HP Sure Click Enterprise

Security by Design: Application Isolation & Containment

WHITEPAPER

Reissued May 2020 by HP Inc.

Executive Summary

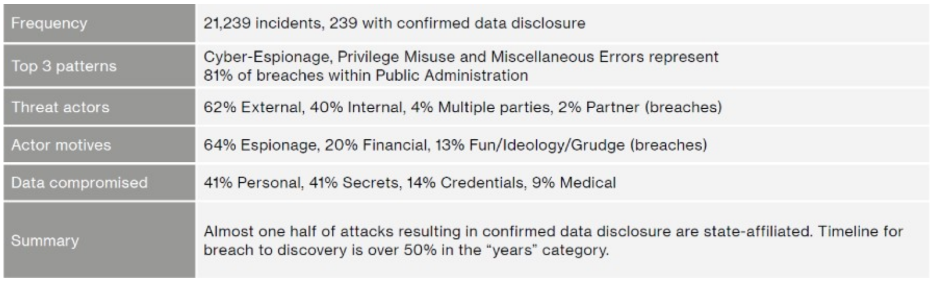
"The U.S. Department of Justice strongly agrees that they no longer worry about endpoint security after installing Bromium"

IT security teams within federal government agencies and their contractors face a daunting series of challenges in securing their networks against modern malware intrusions, including advanced persistent threats (APTs), advanced targeted attacks (ATAs), polymorphic malware, and file-less intrusions. Their networks and infrastructures are prime targets for nation-states, political agitators, organized criminals, and other hackers eager for access to truly critical content, be it for espionage purposes, to cause political embarrassment, or to reap financial gain. Furthermore, they are subject to a myriad of regulations from oversight and standards-setting organizations, both U.S. andinternational.

The Problem

The public sector-including the vital defense industrial and manufacturing bases servicing the government-represent prime targets for malicious actors, criminals, and profiteers of all stripes. High-value strategic military, diplomatic, and personnel records represent gainful and marketable targets to bad actors who go to great lengths—through patience, time, and persistence—to achieve their often-devastating objectives.

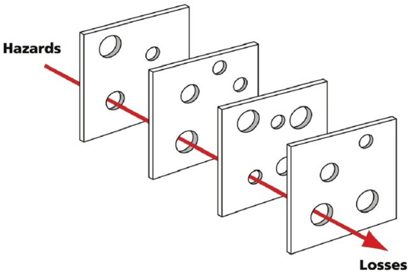
Public sector breach statistics bear this out. According to Verizon's 2017 Data Breach Investigations Report[7]: Approximately 64% of the breaches in this vertical were related to espionage; over 85% the bad actors were either nation-states or state-affiliated; and malware "dwell time" (time in residence prior to discovery) measures in years.



Frequency	21,239 incidents, 239 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Miscellaneous Errors represent 81% of breaches within Public Administration
Threat actors	62% External, 40% Internal, 4% Multiple parties, 2% Partner (breaches)
Actor motives	64% Espionage, 20% Financial, 13% Fun/Ideology/Grudge (breaches)
Data compromised	41% Personal, 41% Secrets, 14% Credentials, 9% Medical
Summary	Almost one half of attacks resulting in confirmed data disclosure are state-affiliated. Timeline for breach to discovery is over 50% in the "years" category.

Public Administration security incidents, Verizon 2017 Data Breach Investigations Report.

The Legacy Approach Not Up to the Task



The Swiss cheese layered defense model

Detection-based security solutions protect against the known 99% of attacks but struggle to resolve the remaining unknown, impossible-to-detect 1%. Threats inevitably get through, due to the dependence on legacy architectures that rely on matching against signatures, heuristics, behaviors, or other attributes that have previously been identified. How does an enterprise solve for new threats that haven't been seen before, including new breeds of file-less malware and malicious code that runs only in memory? Even next-generation AV, artificial intelligence, and machine learning techniques do not enable detection-based solutions to match the rapid innovation of exploits and techniques, due to their fundamentally limiting architectures.

[1] 2017 Data Breach Investigations Report - Verizon Enterprise Solutions

FISMA requires the "development and maintenance of minimum controls required to protect federal information and information systems" and "a mechanism for improved oversight of federal agency information security programs"

Compliance is Just the Beginning

Compliance does not equal security—it's merely a reference basis for the real security discussion. Regulations frequently list "minimum controls" required to achieve compliance certification, a starting point for each organization to then implement their policy controls to meet mission-specific use cases. In fact, in nearly all documented cases involving public sector organizations and government contractors that suffered breaches, the victims were in full compliance with their mandated regulations and current on their certifications.

Often the regulations themselves come up short, like mandating old-school anti-virus as a one-size solution when newer and much more effective advanced security solutions are readily available. Compounding the problem, compliance regulations typically lag current attacker tactics, techniques, and procedures by up to several years. With so much at stake, the minimum-compliance approach is woefully outdated and ill-suited to today's threatscape.

The Public Sector Patching Challenge

Just 33% of public sector systems are patched on time.

- VERIZON 2017 DATA BREACH INVESTIGATIONS REPORT, P.13

According to HP Security Research, Cyber Security 2016[2], the top 10 exploited vulnerabilities are all over a year old, and most have had patches available for months or even years. Unfortunately millions of PCs remain unpatched for lengthy periods within government agencies and service providers. Verizon research indicates that only 33% of public sector systems are patched in a timely manner, leaving critical systems—their valuable data and intellectual property—vulnerable to countless old and new exploits. By Verizon's generous measure, "timely" patch cycles average 12 weeks, even as Microsoft and other vendors offer monthly patches.

[2] HPE Security Research Cyber Risk Report 2016

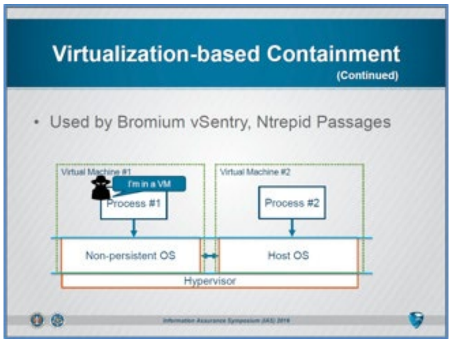
> *"By far the most effective protection solution I have seen to date."*
>
> - DIRECTOR IT GLOBAL SECURITY IN THE MANUFACTURING INDUSTRY

A New Approach is Urgently Needed

HP Sure Click Enterprise embraces application isolation at its core, utilizing hardware-enforced isolation to protect the enterprise from the inevitability of user errors, unpatched machines, and highly susceptible Internet-facing or partner-accessible devices. We've taken the ineffective practice of "bolted-on" detect-to-protect security and fundamentally shifted it to a "built-in" protection model enforced right down at the chipset. Sure Click protects by design, not relying on external detection of the unknown or the judgment of busy, easily-deceived users to keep their organizations safe. By automatically isolating all content originating from untrusted inbound sources, public sector institutions and government contractors are safe from gaps in their traditional defensive stacks and judgment lapses by their users. Conventional, advanced, targeted, file-less attacks, zero-day exploits—Sure Click isolates and prevents them all! In addition, with Sure Click, crisis patching becomes relegated to the past.

Security via Application Isolation & Containment

At the Information Assurance Symposium (IAS) 2016[3], the National Security Agency (NSA) and the Central Security Service (CSS) of the United States jointly published a presentation titled "Application Isolation & Containment for Endpoint Protection." Their premise was that true security can only be achieved by reducing the ability of a compromised process to do damage. That's precisely the approach Sure Click takes—noted specifically in the presentation—leveraging our unique, multi-patented hardware-enforced process isolation and least- privilege restrictions on all tasks running within micro-virtualized environments to create high-fidelity, low-exposure endpoints.



Virtualization-based Containment

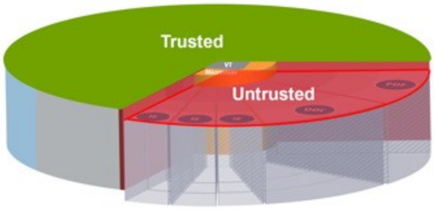
(Continued)

- Used by Bromium vSentry, Ntrepid Passages

Bromium virtualization technology specifically called out by the NSA

[3] Information Assurance Symposium (IAS) 2016 - Application Isolation Containment

Separating the Trusted from the Untrusted



Sure Click Enterprise views the host operating system and all web or file content as either trusted or untrusted

Sure Click Enterprise views the world in terms of trusted or untrusted content. Untrusted content typically originates from outside the organization and enters via various ingress vectors including web, email, cloud services, and USB. Trusted content largely originates from known internal sources or from files that an organization's own users create and distribute themselves. The two types must be treated differently.

Untrusted content might contain anything at all—previously seen or unseen, detected or undetected—and should always be regarded as potentially malicious. It should never be granted access to the actual host PC operation system, the file system, or the internal network. Trusted content, alternatively, can safely execute on actual physical resources. From the user's perspective, however, they should never see any difference in application appearance, behavior or workflow.

Application Isolation and Containment in Micro-VMs

Ransomware is safely contained within a disposable micro-VM, easily clicked away when the user closes the window.

The power of application isolation and containment is simple and straightforward—to remove the opportunity for an unknown threat to cause harm—but the execution is quite difficult. That's why Sure Click Enterprise powered by Bromium stands alone in its unique, patented approach to micro-virtualization at the hardware level, protecting the host PC from below the Windows operating system kernel, thereby dramatically reducing the attack surface. Untrusted application content stays safely protected within each micro-VM. Sure Click's one-of-a-kind approach provides protection-by-design against zero-day threats based on exploits in applications, browsers, and the kernel, a trifecta that traditional and next- generation defensive solutions can't come close to matching.

On Sure Click-protected endpoints, common Office documents such as Word, Excel, and PowerPoint—plus Adobe PDFs and other file types determined by your administrators—are application-isolated from each other and from the host PC—right down at the hardware level— inside of safe, disposable micro-VMs, so users can smoothly conduct their business without workflow disruptions, clicking on any content with confidence, knowing that their systems are secure.

Stops Initial Infection and Self-Remediates

Application isolation and containment primarily protects against the dangerous Patient-Zero infection within the enterprise, the initial compromised endpoint from which attackers seek to gain a foothold into the organization from which they can then conduct reconnaissance from lateral movement and privilege escalation. Whenever untrusted content is run within a Bromium micro-VM, a complete threat analysis is conducted, including full kill-chain analysis.

In addition to preventing malware infections at the endpoint, Sure Click endpoints self-remediate when the user closes the application window or browser tab, preventing costly and time-consuming manual remediation. Malware simply disappears forever when the micro-VM is closed, never impacting the host PC or taking root within the organization, with all threat intelligence and kill-chain analysis shared globally and preserved for security teams.

Prevents Infection Spread

When malware runs on a Sure Click-protected endpoint, it executes as intended inside the safe, disposable container, however it has no possible way of escaping the micro-VM environment onto the host PC or other network devices. Not only is the initial target PC protected, so are all other network-connected devices that interact with the targeted host. Simply put, Sure Click endpoints are complete dead-ends for malware. Malicious code has nowhere to go and can’t reach any sensitive data or processes on the host, the network, or other connected devices. Malware can’t access the intranet or file shares, preventing lateral movement and expansion.

Initial Infection	Lateral Movement	Self-Remediation
Stopped!	Impossible!	Automated!

Sure Click customers have collectively launched over TWO BILLION micro-VMs and have reported ZERO malware escapes!

Genuine User Behavior is theKey

In addition to conducting kill-chain analysis with complete micro-VM containment, Sure Click threat intelligence benefits from having real users perform real tasks on real PCs—something that sandboxing solutions cannot fully replicate through their various “user behavior emulation” techniques. Targeted malware often prompts users to act, or waits for them to act, before unleashing its complete malicious payload. Genuine users interact with documents in both predictable and unpredictable ways. Only Sure Click captures all of this actual user behavior, rather than replicating a generic subset of mouse clicks, cursor movements, text entry, and file system operations. Real user behavior generates high-fidelity intelligence.

Real user behavior cannot accurately be replicated in full by sandboxing solutions, since users are unpredictable and exhibit a wide range of activity in actual usage. Combined with single-purpose micro-VMs, Sure Click generates a very high signal-to-noise ratio for any malicious activity that deviates from genuine expected behavior.

Detection costs real money to investigate and remediate infected devices, and many alerts are faulty or incomplete. A better approach gains complete threat intelligence and full kill-chain analysis without suffering the infection in the first place-there's nothing to clean up.

Lowers Costs of Investigation and Remediation

Ponemon Institute research shows that organizations receive almost 17,000 weekly malware alerts, but only 19% are deemed to be reliable, and only 4% get investigated. Making matters worse, two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty or incomplete intelligence. Detection is clearly broken—it's costly, time consuming, ineffective, and faulty in its premise and its execution. There is a better way.

With Sure Click, investigation and remediation are vastly streamlined and reduced. Since Sure Click-protected endpoints automatically self-remediate every time users close the micro-VMs containing malicious documents or web pages, the organization's actual remediation efforts can be limited to only the remaining non-Sure Click protected endpoints, using Sure Click-supplied indicators of compromise (IOCs) and indicators of attack (IOAs). Furthermore, Sure Click devices form a comprehensive sensor network that allows for managed hunting and automated enterprise file quarantine.

Do More with Less and Simplify for Better Defense

Sure Click allows government agencies and cleared industrial contractors to provide far better security at vastly reduced costs—all with significantly less effort, since breaches are non-existent on Sure Click-protected endpoints and files can be searched for and quarantined across the network using Sure Click's IOCs and IOAs. Under this effective new security-by-design framework, other network and endpoint defenses become less important—in fact, some prominent HP customers are amply protected using only Sure Click Enterprise and Microsoft Defender, which comes pre-installed for free on newer Windows operating systems—allowing organizations to streamline their defensive stack and reduce security complexity. Bromium, now part of HP Inc. has perfected micro-virtualization defense since 2010, with BILLIONS of micro-VMs launched in live customer production environments with ZERO documented malware escapes. We know of no other security solution provider that can make a similar claim.

Talk to your HP Security representative to get started with application isolation and containment today.

HP Sure Click Enterprise

Secure Files

Malicious documents are steadily gaining in popularity with threat actors due to their effectiveness. Ransomware is commonly delivered via malicious office documents or PDFs. Secure Files hardware-isolates each supported document from the operating system and the kernel. If a malicious document is saved via an ingress application—such as Skype, email, or USB—it is hardware- isolated in a micro-VM. When the document is closed, the threat is terminated along with the micro-VM. The full kill chain is sent to the Threat Cloud and shared with all other Sure Click devices via the Sensor Network.

> *"Bromium is a clear differentiator in my security posture."*
>
> – V.JAY LAROSA, VP, GLOBAL SECURITY ARCHITECTURE, AUTOMATIC DATA PROCESSING

Secure Monitoring

Secure Monitoring helps organizations detect and respond to persistent threats already on the network by monitoring the user execution space for malicious activity. Malicious files can be quarantined and automatically removed from all network locations based on blacklist policy settings. Within the Sensor Network, high-fidelity alerts can be sent to the Threat Cloud whenever malicious behavior is found on any protected host. SOC analysts can use Sure Click threat intelligence to quickly catalog and search for indicators of compromise and indicators of attack. Secure Monitoring supports endpoints and servers.

About Bromium & HP Inc.

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.

Bromium Inc. and HP Inc. entered a formal OEM relationship in 2016. HP recognized the need to differentiate their platform security offerings by leveraging hardware-based security solutions. Beginning in 2017, HP successfully began shipping an OEM version of Bromium containment branded as Sure Click onto millions of enterprise-class devices.

Due to the success of Sure Click, HP acquired Bromium on September 19, 2019. Subsequently, HP created a new Global Business Unit, HP Security, with the Legacy Bromium team leading the new unit. As a result of the acquisition, HP has updated the naming convention of the Bromium Secure Platform product to better align with the HP Sure Click brand. HP is committed to supporting the Sure Click solution on any PC device, regardless of manufacturer, running Windows 10. Today, the Legacy Bromium Secure Platform is known as HP Sure Click Enterprise.

For more information

To learn more about Sure Click's game-changing security architecture, please visit **www.hp.com/proactive-security**.