WEBROOT
Smarter Cybersecurity™

FlowScape®
Accelerated Network Threat Detection

Uncovering high risk events with network behavioral analytics

Written by

Thomas Caldwell
Senior Director, Software Development
Webroot

Table of Contents

Introduction

In many fields, 95% effectiveness is considered a high rate of success. This is not the case when it comes to cybersecurity. In fact, the security deficiencies and blind spots that comprise the remaining 5% are the loopholes sophisticated attackers target to infiltrate organizations. In the case of a smart city, that 5% vulnerability opens up their critical infrastructure, police, fire, finance, and more to attacks from organized crime, hacktivist groups, and the most persistent nation states. Additionally, they're vulnerable to insider threats from vendor partners and employees.

To be truly effective against modern threats, security analysts must uncover high risk activities during the reconnaissance phase of an attack. Unfortunately, today's security personnel are often overwhelmed by alerts, allowing advanced persistent threats (APTs) to work low and slow to hide within everyday network noise. Modern organizations need a new security solution that uses advanced machine learning and contextual threat intelligence; that spans domains; that provides insight into endpoint-to-endpoint network activity, in addition to incoming and outgoing traffic; and that is both cost effective and easy to implement.

The Webroot FlowScape® network behavioral analytics solution is next-generation, virtualized security solution that uses sophisticated machine learning to provide continuous visibility into any anomalous behavior within networks. It continually examines and learns network and system behaviors to alert security analysts on anomalous high-risk activity, in real time, without creating unnecessary alerts. Our smarter approach enables partners to solve the "95% problem" with comprehensive protection across computers, mobile devices, servers, networks, gateways, and Internet of Things (IoT) devices.

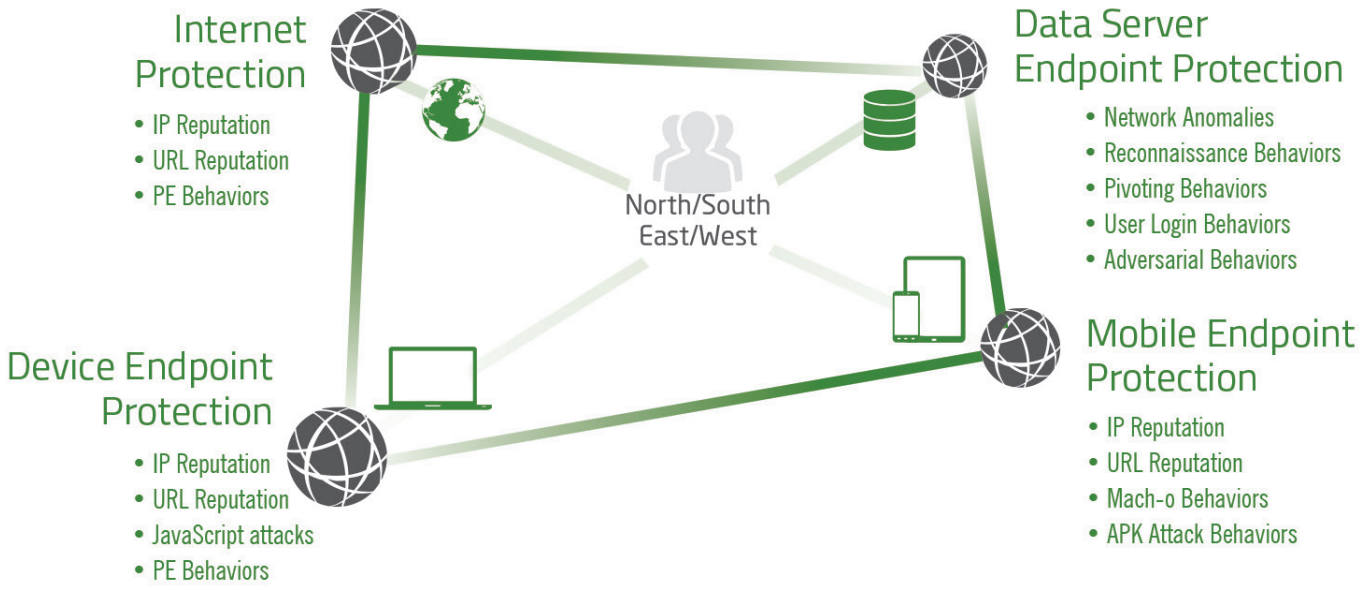

Figure 1: Visualizing the Threat Landscape

FlowScape Features

North-South Protection

The FlowScape solution is tightly integrated with the Webroot BrightCloud® Threat Intelligence. Every internal-external communication to the internet is analyzed in real time to determine the risk level of the connection.

A FlowScape implementation includes access to the BrightCloud Threat Investigator, which provides context into the relationships between different types of internet objects. When an external communication occurs with a file, URL, or IP address with a low reputation score, security analysts are notified and can quickly examine the context of the potential threat through a seamless cross launch into the BrightCloud Threat Investigator.

East-West Protection

In addition to endpoint-to-endpoint communications within the same network, when the connection to a high risk site is made, the FlowScape solution analyzes any internal hops across the network that were made as part of the connection. This East-West traffic inside the business is contextually associated with the North-South traffic to risky sites.

The figures below show a snapshot of a FlowScape display. It shows a guarded server with important data on it, which has been communicating with high risk external sites (North-South) that BrightCloud Threat Intelligence has identified as having a low reputation score (high risk). You can also see the second and third hops away, the East-West communications, and the anomalous communications that have occurred from the Amazon AWS sites and to other internal devices.

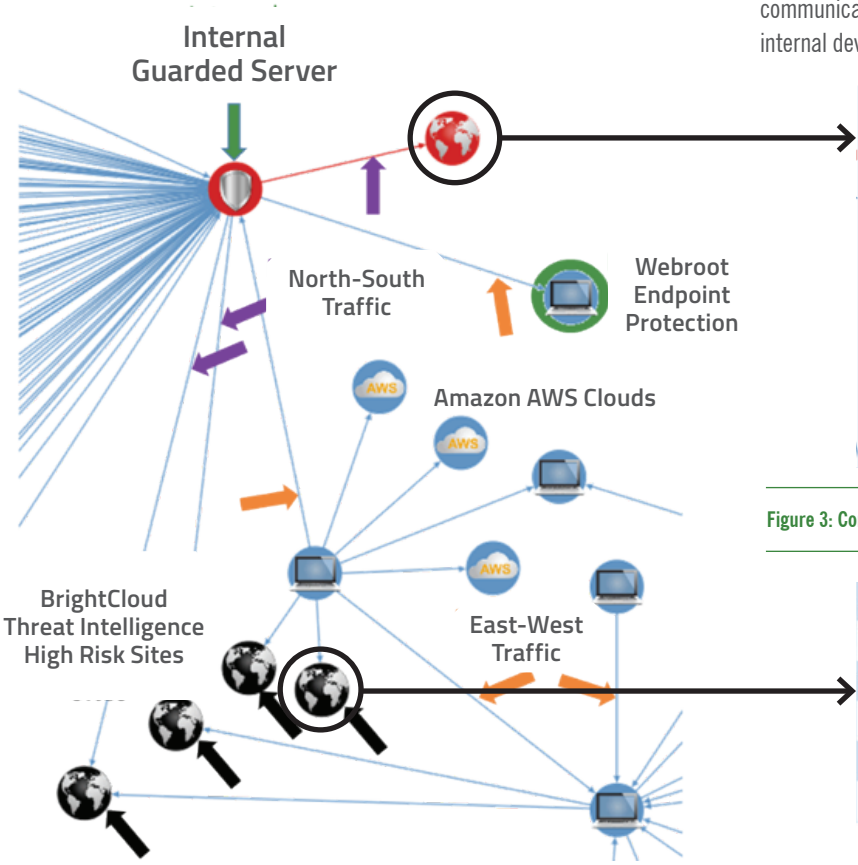

Figure 2: High risk communication between the guarded server and the external site

Severity	0.8
Event	Potential DNS Tunneling Anomaly,...
Model Type	M112
Start Time	2016-11-29 14:04:31
Phase	DNS Tunneling C&C
Port	53
Protocol	UDP

Source
10.0.0.11
Internal, Guarded

Destination
208.67.222.222
External

Figure 3: Contextual information about the blacklisted sites with high risk reputation scores

Severity	0.51
IP Address	50.62.70.1
IP Type	External, Blacklist
Webroot IP Reputation	11
Webroot Threat Category	Mobile Threats, Phishing
Threat Investigator	Investigate this IP

Launch the BrightCloud Threat Investigtor

Figure 4: The BrightCloud Threat Investigator enables further research

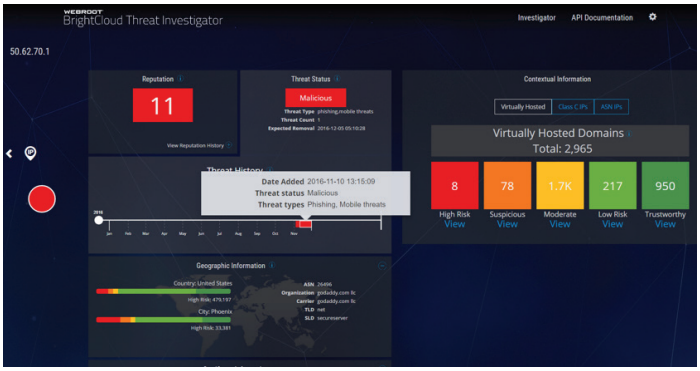

Figure 5: BrightCloud Threat Investigator view

Use Cases

The Webroot FlowScape® network behavioral analytics solution has been deployed in a number of customer environments and vertical industries to accelerate threat detection. These include smart cities, enterprise global data centers, manufacturing environments, biomedical research facilities, and other environments with critical assets and infrastructure to protect. FlowScape sensors can be connected to TAP or SPAN port of a network switch at the egress point where business and Internet of Things (IoT) devices connect to the internet. They can also be placed in data centers where critical resources need to be monitored.

Smart Cities

The FlowScape solution can be deployed in smart cities with a mix of traditional IT systems and a growing number of IoT devices, such as sensors, smart meters, city vehicles, and industrial infrastructure. It can be integrated with a SIEM or other external systems to send events to central operations dashboards. The FlowScape solution also adds value to monitoring the numerous employees and vendors that work across the city and may be involved, often unwittingly, in high risk activity. Police, fire, waste water management, and other critical functions can all benefit from the FlowScape solution, with integrated BrightCloud® Threat Intelligence. Mobile and other endpoint devices in the city can also take advantage of Webroot SecureAnywhere® protection. Different city departments can be set up as sites, each with their own sets of policies and monitoring views.

Enterprises

The FlowScape solution can be deployed in data centers. For example, Webroot has deployed FlowScape sensors in our own London, Denver, and San Diego data centers across a global MPLS network, and they are backhauled to a central FlowScape system running virtually. The servers in the data centers are constantly monitored for connections to high risk external sites (North-South communication) and for internal anomalous activity (East-West communication). FlowScape technology, combined with BrightCloud Threat Intelligence, generates alarms which are imported into a SIEM system for further correlation and reporting.

Industrial IoT

For air-gapped networks or networks that route all traffic through a proxy, the FlowScape solution can carefully monitor for new devices, such as home wireless routers connecting to the network for data exfiltration. The solution can instantly send customizable email alerts if a new internal or external IPv4 or IPv6 address appears on your network. It captures the initial bytes sent and received by this device in real time to alert on a possible breach. Any external communication that is not routed through the correct proxy is instantly reported and evaluated by BrightCloud Threat Intelligence for a risk score.

FlowScape for the Internet of Things

FlowScape network behavioral analytics can track IoT devices, IoT gateways, IoT clouds (including Amazon AWS), and IoT transportation. For smart city implementations, it may be useful to track not only sensors as IoT devices but also police and other city vehicles. The FlowScape solution can machine learn normal behavior of protocols, such as Secure MQQT (or MQQT) to support Amazon AWS IoT deployments. It can also monitor behaviors for industrial IoT protocols, such as Modbus over IP. BrightCloud Threat Intelligence will monitor any external communications from the IoT devices to the internet to alert on

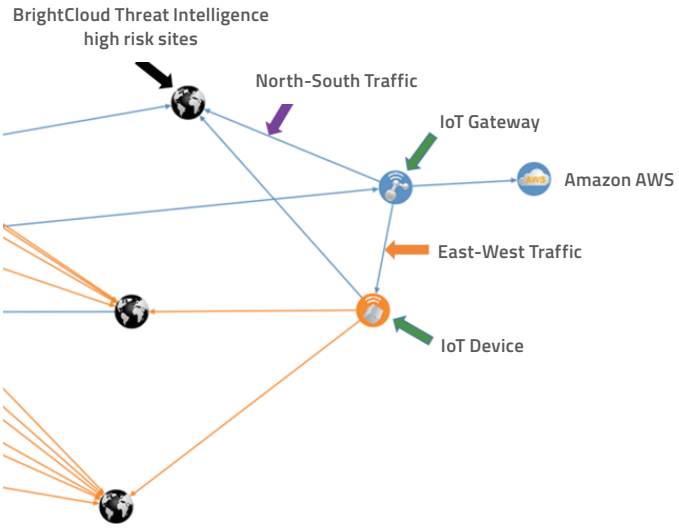

Figure 6: FlowScape insight into connections and traffic

high risk sites. The FlowScape solution can detect new communications from an IoT device to a new external or internal device to enable protection from man-in-the-middle attacks attempting to steal IoT credentials. It can also detect when more (or less) traffic is being sent than what was previously seen on the device.

A Deeper Dive into Network Anomaly Detection

Many vendors only monitor network traffic and look for traffic volumes that exceed thresholds. While the FlowScape solution monitors for volume violations, it also uses more than 30 methods to monitor a network connection from one IP to another over a given port. Additionally, it keeps a behavioral log and looks for changes in behavior over a day, 7 days, or even 30 days. The following is a list of the various FlowScape monitoring methods for identifying potentially adversarial anomalous behaviors in North-South and East-West traffic.

Monitoring and Alerts for Communications between 2 IPs over a Given Port:

1. A new communication never seen before over the history of this network
2. Traffic OverFlow Volume Violation for packets received
3. Traffic OverFlow Volume Violation for packets sent
4. Traffic OverFlow Volume Violation for total packets sent and received
5. Traffic OverFlow Volume Violation for sent, received, and total aggregated packets
6. Traffic UnderFlow Volume Violation for packets sent (for IoT and SCADA Networks)
7. Traffic UnderFlow Volume Violation for packets received
8. Traffic UnderFlow Volume Violation for total packets
9. Traffic UnderFlow Volume Violation for sent, received, and total aggregated packets

Machine Learning Behavioral Analytics Alerts for Anomaly Detection:

10. Clustering Model for IP by IP by Port communication change in Vector Velocity
11. Clustering Model for IP by IP by Port communication change in Vector Magnitude
12. Clustering Model for a Port communication change in Vector Velocity
13. Clustering Model for a Port communication change in Vector Magnitude
14. Clustering Model for a Client Port communication change in Vector Velocity
15. Clustering Model for a Client Port communication change in Vector Magnitude
16. Clustering Model for a Server Port communication change in Vector Velocity
17. Clustering Model for a Server Port communication change in Vector Magnitude
18. Clustering Model for IP by IP by Port communication change in Vector Velocity
19. Clustering Model for IP by IP by Port communication change in Vector Magnitude
20. Clustering Model for External TCP communication change in Vector Velocity
21. Clustering Model for Internal TCP communication change in Vector Magnitude
22. Clustering Model for External UDP communication change in Vector Velocity
23. Clustering Model for Internal UDP communication change in Vector Magnitude
24. Clustering Model for External ICMP communication change in Vector Velocity
25. Clustering Model for Internal ICMP communication change in Vector Magnitude

Machine Learning Analytics for Detecting Specific High Risk Behaviors

26. Supervised TOR Traffic over HTTPS Model
27. BrightCloud Threat Intelligence Alerts
28. High Risk (IP Reputation <20) Alarm on North-South Anomalous Traffic
29. High Risk Alarm on North-South Normal Traffic

Special Device Alarms

30. New Internal Device Alert – New IP on internal network. Good for air-gapped networks with static IPs. Examples are industrial IoT manufacturing environments or critical infrastructure.
31. New External Device Alarm – New IP on external network. Good for industrial IoT and stringent critical infrastructure, air-gapped environments where all external traffic should route through a proxy or should be very restricted.

Note: a single communication can trigger multiple alerts simultaneously. The FlowScape solution adds these alarms as attributes of the event. The entities attached to the event can be one or more of the following:

- MAC address
- IPv4 address of source or destination
- IPv6 address of source or destination
- Source port (used in the communication)
- Destination port (used in the communication)
- Devices acting as relays (such as web services relays that receive a REST API call, then relay into a SQL call to data layer)

FlowScape Management

The FlowScape solution can be deployed with automation to train the machine learning models and self-configure and self-tune with little management or maintenance support. It can be monitored with infrastructure monitoring tools, such as New Relic

The solution also enables advanced users to further customize and access some of the underlying data. Each of the model anomaly scores can be accessed through various scripts, such as Python, to further mine data and search for specific types of anomalies. Remote management tools can also access the FlowScape MongoDB event database to view or perform business intelligence (BI) analysis.

Additionally, the solution enables customers to insert their own JavaScript logic into the event processing flow of the policy engine. For example, you could create special logic for IoT devices or guarded servers to further analyze and adjust risk scores based on custom criteria.

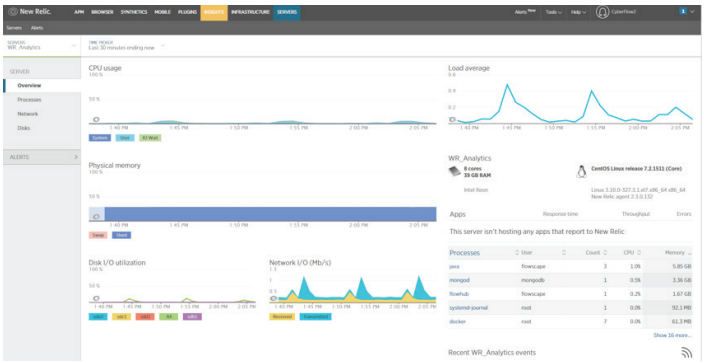

Figure 7: FlowScape view in New Relic

FlowScape SecureAnywhere® SaaS

FlowScape software can be deployed on-premises in VMware or in the cloud. Webroot will offer a new software as a service (SaaS) version of the solution that is integrated with the Webroot SecureAnywhere® Global Site Manager (GSM), which includes Webroot SecureAnywhere® Business Endpoint Protection and SecureAnywhere® DNS Protection products. Visit webroot.com for more information on the full Webroot portfolio of products.

FlowScape Integrations

The FlowScape solution can be configured to send high risk events based on customizable criteria over syslog, TCP, REST API Interface in either JSON or Common Event Format (CEF). Integrations with external partner systems can also occur through the publish/subscribe module known as CyberHooks (a webhook interface for sending events). Other integrations include the new AlienVault SaaS, IBM QRadar, and SumoLogic. FlowScape sensors can also be attached to the GigaMon Visibility Platform, which includes the new G-vTAP agent for monitoring AWS clouds. The integration with GigaMon enables an underlying packet monitoring capability both within your premises and in your public, private, and hybrid clouds.

Frequently Asked Questions

Q: Do I have to add another staff member to manage the FlowScape solution?

A: The FlowScape solution is designed to streamline your security framework, so your staff can worry less about false alarms and spend time focused on the most important IT tasks. As an example, FlowScape data can be integrated seamlessly into your SIEM, and calibrated so that only the truly critical events are sent to your master dashboard for research.

Q: Is it expensive and time consuming to install, configure and tune?

A: The FlowScape solution installs in less than an hour and is completely automated, self-configuring, self-tuning. A bit like a car, the complexity is under the hood, so you just sit back and drive.

Q: Do I need a data scientist on staff to manage a FlowScape implementation?

A: The machine learning analytics are completely automated and self-training, no data scientist required. Larger managed security service providers (MSSPs) and enterprises who want to see the deep analytics in action can view and configure them for their specific environment. Administrators can insert JavaScript into the event policy flow, or write scripts to mine the events in MongoDB and perform deep studies on communication behaviors.

About Webroot

Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® solution protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900