Webroot FlowScape® Network Behavioral Analytics

OVERVIEW

- Security personnel are overwhelmed by alerts, while advanced persistent threats (APTs) work low and slow to hide within everyday network noise
- Network behavioral analytics uses advanced machine learning to provide early warning via robust APIs and investigative dashboards
- Early visibility on attacks can detect APTs, insider threats, newly connected devices, and other adversarial anomalies before they cause damage

Security analysts don't have the time or resources to deal with the constant barrage of often insignificant alerts. Everyday network noise can easily create security blind spots, obscuring APTs and other malicious activity, not to mention employee policy violations and new device connections that put organizations at risk. Although some security solutions claim to address these attacks by identifying such anomalies, many of these are costly and difficult to integrate, rely on log management or signatures that attackers are already familiar with, or create even more alerts to expose further blind spots for cybercriminals to exploit.

To stop advanced persistent threats (APTs) and other malicious events effectively, security analysts must uncover high risk activities during the reconnaissance phase of an attack. Organizations need a new security solution that utilizes advanced inspection, modeling, and analytics, and is cost effective and easy to implement. The Webroot FlowScape solution is a next-generation, virtualized security solution that uses sophisticated machine learning to provide continuous visibility into anomalous behavior within networks. It continually learns network and system behavior and then alerts security analysts to anomalous high-risk activity in real time, without creating unnecessary alerts. Through a multi-model approach that leverages unsupervised machine learning, protocol anomaly detection, and device, DNS, client-server, and client-port analytics, the FlowScape solution builds a history of all IPxIPxPort communication by listening to packet metadata to isolate anomalous breach activity.

ALERTS AND INTEGRATION

As a software-only solution, the passive FlowScape sensors efficiently monitor communications without the need to buy or maintain expensive hardware. The system uses a unique streaming flow technology to find anomalies in milliseconds with minimal infrastructure cost and CAPEX footprint, and uses network packet metadata, not deep packet inspection, to maintain privacy compliance and optimum network speeds.

Designed to complement and augment existing security infrastructure, outputs from the FlowScape solution can be routed to existing commercial or custom security dashboards and SIEM solutions, or integrated into security operations center (SOC), threat assessment, or other incident response architectures and tools. The solution offers a 100% virtualized architecture with Docker Containers to run in your private or hybrid cloud, and can identify attacks on all operating systems, applications, devices, and SCADA without agents or signatures.

With the ability to monitor, track, and classify risks within networks, security analysts can identify and address APTs and other attacks, such as insider threats and employee policy violations, before they cause damage.

FLOWSCAPE BENEFITS

» **Increased visibility**
Gain early warning visibility across all connected assets in the core of your network, both virtual and physical, for adversarial anomalous behaviors early in the kill chain.

» **Machine learning at scale**
Unsupervised machine learning model works for all network deployments, from the smallest networks, to the largest smart cities.

» **Easy integration and use**
Installs in an hour and identifies high risk behaviors on day one, and integrates with SIEM without rule writing or added staffing requirements.

» **No network impact**
By not needing to analyze the payloads of the network traffic (e.g. DPI), there is no impact on network speed, making the solution is massively scalable and secure.

» **Network anomalies with context**
Multiple models identify behavioral anomalies, while Webroot BrightCloud® Threat Intelligence adds adversarial context.

IN ACTION

» **Early threat detection**
Threats are often only detected after an attack. The FlowScape solution can alert security personnel to APTs, atypical BitTorrent traffic, port scanning, DDoS, ransomware, IPv4 and IPv6 high risk anomalies, and more before the damage is done.

» **Bring your own device**
BYOD introduces new risks to the organization, along with your external vendor or employee VPN and WiFi. When an infected device connects to the network, the FlowScape solution will automatically track its communication behavior and identify potential breach activity.

» **Insider threats**
The majority of data breaches begin with disgruntled or thoughtless employees with access to critical data. The FlowScape solution can detect employee policy violations and changes in high risk behavior using machine learning against the normal business process of your networks.

» **Industrial Internet of Things (IoT)**
The FlowScape solution continuously monitors all assets, devices, and protocols, including machine to machine (M2M) communication, as well as people and their devices. The software supports both IT networks and SCADA networks in a single security tool.

» **Cloud infrastructure**
As virtual networks and increasing amounts of data is moved to cloud services, the Flowscape solution enables businesses and SaaS providers to monitor their cloud-based infrastructure for anomalous behaviors.

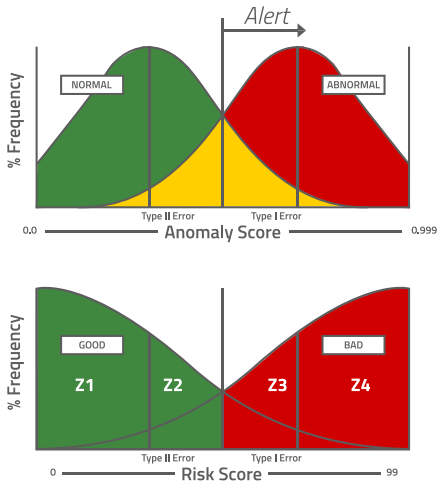

Figure 1. FlowScape technology provides continuous security threat assessment and risk analysis through advanced machine learning.

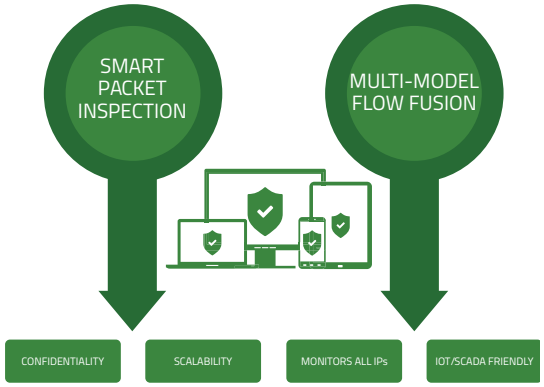

Figure 2. The solution analyzes data flows using advanced clustering analytics to establish baselines, without deep packet inspection (DPI).

About Webroot
Webroot delivers next-generation endpoint security, threat intelligence services, and anomaly detection solutions 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 tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, 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 www.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