Bromium and ForeScout Team to Automate Threat Response

Submitted by: Bratton PR (Middlesex)

Tuesday, 10 December 2013

Integrated approach facilitates accurate, real-time threat intelligence and automates enterprise-wide mitigation against advanced malware

Cupertino and Campbell, Calif. – 10 December 2013 – Bromium® (http://www.bromium.com/), Inc., a pioneer in trustworthy computing, and ForeScout Technologies (http://www.forescout.com/), Inc., a leading provider of pervasive network security solutions for Global 2000 enterprises and government organisations, today announced integration efforts between Bromium Live Attack Visualisation and Analysis (LAVA™) (http://www.bromium.com/products/lava.html) and ForeScout CounterACT (http://www.forescout.com/forescout-counteract-7/). The joint solution will help automatically defeat and remediate advanced malware, gather precise threat intelligence in real time, and protect the enterprise using advanced network-wide defences.

"In today's threat environment, responding to an attack immediately to achieve defence in depth is critical," said Ken Pfeil, CISO at Pioneer Investments. "The integrated solution from Bromium and ForeScout will enable us to cut through the noise of false alerts and automate our response to actual attacks in real-time, enterprise wide. Additionally, the approach leverages our existing investments in endpoint and network security, providing unambiguous and actionable threat intelligence that we can use to quickly and systematically enhance our overall security posture."

Providing an unrivalled comprehensive and accurate view of malware behaviour in real-time, LAVA is a centralised security application that works in conjunction with Bromium vSentry®. Bromium vSentry is built on the revolutionary Bromium Microvisor that protects endpoints by design, using CPU features for virtualisation to hardware-isolate each browser tab, attachment or document in a micro-VM™ that cannot access enterprise data, the Intranet or valuable SaaS sites. Malware is automatically remediated when the user closes the task. LAVA gathers and provides real-time analysis of each hardware-isolated malware attack cycle occurring within an enterprise, providing detailed insight into an attack's origin, techniques and targets while delivering immediate, actionable security intelligence and enabling enterprise security teams to safely analyse threats.

"In conjunction with vSentry, LAVA provides unparalleled intelligence into malware attacks at the most critical point and time, as it happens," said Simon Crosby, CTO and co-founder at Bromium. "Our work with ForeScout, leveraging ControlFabric technology, allows joint customers to respond immediately, network wide, using the rich integration and powerful orchestration capabilities of LAVA and CounterACT."

Based on CounterACT's real-time visibility and policy-based mitigation capabilities, CounterACT can dynamically provision and activate the Bromium endpoint agent, vSentry®. CounterACT can also receive malware details from Bromium LAVA™, Bromium's management system, in real-time and allow organisations to enable CounterACT to quarantine infected endpoints, block the infection source and inspect all other endpoints on the network for presence of a similar infection.

The joint solution benefits include:

• Automated malware response – When Bromium LAVA detects advanced malware, it sends information about the attack to CounterACT in real-time. CounterACT can then take automated actions such as alerting the administrator, emailing the end-user and preventing further malware propagation to unprotected endpoints by blocking traffic to and from the infection source.

• Agent provisioning and monitoring – CounterACT has the ability to discover, classify and monitor all endpoints on the network, including unmanaged and personal devices. This allows CounterACT to detect endpoints without a Bromium vSentry® agent and verify if they meet the minimum hardware and BIOS requirements. CounterACT then deploys the Bromium agent on these endpoints, automatically or via manual action.

• Enterprise-wide attack mitigation – Bromium can determine the signature representative of an advanced malware attack and send this information, including the malware payload fingerprint, to CounterACT. CounterACT can use this information to assess all other endpoints (including unprotected endpoints) to identify and quarantine additional zero-day infection points across the enterprise network.

"We are thrilled to partner with Bromium to provide joint customers with enhanced protection against advanced malware," said Gil Friedrich, vice president of technology at ForeScout. "This integration illustrates how ForeScout's customers and partners leverage the ControlFabric technology to build a central security hub that can bi-directionally share real-time threat intelligence, automate remediation and improve operational efficiency."

ForeScout CounterACT, Bromium vSentry® and LAVA™ interoperability is delivered through the ForeScout ControlFabric Interface (http://www.forescout.com/product/) using open, standards-based formats. ForeScout delivers pervasive network security by allowing organisations to continuously monitor and mitigate advanced malware attacks. ForeScout CounterACT dynamically identifies and assesses all network users, endpoints and applications to provide comprehensive visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology enables vendors, system integrators and customers to integrate CounterACT with a broad range of IT security products and management systems to automate enterprise-wide defences.

About Bromium, Inc.
Bromium is re-inventing enterprise security with its powerful new technology, micro-virtualisation, which was designed to protect businesses from advanced malware, while simultaneously empowering users and delivering unmatched threat intelligence to IT. Unlike traditional security methods, which rely on complex and ineffective detection techniques, Bromium protects against malware from the Web, email or USB devices, by automatically isolating each user-task at the endpoint in a hardware-isolated micro-VM, preventing theft or damage to any enterprise resource. Bromium's technological innovations have earned the company numerous industry awards including being named as a CNBC Disruptor and a Gartner Cool Vendor for 2013. Bromium counts a rapidly growing set of Fortune 500 companies and government agencies as customers, including NYSE and BlackRock.

About ForeScout Technologies, Inc.
ForeScout delivers pervasive network security by allowing organisations to continuously monitor and mitigate security exposures and cyberattacks. The company's CounterACT platform dynamically identifies

and assesses all network users, endpoints and applications to provide complete visibility, intelligence and policy-based mitigation of security issues. ForeScout's open ControlFabric technology allows a broad range of IT security products and management systems to share information and automate remediation actions. Because ForeScout's solutions are easy to deploy, unobtrusive, flexible and scalable, they have been chosen by more than 1,500 enterprises and government agencies. Headquartered in Campbell, California, ForeScout offers its solutions through its network of authorised partners worldwide. Learn more at: www.forescout.com.

Media contacts:
For Bromium: Heather Fitzsimmons
Mindshare PR
heather@mindsharepr.com
001-650-800-7160

For ForeScout: Sally Bratton
Bratton PR
sally.bratton@brattonpr.com
0044 7930 301601

responsesource