IMPACT REPORT

BluVector malware detection and analytics console will work for data

APRIL 18 2016
BY DAN CUMMINS, ADRIAN SANABRIA, SCOTT CRAWFORD (/BIOGRAPHY?EID=876)

The BluVector network-based threat-detection appliance is designed to mitigate security analysts' workflow challenges and information overload, principally by shooting for higher-fidelity positive identification of file-based malware. BluVector uses patented machine-learning techniques to scan all network traffic in near-real-time and make binary good vs. bad determinations at a file level. The product attempts to automate some traditionally manually intensive and slow work steps for malware analysts, including obtaining and scanning custom logs, and the application of custom and third-party analytics tools.

The 451 Take

Significant reductions in false-positive malware identification, in part from faster and more accurate network-based detection, represent leverage to improve overall effectiveness of security automation and orchestration. BluVector is designed as a network appliance and analytic console – enhanced by supervised machine learning and workflow automation – to complement high-value analyst skills and to enable a highly sought proactive threat-hunting use case. BluVector offers security analysts a new 'fighting chance' in terms of detection accuracy and workflow speed. We like a baseball analogy to describe the challenge of spotting malware at line speed. A sharp batter's eye includes the ability to classify pitches in an instant as fastball, off-speed changeup or curveball. In formative training, hitters train their eyes over the course of a lot of at-bats and by seeing a high volume and large variety of pitches. Malware-detection algorithms can and should train as well, because cyberattacks can obfuscate, penetrate over multiple vectors, come at you fast, or stay low and slow. It sounds a bit like facing Hall of Famer Greg Maddux.

Context

BluVector's in-memory analytic correlation and scoring platform was developed over the past five years, based in part on contract research of malware genomes. CISOs and security operations center managers need to alleviate threat fatigue and improve the quality of incident response as a vital capability. Success will almost certainly necessitate high levels of automation and a reorientation of resources and skills toward proactive detection and facility with data science. Whether predictive capabilities of machine learning will provide a definitive big-data edge in the service of malware detection remains to be seen and determined in the market; however, demand-side interest is significant, if not enormous, based on conversations with our vendor and buyer community contacts.

Speedy and accurate malware analysis and effective incident response are among many key activity objectives in the broader desire to orchestrate security operations as processes. BluVector is designed to integrate a high-fidelity detection engine and a malware analyst console. The product attempts to automate some traditionally manually intensive and slow work steps for malware analysts, including obtaining and scanning custom logs, and the application of custom and third-party analytics tools.

BluVector is the only product of the Northrop Grumman subsidiary Acuity Solutions. Kris Lovejoy, president of Acuity, joined in 2015; she is the former GM of IBM Security Services, and adds buyer perspective as a former IBM Global CISO. The technical product team is led by Peter Kaloroumakis, former network and security engineering support executive at Northrop Grumman and former USAF network ops and security officer. Scott Miserendino is chief data scientist. He was previously the principal investigator for a high-speed network processing Internal Research and Design project for Northrop Grumman's Cyber Division. Acuity has 31 dedicated employees.

Product

BluVector was launched just over a year ago as a 10Gbps capacity passive network sensor (2u tap appliance) to see and inspect all traffic, assign risk scores and provide analysis of suspicious files within a unified console interface. BluVector's file inspection covers 30 document, image, compression and archive formats. The capability to quickly add new file-type support and optimize feature selection is differentiated and proprietary, according to the company. Management reports roughly 70 BluVector deployments; the largest scaled configuration to date is on a network with 300,000 endpoints. Current list price is $480,000.

Management believes the market could support higher pricing based on its belief in the product's potential utility in reducing false positives and addressing long-standing security operations productivity and process challenges. BluVector's machine-learning capabilities were upgraded with localized learning in the recently released version 2.0. Management contends that evolving classifiers based on a combination of curated 'factory' data and localized customer environment data can enable 99% accurate confidence scoring, significantly reducing false positives and aiding case prioritization. The context for accuracy improvement depends, of course, on how well a security ops organization is doing currently; nevertheless, the problem of polymorphic malware is one of potency (e.g., targeting credentials) and evasive low profile relative to benign traffic. Notably, management indicates that

BluVector can achieve best identification results, especially with respect to zero-day and polymorphic malware, through exposure to all traffic, with no pre-filtering based on threat indicators of compromise, file hashes and signatures. Analysts can retrain the model whenever the system determines that sufficient new and qualified samples are available to potentially improve the model.

The new release of the console seeks to improve elements of analysts' discovery activities, with targeted logging that is more proactive, contextual and automated through use of the Bro network-monitoring engine. The company is planning to expand to cloud-based configuration as a service, and also to eventually offer MSSPs multi-tenant capability.

Technology

BluVector's sensor technology is software-based; commodity x86-based hardware is provisioned as 48 virtual cores with augmentation via FPGA for high-scale packet collection, data transformations, and analytic wrangling and pivoting. Management indicates that the company's analytic approach is to optimize for speed as well as accuracy, with machine-learning calculations typically requiring less than 10% of the processing resources; other verification and detection analytics on the appliance may consume 10-25% of CPU resources. Traffic inspection is implemented as eight analytic engines, run in parallel and enriched with third-party threat-intelligence feeds, such as iSIGHT Partners and ThreatGRID.

BluVector's proprietary engines include the machine-learning static analysis tool (named Hector), as well as shell-code and URL analyzers (NEMA and Huri, respectively). Several of the scanning engines are freely available, including ClamAV, BroIDS and Yara rulesets. In addition to traffic inspection, users can also submit files for analysis via an API. REST APIs are the primary interface to the software, although management also points to a custom Linux container (BluVector Shell) for running additional user-defined analytics and detection logic as a custom integration with the back end.

Proprietary and patented advantages for BluVector, according to management, are derived through the combination of analytics and modular implementation of localized, 'evolving' classifiers, which enable model heterogeneity. In other words, iterative retraining of the model using local, heterogenous data is designed to improve the model's ability to classify previously unseen bytecode as benign or suspicious. The majority of malware, as research by FireEye and others has indicated, is unique to the environment where it is discovered. In practice, according to BluVector, post-localized learning results in detection models that are up to 50% differentiated, in terms of feature selection, from the base model and other locally retrained models from the same base parent.

Competition

We expect to see competitive distinction emerge from platform capabilities derived from multi-vector approaches to threat intel, traffic inspection, endpoint monitoring and analytics. BluVector's array of detection and analytic engines, console UX/UI, and workflow automation have platform potential, in our view. BluVector is currently most likely to compete with vendors such as FireEye, Blue Coat and large vendors extending product footprints across network-based anti-malware, analytics, sandboxing and other approaches to detection. Other vendors with similar network security product focus include Cyphort, Lastline and ThreatTrack. BluVector's capabilities appear to us as complementary to (so-called post-antivirus) endpoint continuous monitoring and deep domain inspection, represented by vendors such as Tanium, Carbon Black, Resolution1 (Fidelis) and Cybereason. Finally, vendors such as Sqrrl, Reservoir Labs, nPulse (FireEye), Arbor Networks, Tenable, Tanium, Carbon Black, Cybereason and Resolution1 point to threat hunting as being among several core capabilities.

The company's management cites interest by current and potential customers to undercut FireEye on price, in particular in determining what content to forward to sandbox and investigation technologies. That implies competition generally with FireEye's NX appliance and the MVX engine, which appears in all of its products. FireEye's price umbrella was a notable characteristic in network-based APT technology the past several years but appears diminished, which is evident by FireEye's sharp growth deceleration. However, FireEye has its own product roadmap to project integrated capability over a broad activity span, including network forensics (nPulse) and orchestration with Invotas on-board. Some BluVector customers have indicated a desire for in-line deployment and filtering capability, according to management; such an evolution would square up the product to face off against 'next-gen' IPS vendors such as Cisco, McAfee and FireEye.

SWOT Analysis

Strengths

BluVector's unusual combination of network breach-detection appliance and analytics console, enhanced by machine learning and workflow automation, complements high-value analyst skills and may enable a highly sought threat-hunting use case.

Weaknesses

BluVector may be pressed in the near-term to expand deployment options to include cloud-based service or virtual appliances, for example. Some of BluVector's direct and indirect competitors already offer or are currently developing a range of such deployment options.

Opportunities

Threat monitoring has become one of the more important end-to-end activity chains in security operations. Thus, commercial and public sector customer traction on the basis of improving efficiency and accuracy of malware and breach detection, including reducing cycle times through automation, is a notable opportunity to gain competitive profile in a crowded market.

Threats

BluVector may require significant funding and marketing to raise its competitive profile. Primary competition currently comes from FireEye, which has become more publicly focused in recent months on adding cloud-based capabilities, integrating acquired products assets such as nPulse, and reasserting the value proposition of its MVX network sandbox.

Dan Cummins (/biography?eid=934)

Senior Analyst

Adrian Sanabria (/biography?eid=734)

Senior Security Analyst

Scott Crawford (/biography?eid=876)

Research Director

M&A ACTIVITY BY SECTOR

Security / Anti-Malware (193) (https://makb.the451group.com/results?basic_selected_sectors=369)

Security / Premises network security (194) (https://makb.the451group.com/results?basic_selected_sectors=436)

M&A ACTIVITY BY ACQUIRER

Arbor Networks, Inc. (1) (https://makb.the451group.com/results?basic_acquirers=Arbor+Networks, Inc.)

Blue Coat Systems Inc. [Thoma Bravo LLC/Ontario Teachers Pension Plan] (8) (https://makb.the451group.com/results?basic_acquirers=Blue+Coat Systems Inc. [Thoma Bravo LLC/Ontario Teachers Pension Plan])

Cisco Systems Inc. (123) (https://makb.the451group.com/results?basic_acquirers=Cisco+Systems Inc.)

FireEye, Inc. (2) (https://makb.the451group.com/results?basic_acquirers=FireEye,+Inc.)

IBM Corporation (163) (https://makb.the451group.com/results?basic_acquirers=IBM+Corporation)

Intel Corporation (78) (https://makb.the451group.com/results?basic_acquirers=Intel+Corporation)

McAfee Inc [fka Network Associates] (22) (https://makb.the451group.com/results?basic_acquirers=McAfee+Inc [fka Network Associates])

Northrop Grumman Corporation (7) (https://makb.the451group.com/results?basic_acquirers=Northrop+Grumman Corporation)

Figures shown indicate number of transactions

COMPANY MENTIONS (PRIMARY)

Acuity Solutions (/search?company=Acuity+Solutions)

COMPANY MENTIONS (OTHER)

Applied Predictive Technologies , Arbor Networks , Blue Coat , Carbon Black , Cisco , ClamAV , Cybereason , Cyphort , Fidelis Cybersecurity , FireEye , IBM , Intel , Invotas International , iSIGHT Partners , Lastline , Intel Security , Northrop Grumman , nPulse Technologies , Reservoir Labs , Sqrrl Data , Tanium , Tenable Network Security , ThreatGRID , ThreatTrack Security (/search?company=ThreatTrack+Security)

CHANNELS

Information Security , Networking (/dashboard?view=channel&channel=4)

SECTORS

All / Security / Anti-Malware (/search?sector=369)

All / Security / Premises network security (/search?sector=436)