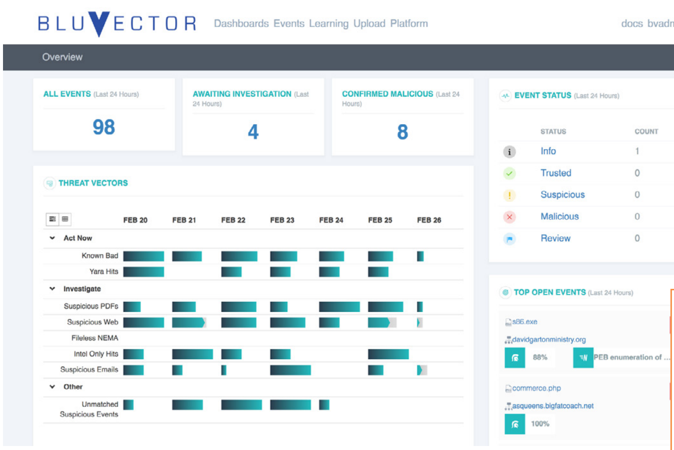
Security Operations teams can dynamically deploy AI-based, sense and respond BluVector Cortex instances anywhere on the network they have EndaceProbes deployed, allowing them to gain advanced threat detection on demand without additional hardware rollouts.

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 BluVector Cortex instances are processing heavy traffic loads.

Conclusion

By deploying BluVector Cortex instances to EndaceProbes in Application Dock, security teams can extend their reach easily, leveraging existing EndaceProbe hardware deployments to extend security monitoring and network recording capability. The combined Endace and BluVector solution provides state-of-the-art detection and definitive evidence to enable rapid remediation with absolute confidence.

How it works



BLUVECTOR Dashboards Events Learning Upload Platform docs bvadmin

Overview

ALL EVENTS (Last 24 Hours) 98

AWAITING INVESTIGATION (Last 24 Hours) 4

CONFIRMED MALICIOUS (Last 24 Hours) 8

EVENT STATUS (Last 24 Hours)

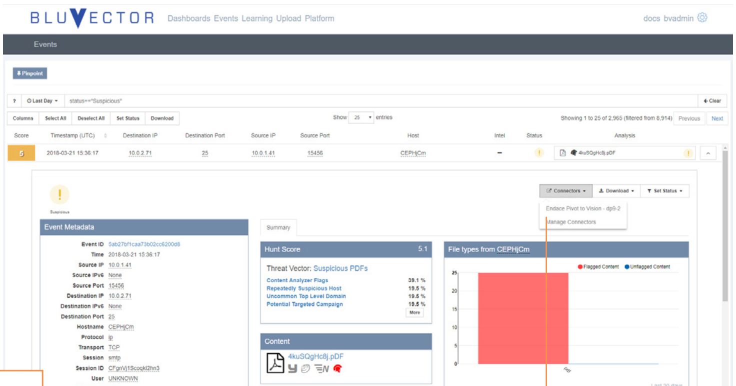
STATUS	COUNT
Info	1
Trusted	0
Suspicious	0
Malicious	0
Review	0

TOP OPEN EVENTS (Last 24 Hours)

s86.exe
davidgartonministry.org
88%
PEB enumeration of ...
commerce.php
asqueens.bigfatcoach.net
100%

Figure 1. The BluVector Cortex Console shows an overview of all detected events

Figure 2. From an event, analysts can select Connectors to go directly to the related packets in EndaceVision



BLUVECTOR Dashboards Events Learning Upload Platform docs bvadmin

Events

status=="Suspicious"

Show 25 entries

Showing 1 to 25 of 2,965 (filtered from 8,914)

Score	Timestamp (UTC)	Destination IP	Destination Port	Source IP	Source Port	Host	Intel	Status	Analysis
5	2018-03-21 15:36:17	10.0.2.71	25	10.0.1.41	15456	CEPHjCm	–	!	4kuSQgHc8j.pDF

Suspicious

Event Metadata

Event ID	5ab27bf1caa73b02cc6200d8
Time	2018-03-21 15:36:17
Source IP	10.0.1.41
Source IPv6	None
Source Port	15456
Destination IP	10.0.2.71
Destination IPv6	None
Destination Port	25
Hostname	CEPHjCm
Protocol	ip
Transport	TCP
Session	smtp
Session ID	CFgnVj1ScoqkI2hn3
User	UNKNOWN
File Bytes	569
Partial File	False

Hunt Score 5.1

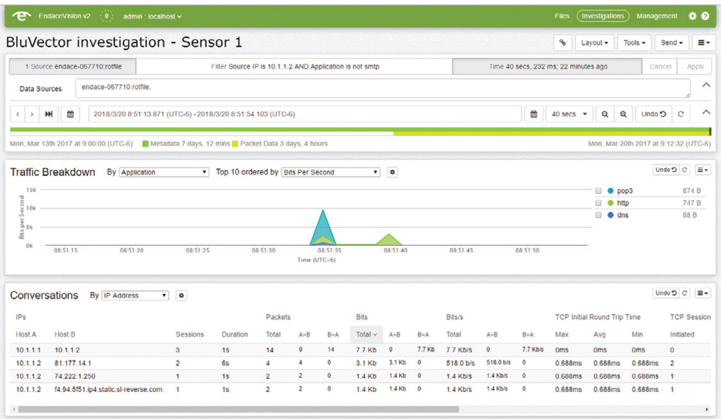
Threat Vector: Suspicious PDFs

Content Analyzer Flags	39.1 %
Repeatedly Suspicious Host	19.5 %
Uncommon Top Level Domain	19.5 %
Potential Targeted Campaign	19.5 %

More

Content

4kuSQgHc8j.pDF



BluVector investigation - Sensor 1

1 Source endace-067710:rotfile

Filter Source IP is 10.1.1.2 AND Application is not smtp

Time 40 secs, 232 ms; 22 minutes ago

Data Sources endace-067710:rotfile,

2018/3/20 8:51:13.871 (UTC-6) - 2018/3/20 8:51:54.103 (UTC-6)

40 secs

Undo

Mon, Mar 13th 2017 at 9:00:00 (UTC-6) Metadata 7 days, 12 mins Packet Data 3 days, 4 hours Mon, Mar 20th 2017 at 9:12:32 (UTC-6)

Traffic Breakdown By Application Top 10 ordered by Bits Per Second

pop3	874 B
http	747 B
dns	88 B

Conversations By IP Address

IPs				Packets			Bits			Bits/s			TCP Initial Round Trip Time			TCP Session
Host A	Host B	Sessions	Duration	Total	A>B	B>A	Total	A>B	B>A	Total	A>B	B>A	Max	Avg	Min	Initiated
10.1.1.1	10.1.1.2	3	1s	14	0	14	7.7 Kb	0	7.7 Kb	7.7 Kb/s	0	7.7 Kb/s	0ms	0ms	0ms	0
10.1.1.2	81.177.14.1	2	6s	4	4	0	3.1 Kb	3.1 Kb	0	518.0 b/s	518.0 b/s	0	0.688ms	0.688ms	0.688ms	2
10.1.1.2	74.222.1.250	1	1s	2	2	0	1.4 Kb	1.4 Kb	0	1.4 Kb/s	1.4 Kb/s	0	0.688ms	0.688ms	0.688ms	1
10.1.1.2	f4.94.5f51.ip4.static.sl-reverse.com.	1	1s	2	2	0	1.4 Kb	1.4 Kb	0	1.4 Kb/s	1.4 Kb/s	0	0.688ms	0.688ms	0.688ms	1

Figure 3. Examine related packet history in EndaceVision, view packet-level detail in EndacePackets or download packet capture file for archival or analysis.

RoHS Compliant

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

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

For further information, email: info@endace.com