Bromium®

Safely embrace the promise of the Internet

Comparing Bromium vSentry® with traditional security technologies

Bromium®

Executive Summary

Productivity vs. Security The internet enables unprecedented increases in efficiency, productivity and creativity while posing the greatest risk of damage and loss to digitally enabled organizations of all forms and sizes.

End-users demand free access to, and unrestricted use of the information on the web to maximize their ability to get their jobs done today. At the same time organizations have been forced to impose restrictions and cumbersome procedures to try and secure their information and resources from attack.

Today's end-user computing environment has expanded beyond the traditional control of the inner walls of the enterprise and as such, a solution must be created that provides effective end point security for the enterprise as well as a high performance interface for the user. The goal is effectively eliminating real time Internet based advanced persistent threats with minimal impact to job functions and productivity.

The problem with traditional security

The fundamental problem security today is the legacy computing architecture inherited from a much simpler time when computers were isolated systems that were only accessible to IT staff and corporate employees. The operating systems and many applications we use today were developed with little concern about the potential for introduction of hostile or "untrustworthy" applications or data. Unfortunately these systems have not kept pace with the growth in connectivity, and our computer systems still have no way to decide whether a document or an application is trustworthy or hostile. Malware continues to exploit the interaction between and within the software installed on a system to achieve its goals with little protection provided by the system itself.

Current IT security products evolved in response to the earliest cyber-attacks of the 1980s. Network firewalls were developed to foil attacks originating across network links and isolate the entire network. Anti-virus programs were developed to address the new phenomenon of "infected" files being shared via floppy disks and attempted to isolate individual computers from harm. Over time, new security products have been continually "layered on" as new attack vectors, such as the Internet, have become available. Each layer tries to solve the same problem: Is the data or the application trustworthy? Untrustworthy content is detected and blocked, and trustworthy content is allowed, but if an incorrect decision is made, the malware is free to interact with, and compromise all the other parts of the system.

Malware is now designed to evade detection. By leveraging zero day exploits, polymorphism and the rapid evolution of web technology, malware evades "detection" based security solutions and infiltrates the organization by exploiting the inherent trust between operating system components. It may be weeks or months before a successful attack is discovered. Meanwhile valuable information can be stolen or critical infrastructure can be disrupted by the attackers.

"Over 1 trillion dollars' worth of intellectual property is reported to have been stolen every year as a result of cyber-attacks"
NATO Deputy Assistant Secretary General for Emerging Security Challenges, 2011

***"The average organizational cost of a data breach this year* increased to $7.2 million"**
Ponemon Study 2011

"40% of IT executives expect a major cyber security incident to hit their sector within the next year"
Center for Strategic and International Studies

End-users have emerged as the weak link in enterprise security. With the proliferation of web, email and social communication, users are one click away from compromising their desktop. Mobile laptop users are further exposed as they have limited protection from the corporate network based security mechanisms. Current defenses can be cumbersome to use and manage. All too frequently employees feel disempowered by security restrictions, which can have a major impact on productivity. As security policies become ever more complex to address compound threat vectors, the likelihood for mistakes by well-intentioned users grows. Unfortunately, all it takes is one mistake on the part of one employee to compromise the entire enterprise.

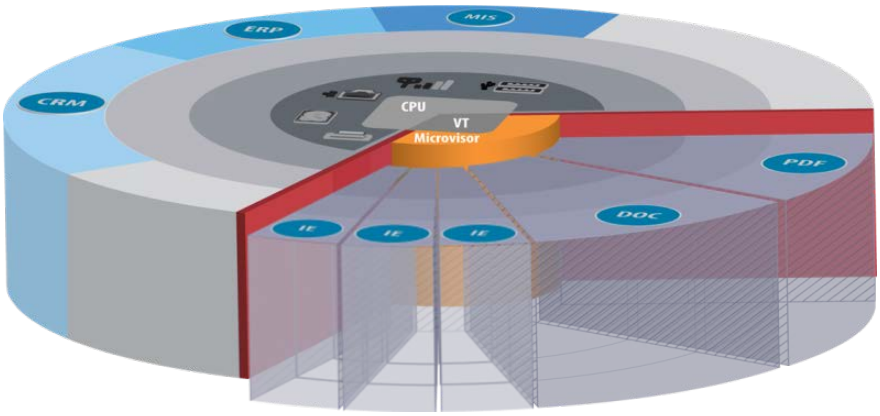
Enterprises have spent billions of dollars on security but can't stop all of today's attacks Legacy security solutions attempt to detect and block malware using signatures or behavioral analysis. This black-listing approach can only detect known threats and fails to stop sophisticated malware that is used for today's targeted attacks. White-listing - allowing only trusted applications, such as a corporate browser or pdf reader - is ineffective because attackers take advantage of the fact that enterprises are slow to update their software, and use malicious content and documents to exploit supposedly trustworthy applications.

All software is inherently insecure Modern desktops and apps offer rich feature sets that offer a huge target to attackers. Microsoft Windows now has more than 60 million lines of code, and Adobe® Acrobat more than 1 million, leaving many loopholes that can be exploited by attackers. This vast "attack surface" is responsible for the enormous number of ongoing vulnerabilities and exploits we see in the news every day.

Efforts have been made to increase productivity and decrease resource consumption by allowing users to perform multiple instances of a programs function using a single instance of the application such as "tabbed" browsing. These multiple instances or "tasks" make security more difficult as compromising the parent application automatically compromises all the tasks being performed by the application.

The "whack a mole" approach to creating a new signature or patch to detect and block the latest attack, or developing a new security product for a new kind of vulnerability is unsustainable. The security industry needs to address the fundamental shortcomings of the current approach, and adopt a new architecture that transforms computer systems into trustworthy endpoints that are protected by design.

Bromium micro-virtualization: A new approach to endpoint security



Bromium has developed a second-generation virtualization technology, micro-virtualization, that addresses the fundamental shortcomings of the legacy computing model by executing each vulnerable task in a tiny, hardware-isolated micro-virtual machine (micro-VM). Tasks are isolated, along with all the associated resources that a task needs, all the way down to the security hardware (Intel VT) layer, including any resources that interact directly or indirectly with the task. Protected tasks have only "need to know" access to data, networks and local hardware devices,

so if a task is compromised, the system still protects the enterprise and the user. Micro-VMs are created and destroyed in milliseconds automatically discarding malware and ensuring that the desktop always remains in a “golden” state. These capabilities are implemented automatically, unseen by the user, and with minimal impact on the user experience.

Bromium micro-virtualization has profound consequences for system architecture, and applies to both server and client systems. Its application in endpoint protection transforms the resilience of enterprise clients and will massively increase the cost and complexity of system penetration.

Introducing Bromium vSentry - Security by Design

vSentry offers a completely new approach to endpoint security that relies on isolation rather than detection and blocking of threats. vSentry uses Bromium microvirtualization to isolate malware delivered via Internet Explorer or untrustworthy documents and e-mail attachments. Malware isolated by vSentry is unable to steal data or access either the Windows system or corporate network and is automatically discarded when the web session or document is closed by the user.

vSentry is engineered to defeat malware Each micro-VM is optimized and provisioned for the specific task at hand and is hardened against the installation of malicious code. Today’s software presents millions of lines of code and a seemingly infinite number of possible interactions and vulnerabilities that hackers exploit to gain control of a system. vSentry delivers significant attack-surface reduction as a direct result of micro-virtualization which delivers an inherently more secure platform for running risky tasks.

If unknown malware does manage to exploit the application performing the protected task only a single browser tab or a single instance of the document handler (Acrobat, Word, etc) will be compromised. Malware cannot gain access to other applications or tasks, the Windows system itself, the protected file system, the enterprise network, or trusted SaaS applications. Since each web page or document is run in a hardware-isolated, hardened and independent container within the Windows environment, threats can’t propagate and compromised sessions can’t be used for surveillance or to launch attacks on other systems in the network. Malware is not allowed to persist and is automatically removed on closing the web browser tab, document or attachment.

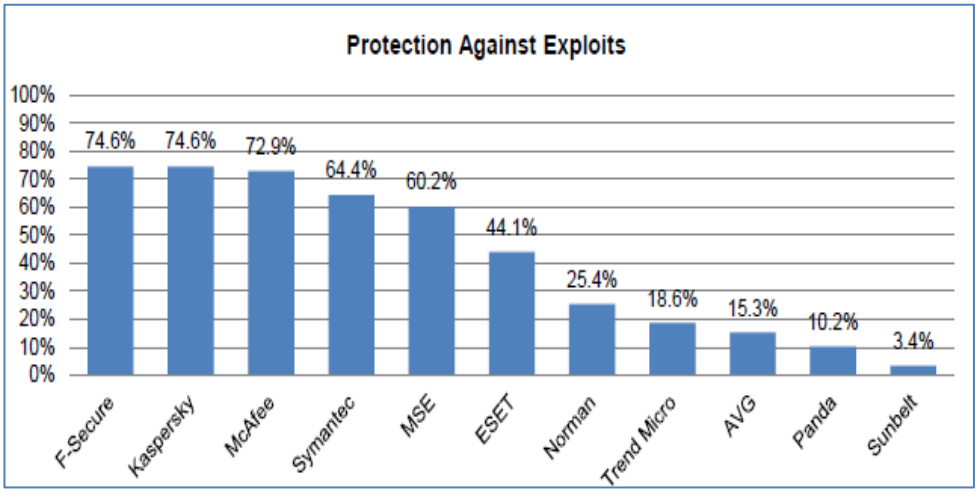
vSentry isolates and protects today’s most risky behavior Installed on a standard Microsoft Windows 7 desktop, vSentry automatically and instantly isolates vulnerable tasks, such as opening an unknown web page in a new browser tab or an email attachment or document from an unknown sender. vSentry enables the creation of hundreds of micro-VMs dynamically and in real time on a desktop. Users are not prompted to “allow” or “deny” actions and can focus on getting the most from their system without worrying about the chance of compromise.

vSentry leverages advanced hardware security capabilities to defeat advanced malware The Bromium Microvisor on which vSentry is based integrates directly with Intel VT advanced hardware virtualization technology which is built into every CPU, to ensure that malware can’t break out of the vSentry micro-VM to compromise the rest of the Windows operating system, other applications or tasks.

vSentry and traditional endpoint security products

Anti-Virus systems detect malware by using signatures that are developed from samples of attacks that have successfully compromised other users. The addition of heuristics and cloud based lookups has decreased the time needed for AV systems to detect known attacks, but with over 3 billion unique pieces of malware discovered in 2011 alone, today's attackers have little problem avoiding these systems. Anti-virus does provide detection of most known forms of malware and provides protection against those attacks that are targeted at the areas vSentry does not currently address such as exploits of shared internal network servers.

Bromium vSentry does not rely on detecting malware to protect against its malicious intentions. Instead, the granular isolation and "need to know" access model for each task ensures that malware cannot gain access to any data, persist the attack, or penetrate deeper into the network.



NSS Labs Consumer AV test 2009

Host Intrusion Prevention Systems attempt to detect and block malicious attacks by comparing the behavior of vulnerable applications with a pattern that could indicate "malicious behavior". The shortcomings of this technology are that malicious and benign code can perform the same types of operations within an endpoint and singling out the behavior of a single piece of software can be challenging. A Host IPS system that is tuned to be effective against unknown malware will also block many unknown but benign software functions leading to user dissatisfaction and an avalanche of corporate help desk calls. Host IPS is often disabled or tuned to the point that malware is no longer blocked in reaction to these problems.

Bromium vSentry does not interfere with the execution of the vulnerable application or the productivity of the user while ensuring that critical enterprise resources are protected at all times.

Desktop Firewalls protect the host system by blocking low level network requests to specific processes within the the endpoint. Desktop Firewalls do not provide any protection for the most risky applications like the web browser or opening files and attachments as these processes must be able to communicate with the outside world to function.

Bromium vSentry implements a per micro-VM, task-specific, granular isolation or task “firewall” capability by intelligently isolating, filtering and enforcing the communications between each task and the rest of the Windows environment.

Desktop Virtualization Systems provide a mechanism for running multiple operating systems on a single desktop or laptop computer. Migrating computing resources to a virtualized environment has little or no effect on most of the resources’ vulnerabilities and threats. While running, these solutions provide no protection beyond that provided by standard desktops and the monolithic nature of traditional hypervisors lend themselves to the execution of multiple applications within the virtual machine. Attempting to run multiple virtual machines often incurs a heavy performance penalty and restricts the granularity and effectiveness of this approach.

Bromium vSentry represents the next generation of virtualization technology that hardware virtualizes each vulnerable task without the performance penalty incurred by legacy virtualization solutions. vSentry works at the task level within the Windows environment and provides full code level visibility and extremely granular control for all interactions between the active task, Windows, system devices, the file system, storage and networks.

Application Whitelisting Solutions restrict end users from using “non-approved” programs on their systems. This approach typically has a large impact on user productivity which often results in users finding “workarounds” such as performing critical tasks on mobile or home products. Application whitelists provide no protection from attacks targeted at the “approved” programs which remain vulnerable to zero day or targeted attacks routinely delivered within the content the applications are tasked with processing.

Bromium vSentry does not impact user productivity and enables them to use their key productivity applications safely and with no risk to the critical information contained within their systems or on the corporate network.

Patch Management Solutions attempt to address the root cause of security exploits by providing fixes or ”patches” to the underlying vulnerabilities in the programs that are at risk. Unfortunately the sheer scale and attack surface of today’s operating systems and application suites provides endless vulnerabilities. Organizations spend huge amounts of time and money testing and deploying patches in an endless attempt to keep their systems secure with little impact on the number or frequency of successful attacks.

Bromium vSentry protects PCs from being compromised, *even if they have not been patched*. This enables organizations to schedule patches for the lowest impact on the organization.

In Conclusion

A Platform for the Future: Bromium micro-virtualization addresses the two fundamental challenges of today’s computer systems: Users will make mistakes, and software will have vulnerabilities. vSentry allows users to make mistakes, but protects them nonetheless. vSentry is designed to protect the system even though vulnerabilities exist by using hardware-enforced isolation. vSentry delivers a user-experience that delights users, empowering them and protecting them, and enabling them to experience all of the power and capabilities of a great modern desktop environment.