Whitepaper

A New Model for Defeating Cyber Attacks and Reducing Costs

The ROI of The Isolation Approach

Bromium®

Executive Summary

"According to the Verizon 2013 Data Breach Investigations Report, 71% of analyzed data breaches occur at the endpoint—up from 17% in 2008. Detection rates for antivirus range from only 25% to 50%."

We live in a world where the question is no longer whether your company will experience a data breach, but when. Hardly a day goes by that you don't hear about a major data breach or a new cyber attack that's making headlines—and the costs associated with these security events continue to mount.

As the Ponemon Institute points out in its benchmark report, 2014 Cost of Data Breach Study: Global Analysis, the potential costs of a data breach can be significant:[1]

- Average cost per stolen record: $201
- Average cost of lost business: $3.2 million
- Average cost per data breach: $5.9 million

The study also points out that the leading cause of these costly and potentially damaging events is malicious or criminal activity. Many enterprises are spending billions of dollars every year on network and endpoint security defenses—often to no avail, as data breaches persist and accelerate. The most common and effective way for cybercriminals to target data of interest is to compromise vulnerable endpoints and use them as launchpads for advanced threat campaigns. According to the Verizon 2013 Data Breach Investigations Report, 71% of analyzed data breaches occur at the endpoint—up from 17% in 2008.[2] Old-school detection and blocking defenses have proven to be ineffective at defeating these targeted attacks. Detection rates for antivirus, for example, range from only 25% to 50%.[3]

To stand a chance at defeating highly sophisticated and well-funded cybercriminals, we have to think differently. The only surefire way to protect users and safeguard sensitive data both on and off the network is to defend the endpoint itself. A revolutionary new way of protecting the endpoint is called for—a game-changing model built around isolation and micro-virtualization.

This paper provides a compelling business case for isolation technology, detailing how you can leverage it to improve security, decrease operational costs, and reduce the likelihood of a costly breach at your organization. With a typical payback period of six to 18 months, it's easy to justify advanced isolation technology to business owners concerned about the bottom line.

A New Generation of Cyber Attacks

"Bromium's isolation technology helps enterprises defeat cyber attacks, streamline IT processes, free users to click on anything, anywhere without getting compromised, and dramatically reduce costs."

Although enterprises face everyday, run-of-the-mill viruses, Trojans, and worms, IT teams are now combating a new class of advanced threats that sail right past traditional security defenses. Over the past half-decade, there has been a paradigm shift in the way attackers penetrate corporate networks. Rather than targeting servers of interest directly, cybercriminals attack primarily Microsoft Windows endpoint devices. Once compromised, these devices can serve as launchpads for advanced persistent threat (APT) campaigns, which can spread throughout the network, exploiting servers where valuable data can be exfiltrated.

Bromium—A Revolutionary Approach to Endpoint Security

Bromium has transformed endpoint security with an innovative approach that leverages leading-edge isolation and micro-virtualization technology. Bromium's isolation technology helps enterprises defeat cyber attacks, streamline IT processes, free users to click on anything, anywhere without getting compromised, and dramatically reduce costs.

Bromium's isolation approach 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 (micro-VM) for vulnerable user tasks, like Web browsing and opening untrusted documents. After the task is completed, the micro-VM is discarded in milliseconds, and along with it, any malware that may be present. These operations are isolated from the host operating system, eliminating the need for any type of detection or behavioral analysis—and the possibility of compromise. All of this occurs automatically, with minimal impact on the user experience. Additionally, because IT spends much less time chasing false positives, patching, and remediation, Bromium pays for itself within a short period of time.

Measuring Bromium Return on Investment

"Bromium pays for itself in less than a year."

Let's take a look at the factors that contribute to ROI for a typical enterprise-wide Bromium deployment, including sample ROI analyses for two Bromium customers. This will help you understand how Bromium pays for itself in less than a year.

Financial costs

Costs associated with Bromium deployments include:

- Bromium licensing
- Labor involved in deploying Bromium
- Training employees to use Bromium
- Annual maintenance plans, including software updates and access to technical support

Financial gains

Costs that can be avoided as a result of deploying the Bromium solution include:

- IT labor involved with reimaging Microsoft Windows PCs and laptops after they've become infected with malware
- Lost worker productivity while employees are sitting on the sidelines waiting for their computers to be fixed
- Forensic costs of investigating endpoint cyber attacks
- Incremental out-of-band (emergency) patching on endpoint devices outside of regular monthly or quarterly patching cycles

In the event of a breach where confidential data (e.g., credit card numbers, Social Security numbers, software source code, hospital records) is exfiltrated, some of the financial costs are amplified. In these scenarios, these costs would be avoided with Bromium:

- Lost revenue from current and potential customers due to lack of trust following a data breach
- Fines associated with violating PCI, HIPAA, or other regulations
- Legal fees associated with defending class-action lawsuits filed by customers and/or partners
- Cost of notifying customers that a data breach has occurred
- Public relations costs associated with "containing" bad press following a successful data breach

Sample Bromium Customer ROI Calculations

"Bromium is a game-changer in the industry."

COLIN HAUBRICH, SENIOR MANAGER, OFFICE OF THE CIO, ALTERA CORPORATION

"The world's largest payroll processor expects to achieve a three-year ROI of 265%."

To illustrate potential ROI of an enterprise-class Bromium deployment, two Bromium customers were interviewed to assess the financial costs and gains of their deployments. The results are compelling.

World's largest payroll processor

This company has more than 50,000 endpoints that will ultimately be protected by Bromium software. A security operations center (SOC) analyst at the company confirmed that an average of 16 labor hours are spent investigating and analyzing each compromised endpoint, plus another 40 minutes per false-positive endpoint security alert.

Figure 1 compares the financial costs associated with acquiring and deploying Bromium software against the financial gains associated with recuperating costs that would typically be incurred if Bromium software were not present. As you can see, there is a modest ROI during the first year, but when you compare all of the financial costs and gains for the first three years, the company expects to achieve a three-year ROI of 265%.

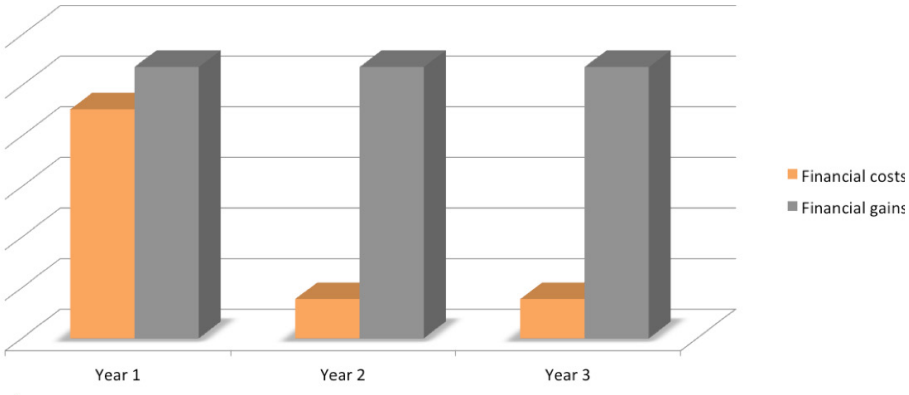

Figure 1: Payroll processing customer's ROI for first three years

Of course, the financial gains in Figure 1 do not incorporate the significant costs averted from a successful data breach (potentially millions of dollars), as there are too many variables to capture, including the size of the data breach and the value of the data that was exfiltrated. However, the operational financial gains alone dwarf the costs associated with the Bromium investment in the second year and beyond.

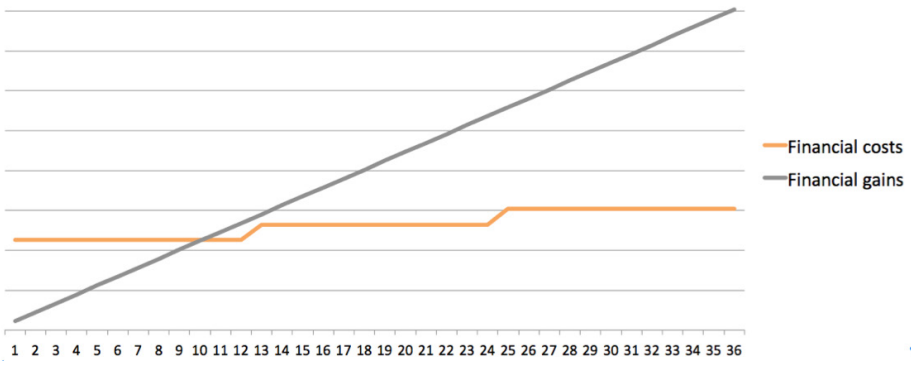

Figure 2: The payroll processing company's payback period is 11 months

Figure 2 illustrates the payback period for the payroll processor's Bromium investment—the number of months where the cumulative financial gains outweigh the cumulative financial costs. In this case, the company expects to recuperate its up-front Bromium investment after just 11 months. Ongoing annual Bromium expenses correspond to annual maintenance fees, which provide the company with software updates and technical support.

As you can see in Figure 2, after the first year of investing in Bromium, the company's ROI will continue to grow as the cost of annual maintenance pales in comparison to the cost of investigating and remediating endpoint security breaches.

Financial services firm

This financial services firm has 45,000 endpoints that will be protected by Bromium endpoint software. Once again, an SOC analyst was interviewed to ascertain the company's cost of mitigating endpoint security incidents. Here the analyst estimates that the company spends approximately 24 labor hours analyzing each compromised endpoint.

"A financial services firm projects its three-year ROI at 178%."

Figure 3 illustrates the projected ROI for the company's Bromium deployment for the first three years. Unlike the payroll processor, the financial services firm's financial costs exceed its anticipated gains in year one, but that gap is quickly closed in year two and beyond as the company reaps the benefits of its Bromium solution. In this case, the financial services company projects its three-year ROI at 178%.

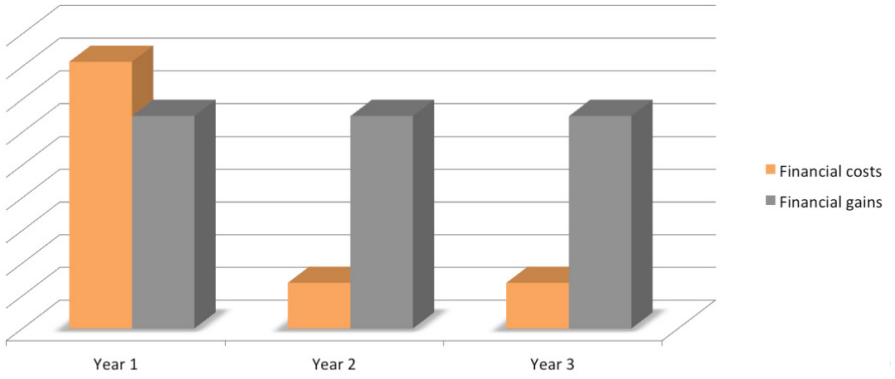

Figure 3: ROI for financial services customer over the first three years

Figure 4 shows the projected payback period for this customer's Bromium investment. The company projects to recuperate its initial investment after 18 months and will continue to have positive rates of return each month following.

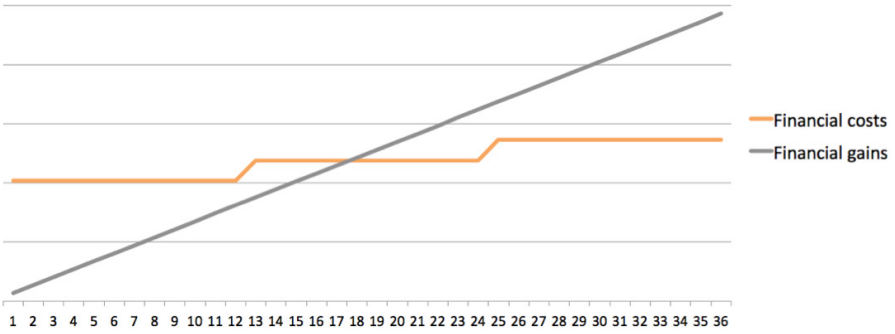

Figure 4: The payback period for the financial services customer is 18 months

Conclusion

Bromium affords enterprises a fresh new approach to tackling a serious dilemma facing every enterprise IT security team. By eradicating the vulnerabilities that advanced threats are designed to exploit after each Internet-facing computing task is completed, Bromium effectively eliminates the attack surfaces of your endpoints, which are almost always the initial target of APTs and other advanced threat campaigns. After a short payback period of six to 18 months, you'll reap the financial benefits of your investment, allowing you to refocus critical IT resources on what matters most—growing your business.

For more information

To learn more about Bromium endpoint security solutions, contact your Bromium sales representative or 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.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

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

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

Bromium US
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.598.3623

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

For more information refer to www.bromium.com, contact sales@bromium.com or call at 1-800-518-0845

WP.ROI.US-EN.1409