Closing the 1% Gap that Costs You Millions

January 2017

"Three out of five CIOs from enterprises across North America and EMEA feel they are losing the battle against cybercrime."

VANSON BOURNE 2016

Exec Summary

Global security spending was expected to reach $81.6 billion in 2016 and is growing at a compound annual growth rate (CAGR) of 8%[i]. But, ransomware is growing at 300% and will cost business over one billion dollars in 2016, according to Gartner.

There is an arms race going on in cyber. New machine learning is meant to be the hope for cyber security in the continuous arms race between cybercriminals and cybersecurity vendors, both sides have it, and both sides are using it[ii].

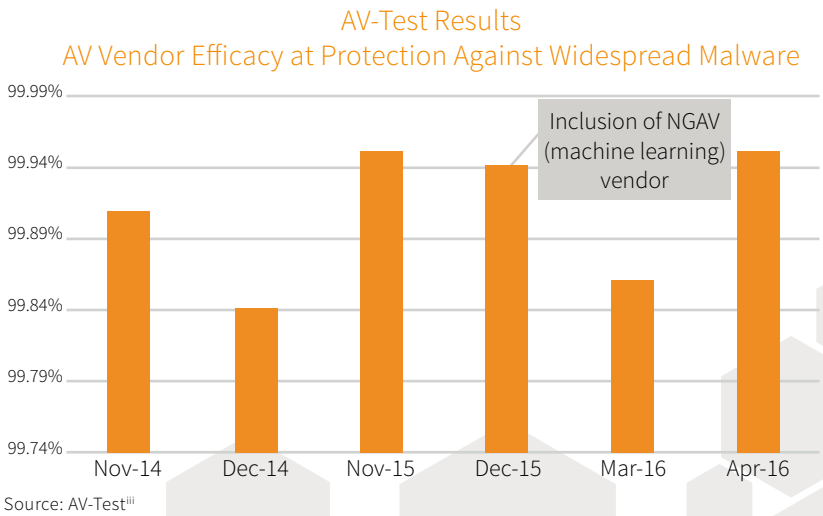
Antivirus is no longer very effective against new threats, zero-days or targeted malware, but most organization are required to have it for compliance reasons.

Using Bromium and Microsoft Defender, organizations can win the arms race against cybercriminals.

And do it while saving money.

The 1% Arms Race

For many years, antivirus vendors have competed for the best detection rate. The constant arms race between cybercriminals and antivirus vendors has resulted in what can be referred to as the 1% race. Over the course of multiple years, third party testing shows that the race to close the 1% gap still continues. Even with the introduction of new NG-AV vendors that utilize machine learning, the gap still remains at 1% for widespread and prevalent malware.



Source: AV-Test[iii]

It's the 1% of threats that are slipping through layered defense systems and AV solutions which results in an average cost of $4 million per breach for an enterprise organization[iv].

There are some fundamental truths that every security vendor needs to take into account.

- There will always be software vulnerabilities that cyber criminals can exploit.
- Organization will always be subject to malicious code and threats.
- It is not possible to anticipate an attacker's next move.

It's the 1% of threats that are slipping through layered defense systems and AV solutions which results in an average cost of $4 million per breach for an enterprise organization[iv].

Signature-based AV is effective at catching what has previously been seen. Unfortunately, this is not at all effective against threats today. Polymorphic malware is so prevalent nowadays that it's estimated that 97% of malware is unique to the endpoint[v].

Even new machine learning techniques models are ineffective against zero-day or unknown malware. This is because machine learning can be bypassed fairly easily through a couple of different techniques:

- Manipulation of the training data where the sample set of data is poisoned so that the machine learning classifier falsely classifies legitimate samples as malware, or malware that has been designed to resemble benign software is classified as safe.
- Obfuscation of malware through bit shifting, repacking, or compressing the malware so that the machine learning classifier falsely classifies malware as safe[vi].

99% of malware hashes are only seen for 58 seconds or less.

Median rate for protecting against zero-day attacks	
Existing AV vendors	99 .4%
Machine learning	97.9%

Detection-based solutions that try to prevent an attack using machine learning don't fare much better than traditional security vendors when comparing the test results delivered by AV-Test[vii].

One reason for the increased gap for machine learning efficacy could be related to the recent finding published in the Verizon Data Breach Investigations Report for 2016 that showed that 99% of malware hashes are only seen for 58 seconds or less . By the time the malicious code has been classified it's already morphed into something completely different[viii].

AV compliance with PCI DSS does not mean your environment is protected from today's threats.

Is AV Still Required?

Even though some, like Netflix, have decided openly to drop AV in 2015, most organizations are required to use AV in order to adhere to compliance regulations[ix]. PCI DSS Requirement 5 specifically states the need for AV in order to achieve compliance[x].

> 5.1 Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).
>
> 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

When considering the efficacy of antivirus against threats today many organizations question whether or not it makes sense to keep paying for AV. Most view AV as a checkbox item that is required to stop known threats as part their layered defense strategy and to avoid any penalties for non-compliance.

Compliance with PCI DSS does not mean that your organization will be protected. When the retailer, Target and other entities like, Heartland Payment Systems were breached, they were PCI-compliant. The compliance regulations for security need to be updated to address current threats to organizations.

For compliance reasons, AV is still required. If an organization views AV simply as a checkbox item for compliance, perhaps one should question the return on investment of the AV. It may not make sense to spend budgeted dollars on AV when those funds can be used for more strategic security solutions that will stop today's threats. Instead take advantage of free AV solutions that are already bundled existing licensed software. Once such example would be Microsoft Windows Defender.

Stopping the 1% that Everyone Misses

It's estimated that 80% of attacks are targeted directly at end users over the web or with malicious URLs in emails[xi]. Last year, cybercriminals created 230,000 new malware samples *per day*. Trying to keep up with detection-based solutions that attempt to prevent a breach will continue to fail. A paradigm shift is needed if we are to succeed at stopping new threats.

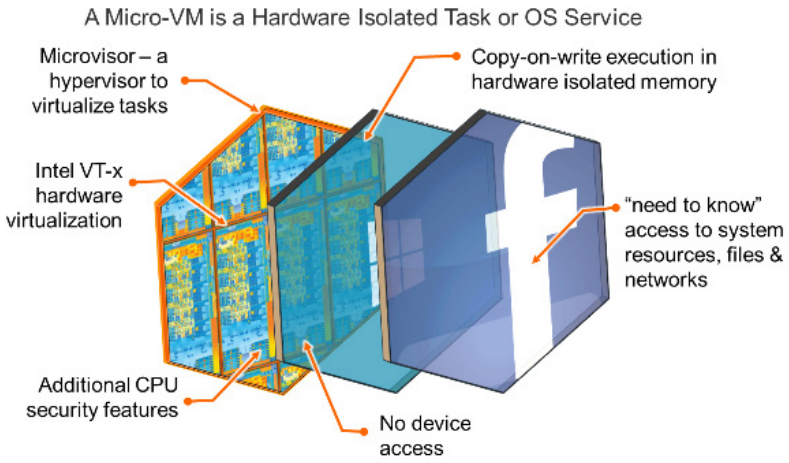
"I've worked with Bromium for more than two and half of years. It is a good project for us as it allows us to browse our Internet and Intranet sites securely. In addition, it allows us to locate any threats and the support team is very effective when replying to all of our problems."

IT SPECIALIST, GLOBAL AEROSPACE COMPANY

Instead of trying to identify whether or not code is malicious before it runs, why not let it actually run to confirm its real intention? Unlike other security technologies that try stop malicious code from running pre-execution, Bromium allows malicious code to run while fully tracing the kill chain to generate a complete malware manifest. All while malware is prevented from infecting the operating system.

Bromium Secure Platform does this by opening each application and process in hardware-enforced micro-virtual machines (micro-VMs), assembled within the endpoint, and then it looks to see what the application or process does before accepting it as safe.

Isolated malware cannot access high-value information, credentials or the enterprise network or sites. Bromium records detailed, false-positive free forensic intelligence for each attack, and the endpoint self-remediates by automatically discarding each micro-VM, eliminating persistence.



Because Bromium isolates the malware in the hardware-enforced micro-VM there is no need for signatures to detect malicious activity. Each Bromium protected endpoint learns about the attack through introspection of what is going on inside the micro-VM. Once the browser tab, or file is closed the malware is disposed of with the micro-VM. The threat information collected is shared in real-time with other endpoints to protect the organization.

Virtualization-based security and isolation technology dramatically decrease attack surfaces and protects users whether they are online or offline, using introspection and behavioral analysis. It is easy to deploy and delivers quick time-to-value. Most importantly, it turns your largest liability, your endpoints and servers, into your best defense.

"We use Bromium on all our machines in the environment. We use Bromium monitoring on all our machines that are below core I3 processors. Everything we have encountered with Bromium has been great!"

IT SECURITY SPECIALIST,
MASONICARE CORPORATION

"Bromium adds more security to our infrastructure, and deepens our confidence about staying protected."

IT SPECIALIST, GLOBAL 500 BANKING COMPANY

Bromium customers have launched over a billion micro-VMs and have never reported any malware escape. According to Gartner, ransomware accounts over $1 billion in fees that organization will pay in 2016. Bromium customers do not need to worry about the impact of ransomware simply because they remediate it by closing the application. Learn how Bromium defeats ransomware in 90 seconds by watching this video.

Insider Threat Detection

An insider threat may not necessarily be a disgruntled employee. More often than not its persistent attacker that has already infiltrated your organization and is moving laterally. Furthermore, file-less malware and PowerShell are increasingly being used with nefarious intent. In a recent study, it was found that 95% of the PowerShell scripts evaluated, for 111 malware families, were malicious[xii].

It's incredibly difficult to catch an insider, especially if they are using tools like PowerShell that is installed by default on most Windows systems, and most organizations do not have extended logging enabled for the framework.

In addition, each endpoint becomes a tamper-proof sensor in a distributed breach detection system: The endpoint monitors its own execution to detect malicious execution, and shares its intelligence with the security team in real-time to accelerate enterprise-wide response. The monitor is protected using micro-virtualization to prevent it from being disabled by malware.

Bromium also helps identify and stop persistent insider attacks. By monitoring all user tasks and processes Bromium Secure Monitoring quickly identifies malicious insider activity as well as file-less threats like PowerShell attacks. Confirmed by Gartner, Bromium supports one the largest managed hunting services in the industry with over one hundred thousand users throughout the world. Within weeks of deployment, Bromium can quickly insider misuse and unauthorized software running on the network.

Each endpoint protected by Bromium is part of a Sensor Network that performs threat analysis and instantly shares IOCs with the rest of the network, for faster time to resolution. The question still remains, why spend money on AV when there are alternatives like Microsoft Defender?

Using a combination of Bromium and Microsoft as your endpoint solution gives you the best security against the latest threats and bottom line financial rewards.

Bromium and Microsoft ROI

For organizations that want close the 1% gap and effectively stop zero-days, or unknown targeted malware, and still be in compliance, Bromium suggests a dual solution with Microsoft Defender and Bromium: a robust enterprise security strategy for endpoints.

Incident response savings can be achieved.

When considering the false alerts that a SOC team has to investigate and license fees for AV, an organization can save a considerable amount in cybersecurity expenditure by using this solution. For example, take the SOC team saving on false alerts. According to Ponemon Research, the average large enterprise SOC team receives 17,000 malware security related alerts for investigation in a typical week. They only get to investigate 4% (680) of the alerts[xiii]. Moreover, organizations waste an average of 395 hours each week detecting and containing malware due to false positives and/or false negatives. The average time to investigate a security incident is 42 minutes. Based on 2016 IT Salary Survey, the average hourly rate for a security specialist is $46. That equates to a little over $18,000.00 wasted on false alerts *per week*.

Security Analyst hourly rate	$46
Reported security incidents per day	3000
Time to investigate security incident in minutes	42
Percentage of alerts reviewed by security team	4%
Daily incident investigation cost	$3,864
Annual incident investigation cost	$981,456

Security events generated by Bromium for isolated threats do not result in false alerts which can dramatically reduce an organization's costs for alert investigation. Using the abovementioned example, if Bromium reduces an organization's number of security incidents that require investigation by 30%, which equates to saving $294,000 annually.

Antivirus licenses are still required but should not cost anything.

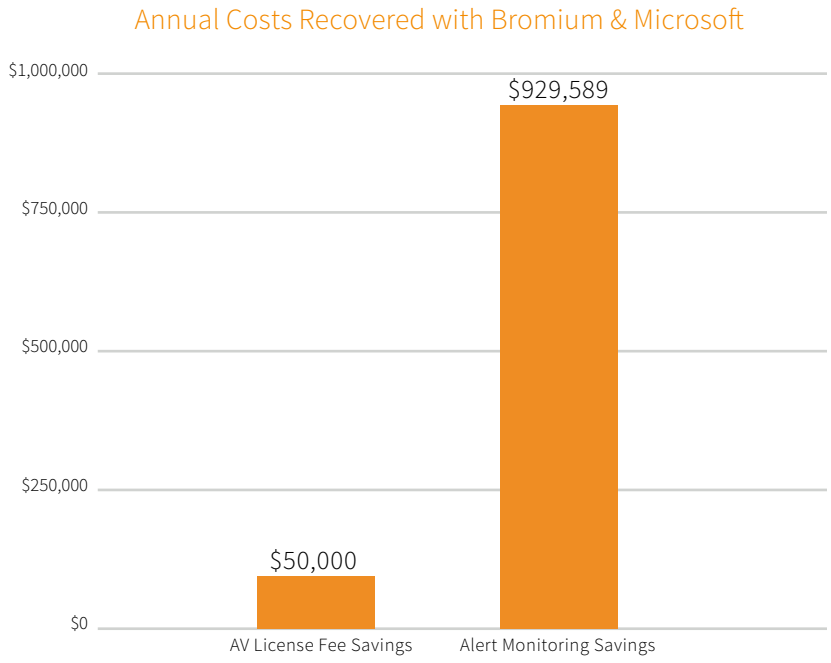
As discussed, AV is still required from a regulatory perspective. Microsoft Defender comes free and already built into Windows 10. IT organizations can still centrally manage Defender using Active Directory GPO or Windows Server Update Services (WSUS)[xiv].

The average license cost for endpoint security ranges from $5 - $25 per endpoint. For the sake of this whitepaper we will use $20 per endpoint to determine the potential cost savings an organization can achieve by using a Bromium and Microsoft solution. For an organization that consists of 2500 endpoints, the cost savings on AV alone can be $50,000.

Conclusion

The race to close the 1% gap continues to drive innovative new ideas to stop cyberattacks. Most still rely on detection techniques in an attempt to prevent malware from pre-execution. Bromium takes a completely revolutionary approach by letting untrusted files and applications run in hardware-enforced micro-VM's where the malware has no way to escape.

By using a combination of Bromium and Microsoft as your endpoint solution, you not only get the best security against the latest threats, but you can also reap the cost savings achieved by moving to the free Microsoft Defender.



[i] https://www.gartner.com/document/3512217

[ii] http://www.computerworld.com.au/article/611011/machine-learning-new-cyber-security-weapon-good-ill/

[iii] https://www.av-test.org/en/press/test-results/

[iv] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

[v] https://www.webroot.com/us/en/about/press-room/releases/webroot-2016-threat-brief-explores-next-generation-cyber-threat-landscape-and-targeted-intrusion-trends

[vi] https://www.bromium.com/resources/threat-information/advanced-malware.html

[vii] https://www.av-test.org/fileadmin/tests/corporate/avtest_summary_corporate_2015-12.xlsx

[viii] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[ix] http://www.forbes.com/sites/thomasbrewster/2015/08/26/netflix-and-death-of-anti-virus/#34d9cd873256

[x] https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

[xi] https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf

[xii] https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/increased-use-of-powershell-in-attacks-16-en.pdf

[xiii] http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

[xiv] https://technet.microsoft.com/itpro/windows/keep-secure/windows-defender-in-windows-10

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

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

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