Whitepaper

The C-Level Executive's Guide to Transforming Endpoint Security

Defeat Attacks. Reduce Costs. Empower Users.

Bromium®

Executive Summary

"Over 70% of breaches occur at the endpoint."

VERIZON 2013 DATA BREACH INVESTIGATIONS REPORT

IT security is at a major turning point and is undergoing a major transformation. CIOs and CISOs are facing realities that are challenging traditional security concepts and methods. Eager to expand and increase profitability, their companies continue to embrace business-enabling technologies like mobility, the cloud, and consumerization of applications—causing network perimeters and IT control to evaporate.

Clearly, security as usual is not the optimal strategy. The only surefire way to protect users and safeguard sensitive data both on and off the network is to defend the endpoint itself. According to the Verizon 2013 Data Breach Investigations Report, 71% of analyzed data breaches encompassed compromised endpoint devices—up from 17% in 2008.[1] And old-school detection and blocking defenses are incapable of defeating these targeted attacks—detection rates for antivirus, for example, range from only 25% to 50%.[2]

A revolutionary new way of protecting the endpoint has emerged—a game-changing model built around isolation technology. CIOs and CISOs can leverage this approach to improve security, streamline IT, satisfy users' demands for flexibility, and reduce operational costs and security expenses.

The Evolving Cyberattack Landscape

Today's cyberattacks are constantly evolving. Long gone are the days of hacking for kicks. Cybercrime is big business. Cybercriminals are bright, well trained, and highly motivated. And, in many cases, they're extremely well funded and organized. Although enterprises certainly face everyday, run-of-the-mill viruses, Trojans, and worms, IT security organizations are also combating a new class of advanced threats that are designed to sail right past traditional security defenses as if they weren't even there.

"Antivirus's reign as the king of endpoint protection is nearing an end. Signature-based AV engines can no longer keep up with the explosion of malware variants."

CHRIS SHERMAN, PRINCIPAL ANALYST, SECURITY AND RISK, FORRESTER RESEARCH

A new generation of cyber attacks

Over the past half-decade, we have witnessed a paradigm shift in the way cybercriminals penetrate corporate networks. Rather than targeting servers of interest directly—which are centrally managed and highly guarded—cybercriminals have shifted to attacking endpoint devices, primarily Microsoft Windows PCs. Although there is little data of interest on an individual PC or laptop, once compromised, these devices can serve as a launch pad for advanced persistent threat (APT) campaigns, enabling criminals to spread laterally through the network until servers of interest are identified and exploited and targeted data is exfiltrated.

Today, cybercriminals target endpoint devices using a variety of highly targeted and customized techniques, including:

- Spear phishing
- Whaling
- Water holing
- Baiting
- Search engine poisoning
- Drive-by downloads

Why Current Cybersecurity Efforts Fail

No matter how much money enterprises invest in security, the bad guys always seem to find a way in. Let's explore the reasons why.

Threats are highly customized and evasive

Unlike everyday viruses, Trojans, and worms—which are intended to infect large numbers of organizations—advanced threats are highly customized for each attack. All cybercriminals need to do to bypass most signature-based defenses (for example, intrusion prevention systems, antivirus, and secure Web gateways) is change a single byte of code. Doing so alters the threat's profile and makes it "unkown." And until signature-based defenses are updated, they don't stand a chance at catching them.

"Most enterprise security protection efforts and products have focused primarily on blocking and prevention techniques (such as antivirus). Existing blocking and prevention capabilities are insufficient to protect against motivated, advanced attackers."

GARTNER, FEBRUARY 2014, DESIGNING AN ADAPTIVE SECURITY ARCHITECTURE

IT can't keep up

Regardless of how sophisticated and targeted the cyber attack, it's destined to fail if the vulnerability on the host it's targeting has been patched. Unfortunately, IT organizations often can't keep up with system patching, relegating patching to once per month or sometimes once per quarter. When patching occurs infrequently, it opens the door to criminals who design malware to exploit recently disclosed vulnerabilities.

Humans are error-prone

IT security is about people, technology, and processes. You can have the best security products that money can buy and you can hire the most talented security analysts around, but, if you don't have the right processes in place, you might as well pack it in.

A case in point is Target, which reportedly invested more than a million dollars in an advanced threat protection platform just six months before its historic data breach in November 2013. The system apparently detected a threat and triggered an alert that was sent to a security team in Bangalore, India. That team forwarded the alert to Target's security operations center at its headquarters in Minneapolis. From there, the alert fell into a black hole. No action was taken—and more than 40 million credit card numbers were stolen.[3]

Isolation—A Revolutionary Approach to Endpoint Security

Given how vulnerable organizations are, how targeted and sophisticated cyber attacks are today, and how traditional security defenses don't do an adequate detection job, there has to be a better way to defend endpoints and networks. What if there was a way to detect cyber attacks and render them harmless in the process?

There is. Enter the revolutionary isolation approach, which defeats cyber attacks, streamlines IT processes, frees users to click on anything, anywhere without getting compromised, and dramatically reduces costs.

"Micro-virtualization is game-changing technology for the information security professional and the enterprise today."

JIM ROUTH, CISO, AETNA

"Bromium is a game changer in the industry."

COLIN HAUBRICH, ALTERA CORPORATION

"Tests conducted with Bromium vSentry showed that the software was able to defeat 100% of the attacks."

NSS LABS

Defeat cyber attacks

Isolation far exceeds the capabilities of detection and blocking technologies like antivirus, whitelisting, Web gateways, and sandboxes. It defends the endpoint by isolating all content for each task—including threats—through breakthrough micro-virtualization technology that leverages CPU hardware technology. Advanced isolation technology creates a micro-virtual machine for vulnerable actions, like Web browsing and opening untrusted documents. These operations are isolated from the host operating system, eliminating the need for any type of detection or behavioral analysis—or the possibility of compromise.

Even if malware finds its way into a micro-virtual machine, the system still protects the enterprise network, the endpoint, and the user. Micro-virtual machines are created and destroyed in milliseconds, discarding malware and ensuring that the system is unaffected. All of this occurs automatically, with minimal impact on the user experience.

Streamline IT

Today's IT professionals face a constant flood of alerts from every system. It's a challenge to find the critical threats in a sea of false alerts or insignificant events. The isolation approach streamlines IT processes, dramatically reducing and even eliminating:

- Compromises on endpoints
- Costly remediation and reimaging
- The need for urgent security-related patching
- The noise and cost of security alerts and the wasted effort of chasing false positives

Empower users

Users want the flexibility to use the latest available tools, freely access the Web, and work anywhere: at home, branch offices, hotels, and airports. Restrictive policies and security solutions can get in their way and slow them down. With the isolation approach to endpoint security, CIOs and CISOs can give users the freedom to do their jobs anywhere and access anything—without ever worrying about security.

Reduce security expense

Isolation technology pays for itself in just a matter of months. Its powerful and effective endpoint security technology helps enterprises dramatically reduce costs related to remediation, lost productivity, forensic analysis, and urgent security patching. Beyond reducing operational expenses, this technology significantly amplifies its value by virtually eliminating the possibility of all-too-common breaches and the financial losses associated with those events.

Bromium Leads the Way

The new cyber attack landscape requires a new way of thinking. Trying to keep up with the bad guys is an exercise in futility. Bromium offers CIOs and CISOs a fresh, new approach to tackling a very serious dilemma facing their IT security teams and their enterprises as a whole. Bromium's expert technologists have developed state-of-the-art innovations in virtualization, systems architecture, security, and high-performance computing. By eradicating the vulnerabilities that advanced threats are designed to exploit after each Internet-facing computing task is completed, Bromium's isolation solution effectively eliminates the attack surfaces of Windows-based endpoints, which are almost always the initial target of APTs and other advanced threat campaigns.

In addition, Bromium helps the bottom line. Enterprises reap the financial benefits of their investments within a short period of time, allowing critical IT resources to focus on what matters most—enabling business. Enterprises that have embraced Bromium reduce expenditures in four key areas: breaches, reimaging PCs, lost employee productivity, and security operations.

Conclusion

As C-level information and security executives are well aware, we now live in a world where the question is no longer "if" your network will be compromised, but "when." Verizon and other research studies have proven that the most common and effective way for cybercriminals to target data of interest is to compromise vulnerable endpoints and use them as launch pads as part of an advanced threat campaign.

Forward-thinking CIOs and CISOs are taking a serious look at the isolation approach as a way to transform the resilience of enterprise endpoints, substantially reduce their investment in security, boost operational efficiency, and free up users to be more productive and creative securely.

For more information

For more information on Bromium endpoint security solutions, contact your Bromium sales representative or Bromium channel partner. Visit us at www.bromium.com.

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

1 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

2 http://www.forbes.com/sites/ciocentral/2014/05/21/duck-test-antivirus-software-wont-detect-advanced-malware/

3 http://www.pcmag.com/article2/0,2817,2454977,00.asp

Bromium US
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information refer to www.bromium.com
or contact sales@bromium.com

WP.CLevel.US-EN.1409