Bromium®

Bromium vSentry®

Defeat the Unknown Attack

Introduction

Bromium vSentry protects enterprise PCs and virtual desktops from undetectable advanced malware that attacks the enterprise by tricking users into accessing untrustworthy content that originates outside the enterprise. vSentry is built on the Bromium Microvisor™ – a small, security-focused hypervisor that automatically, instantly and invisibly hardware-isolates each untrustworthy task – one that is processing data or executing code from an untrustworthy source – in a micro-VM that cannot modify Windows or gain access to enterprise data or networks. vSentry protects enterprise desktops that haven't been patched and eliminates costly remediation by automatically discarding malware.

vSentry does not rely on legacy signature-based detection that can only block *known* attacks. It defeats *all* attacks by design. And when malware strikes, that same design enables vSentry to deliver real-time live attack visualization and analysis, permitting security teams to rapidly achieve defense in depth.

vSentry allows IT to focus its resources on strategic business needs, safely embracing key trends in mobility and consumerization of IT. It eliminates the risk of the unknown – so IT can let users open attachments, click on any link, or open any file – without risk. It delivers real-time insights into undetectable, targeted attacks, without false alarms, helping IT to quickly respond to new attacks. It revolutionizes information protection, ensures compliance – even when users make mistakes, eliminates remediation, and empowers users – saving money and time, and keeping employees productive.

vSentry is deployed as a standard Windows MSI package, and configured with simple policies using Microsoft® Active Directory. It delivers XML formatted logs and alerts to third party management consoles via the Bromium Management Server, a lightweight, web-services based management server that centralizes alerts and ensures that vSentry is running on all clients.

The Challenge

Today's users are mobile and technology-literate. Their demands for a rich computing environment that supports both personal and work activities have placed the CIO in an awkward position: On one hand users demand the ability to access both work and consumer applications from any device, anywhere, and on any network. On the other, regulatory requirements and the need to secure the enterprise from targeted attacks require constant vigilance to protect enterprise data and infrastructure. These conflicting demands leave IT in crisis: Hobbling users with the goal of increasing security makes IT a barrier to productivity, and doesn't demonstrably increase security. IT needs to get back to its core mission – empowering users to deliver value – but lacks the tools to achieve this.

The Desktop: Achilles Heel of the Enterprise

Over the last decade server virtualization has transformed legacy tactical and manual data center IT practices into strategic, agile, scalable and highly available virtual infrastructures and private clouds. But the majority of enterprise desktops have remained mired in expensive, manual and non-strategic labor practices.

Today's enterprise desktop environment is undergoing tremendous change. Mobility, tablet form factors, application compatibility across environments and security challenges leave IT with massive challenges. Many environments still rely on Windows XP, but most are well on their way to adopting Windows 7 on both PCs and via server hosted desktop virtualization.

The diversity of desktop OS versions, client devices and access modes has left security professionals reeling. Keeping environments patched and secure is an increasingly daunting task, and security is further challenged by the rapid evolution of malware and the sophistication of advanced attacks that can be precisely targeted at both the enterprise and a specific user. The cost of remediation and forensic discovery is escalating, and breaches place proprietary information, regulatory compliance, and brand reputation at risk.

Today IT has no choice but to assert control over users – and the networks, applications, media, websites, and documents that they use. But this approach will surely fail: productive employees have to collaborate and communicate, and when they do so a single click can lead to the next major breach. It is impossible to protect against the unknown, undetectable attack.

"Detection" and "Security": A Relationship in Crisis

Today's end point IT practices are out of step with users *and* attackers: The problem is a comprehensive failure of the "detect to protect" paradigm that evolved from traditional anti-virus design: A dependency on signatures to detect known threats.

McAfee reports identifying 100,000 unique malware variants per day. Traditional signature and behavior based endpoint protection vendors now face the staggering challenge of creating and distributing almost a million signatures per month – to every endpoint. Today's signature files easily exceed 100MB, posing severe distribution challenges. And even the most sophisticated detection algorithms are far from perfect: Tuning detectors is an art – trading off false alarms (which train users/IT to ignore alerts) against false negatives (which let attackers succeed) – and requires careful analysis and a large, current data set. But

- Today's organization- and asset-targeted malware adapts fast, leaves no time for human assessment, and reduces the value of historical attack data sets. Moreover,
- It is provably *impossible* to accurately detect polymorphic malware. We quote: "The challenge of signature-based detection is [to check…] O(2 8n) signatures. […] To cover 30-byte [malware] decoders needs O(2240) signatures; for comparison there are about 280 atoms in the universe."

The Result: “Compromise-first Detection”

Since a failure to detect allows an attacker to succeed, vendors must either tune their detectors to alert at the first sign of an attack – increasing false alarms, or delay detection until malware actually compromises the system – at the risk of allowing the attacker to succeed. Whatever the case, the system must be re-imaged, incurring remediation costs and downtime for users.

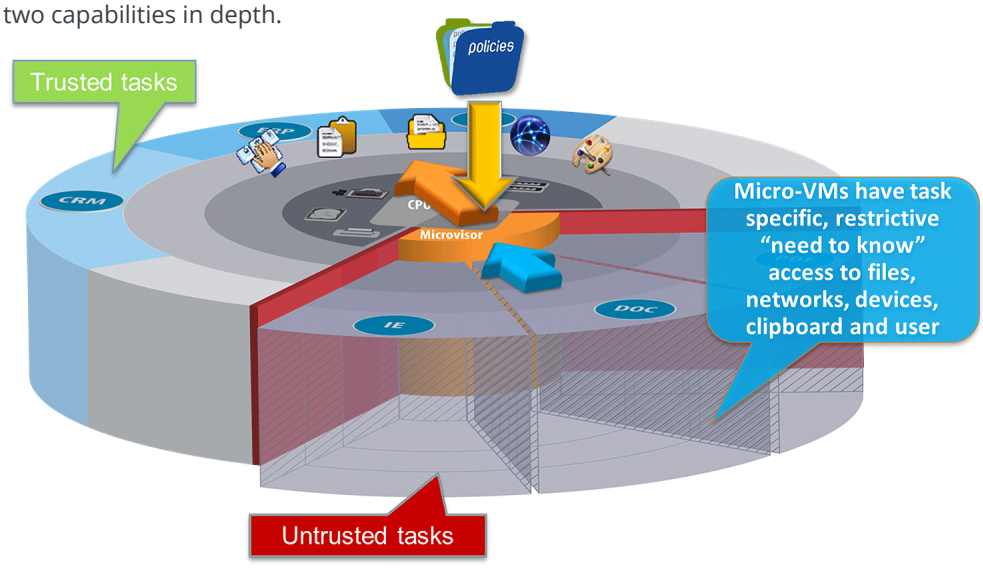
vSentry: Protect-first, and Defend in Depth

Bromium vSentry makes enterprise Windows® desktops – both PCs and hosted virtual desktops – more secure *by design*, enabling IT to securely empower users to access untrusted attachments, documents, media and the web without risk to data, applications or networks. vSentry protects – always – without any need for signatures. In addition, vSentry delivers real-time analysis of targeted attacks that legacy detection-centric tools can neither identify nor block. Accurate analysis of targeted attacks allows IT to rapidly achieve defense in depth. The attack will be defeated, no remediation is required, and the attacker cannot penetrate the infrastructure.

vSentry was designed to deal with the inescapable realities of vulnerable software and targeted persistent attacks that trick users into executing malware that is impossible to detect using traditional tools. It is built on the Bromium Microvisor, which automatically and invisibly hardware-isolates each vulnerable desktop task using CPU features for hardware virtualization. A compromised task cannot attack the desktop, persist an attack, steal data or penetrate the enterprise network. When the user closes the task’s window any changes it has made are discarded – automatically erasing all malware.

In addition, the granular confines of a micro-VM afford vSentry a perfect view of executing malware as it attacks. Since its architecture will defeat malware by design, vSentry can safely permit malware to execute to completion. In doing so it accumulates detailed insights that enable *live attack visualization and analysis* for unknown malware, without any risk of the attack succeeding. Security teams can immediately use these analytical insights to achieve defense-in-depth.

Bromium has for the first time de-coupled *protection* from *detection*. vSentry protects by hardware-enforced isolation. Its design also revolutionizes malware analysis, and hence real-time defense against un-detectable malware. The following sections discuss these two capabilities in depth.



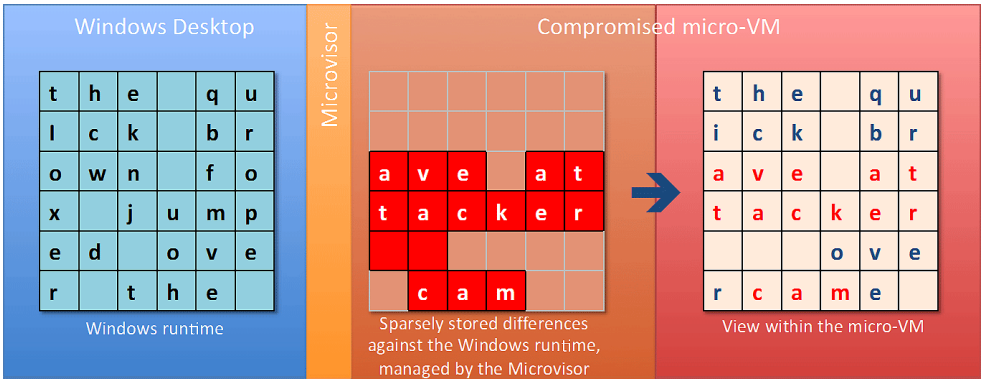
Micro-virtualization Enables “Protect-always” Security

The Microvisor extends the isolation and protection of hardware virtualization into Windows and its applications, adding a new hardware-protected execution mode for untrustworthy tasks. These micro-VMs are automatically created in a fraction of a second to isolate any task that processes untrusted data or interpreted code, or that accesses an untrusted network.

Windows sees micro-VMs as tasks under its control – it schedules them and tracks their performance and resource use. Micro-VMs are small because they contain only task-specific state, and they run natively with full performance. They offer complete compatibility for all applications, and provide hardware-enforced protection for the desktop, enterprise data, applications and networks. Best of all, micro-VMs do not negatively impact the user experience.

Two key innovations in the Microvisor are critical to the vSentry security model:

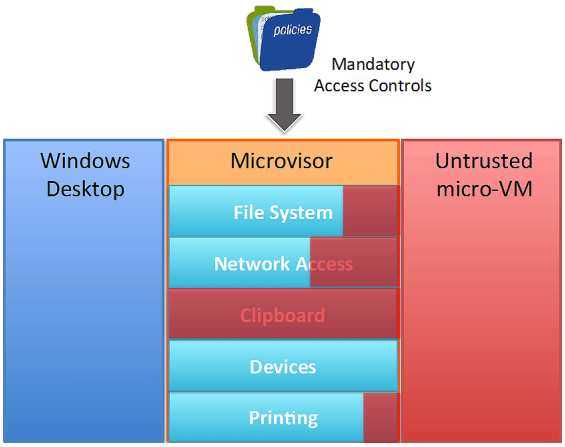
1. Micro-VMs execute “Copy on Write” against the IT-provisioned Windows desktop.
2. Critical system resources are isolated from micro-VMs based on “need to know”.



Copy-on-Write Execution

As a micro-VM executes, any changes that it makes to Windows memory or to files in the IT-provisioned golden image are made on a “Copy-on-Write” (CoW) basis – the writes are cached locally in the micro-VM but no changes are made to the running Windows desktop or its file system. As far as the task in the micro-VM is concerned, its changes are real.

If malware tries to modify the Windows kernel or overwrites a DLL in the file system, it will (incorrectly) believe that its attack succeeded, and when the user closes the task window the micro-VM and all of its cached CoW changes are discarded, automatically discarding the malware.



Micro-VMs See Only What they “Need to Know”

vSentry uses the Microvisor to enforce strict control over access to key system resources, including the file system, network services, all devices, the clipboard, and any interaction with the user.

When a micro-VM is created its access to these resources is narrowed according to a set of (automatically configured) task-specific policies that enforce an *absolute* "need to know" – the micro-VM can access only the absolute minimum resources that it needs. This is superior to the ACLs used in today's operating systems because:

1. *Only* the specific resources needed by the task are visible to it; all others are invisible.
2. An idealized subset of the file system of the IT provisioned Windows installation is visible – to ensure that isolated tasks execute correctly – but is protected by CoW semantics.

For example (these policies can easily be changed):

- A browser task for an untrusted site such as Facebook needs only the cookie for facebook.com in order to correctly execute, so the file system for the micro-VM should contain just this single file, and no others. The task needs connectivity to the untrusted Internet, but should never have access to the corporate Intranet or to any high-value SaaS sites. It needs to play video, so it ought to see the speakers, but it should not be aware of the web-cam or other USB devices.
- A task that is rendering an untrusted PDF email attachment needs only the PDF file in its file system, and should have no network or device access.

A granular implementation of "need to know" is key to defeating un-detectable attacks: Because users must open untrustworthy documents, sites and attachments that could hide an attack, the absence of high value data, networks and devices in a micro-VM prevents an attacker from gathering information and reaching deeper into the enterprise infrastructure. Malware cannot open a file that doesn't exist, probe an un-reachable DNS or network, or turn on a non-existent web-cam. It cannot compromise the clipboard either, because it can only be used by the user at the keyboard, and then only if IT permits it.

Enforcing "Need to Know"

Whenever a micro-VM attempts to access any restricted resource, its execution is automatically interrupted by the virtualization hardware, which hands the CPU to the Microvisor. The Microvisor enforces "need to know", taking into account

- The resources that *are* explicitly visible to a micro-VM
- Any additional per-task policies set by IT that grant additional privileges: For example
  - The enterprise web-conferencing SaaS service might be permitted to use the web-cam.
  - A spreadsheet might need data from an Intranet share-point site.

File System Isolation

Each micro-VM is presented with a file system which contains an idealized, de-privileged golden Windows installation (automatically created by vSentry from the IT provisioned Windows installation), that is protected from modification by an efficient block-wise Copy-on-Write cache mechanism managed by the Microvisor. On exit all CoW file system modifications are discarded.

Each micro-VM has a task-specific persistence policy that dictates which of its files (if any) can be saved. For example, a browser task is only permitted to make changes to its cookie and DOM storage. Any persisted files are securely tagged as untrusted, and the Microvisor ensures that any attempt to access an untrusted file can only be made be made from another untrusted micro-VM. Subject to enterprise policy, untrusted files can be attached to emails and managed like normal files. In addition, IT can choose to allow users to trust files that they need to edit. Untrusted files can also be securely printed.

A micro-VM can only access files that are visible in its file system. However, it can also ask the Microvisor to give it access to additional file(s). For example, when a user clicks on "attach a file" within web-mail, vSentry (subject to IT policy) can enable the user to select a file(s) in Explorer to be injected into the file system of the micro-VM – without changing the user experience in any way.

File Shares

Most enterprises expose CIFS/SAMBA based shares to end-users for backup and to permit collaboration. vSentry offers two key capabilities to manage trust and data provenance in a shared storage environment:

- IT can define Trusted Shares. These are in essence equivalent to C:\ on the PC. Any file on a Trusted Share is trusted, unless it has been securely tagged as untrusted by vSentry.
- Shares that are not explicitly trusted are Untrusted Shares. All content on an Untrusted Share is automatically untrusted. By default all externally mounted media (including USB keys) are treated as Untrusted Shares.

Network Segmentation and Isolation

Today's targeted malware seeks to use compromised PCs as a way into the enterprise network, attacking other systems to persist software that exfiltrates data. When a single PC is compromised the Incident Response (IR) team has to investigate every possible move of the attacker, at enormous cost.

vSentry solves this problem by enforcing "need to know" for network services. It divides network sites into four categories (which are configured by IT, and optionally the user):

1. The **untrusted Internet** contains all sites by default, excluding the following:
2. **SaaS and cloud sites** include applications and services used by the enterprise, and (if enabled) sites of high value to the user such as their bank;
3. The **enterprise Intranet**;
4. Nominated **trusted sites** such as update.microsoft.com that need direct access to the underlying OS are allowed privileged access to Windows.

Any traffic to or from a micro-VM is firewalled (up to the application layer) by vSentry, which also controls access to the DNS and other network services, including enterprise web-proxies that require NTLM authentication. Micro-VMs do not share the same logical network and have no access to or awareness of each other, ensuring that there is no opportunity for micro-VMs to communicate. Finally, vSentry polices access by each micro-VM to ensure that the micro-VM can only communicate with hosts on the networks that are available to it in its network containment policy. The default policies are as follows, but can be overridden by IT:

- A task that needs no network connectivity (such as a PDF reader) is unable to access any network services. DNS queries will fail, as will directly addressed IP flows.
- A task accessing a trusted site or an Intranet site with a valid certificate, over a secure connection, does so directly outside vSentry. (eg: updates from update.microsoft.com). Intranet sites need not be trusted.
- A task accessing a SaaS site, such as salesforce.com, can only communicate with that site and sites that the SaaS site explicitly incorporates. For example salesforce.com uses chatter.com and force.com.

› Finally, a task accessing any untrusted site is only permitted to communicate with sites on the untrusted Internet. It cannot resolve a DNS query or send directly addressed packets to any SaaS sites, the Intranet, or trusted sites. A good example is facebook.com, which needs access to other sites to deliver elements of each page, but which must not be allowed to "follow the user" onto the enterprise SaaS site salesforce.com.

The Registry

A task's view of the Windows Registry in a micro-VM is substantially reduced from that of the Windows desktop. SAM (Security Accounts Manager) entries are removed, and only a subset of the registry of the IT-provisioned Windows image is visible, namely settings for applications that can be spawned in micro-VMs.

Printing

Targeted malware can persist within a printer where it copies data for exfiltration, but all users need to be able to print untrusted content (e.g. maps). vSentry allows untrusted content to be safely printed (if permitted) by first securely converting the document into a trustworthy format that can be safely directed to an enterprise printer.

The Clipboard

The Windows Clipboard and other sharing mechanisms are common vectors for malware. vSentry offers several enhancements to the traditional insecure "cut & paste":

1. Access to the clipboard is controlled by IT policy, and enforced by the Microvisor
2. If clipboard access is allowed, then
   a. Only the user at the keyboard can initiate it. It cannot be accessed programmatically.
   b. Its use is not symmetric. By policy, each user can have the following controls implemented: Copy/Paste between micro-VMs is enabled or disabled; Copy/Paste between an untrusted micro-VM and Windows is enabled or disabled, or they are enabled only in particular cases.
3. Format conversion forces untrusted data into a safe format before it can be pasted. For example, data containing font and text information is safe, but Word® macros represent a risk.

Device Isolation

By default vSentry prevents direct USB device access from a micro-VM to prevent these devices from being used by malware. Task specific exceptions can be configured to permit USB devices to be exposed. For example, a web-conferencing SaaS service may need access to the webcam. By default all USB based file systems are always untrusted.

vSentry's Live Attack Visualization and Analytics

vSentry defeats attacks by design, and that same design also enables it to offer unparalleled live analysis and visualization (LAVA) for otherwise undetectable malware, before signatures are available. This section describes how vSentry gains the insights needed to understand the origin, targets and vectors of an attack, to permit defense-in-depth.

vSentry has three unique advantages:

1. Because it will defeat the attack by design, vSentry can allow suspected malware to execute to completion. Accurately detecting the early stages of an attack is difficult, but at some point the attacker must persist the attack and compromise Windows – these are readily observed in a micro-VM.
2. Since each micro-VM contains only a single (known) task, it is easy to spot abnormal activity for the task (for example, an Internet Explorer task cannot install a USB device driver into the Interrupt Dispatch Table). In addition, genuine malicious behavior within the micro-VM clearly indicates that its task has been attacked.
3. The Microvisor can observe the execution of a micro-VM from the outside – known as introspection – obtaining a perfect view of every stage of execution and enabling it to spot OS-level compromises such as boot-kits and root-kits that are invisible to in-OS detectors.

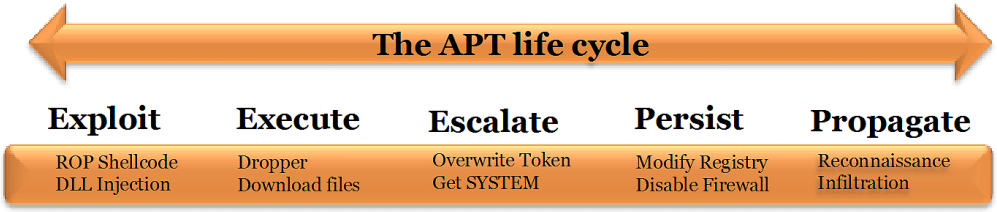
Bromium's use of introspection in the context of micro-VMs is uniquely powerful. Although the potential for a hypervisor to use introspection to detect malware in a *traditional* VM is widely known, it is impractical:

- It imposes a significant performance penalty on the VM
- Observing an entire VM as a single entity offers insufficient granularity for accurate detection of application-specific attacks
- The transactions that a traditional hypervisor can observe in a VM are too coarse grained to be useful for analysis. For example :
  - It is impossible to properly relate low level block storage or packet I/O to application layer semantics.
  - On a desktop, modifications to the kernel include dynamic addition of drivers – for example for a USB stick. It is impossible to tell in the context of a VM, if this is malicious or benign.

The Bromium Microvisor isolates each vulnerable task in its own micro-VM, permitting vSentry to be intimately aware of both task level semantics and application layer transactions. vSentry:

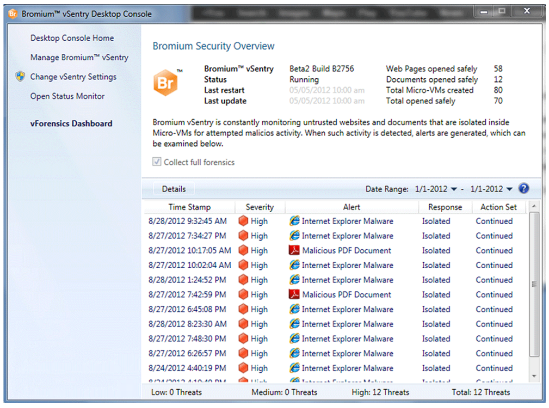
- Controls file system and Registry access;
- Controls all communication services such as DNS queries, domain / share access, connection and SSL VPN setup, and NTLM authentication; and
- Monitors all system calls made by a micro-VM.
- Task-level awareness, together with (CoW managed and micro-VM cached) updates to the Windows file system, runtime memory and registry make it much easier to determine malicious intent.

Micro-VM Behavioral Analysis

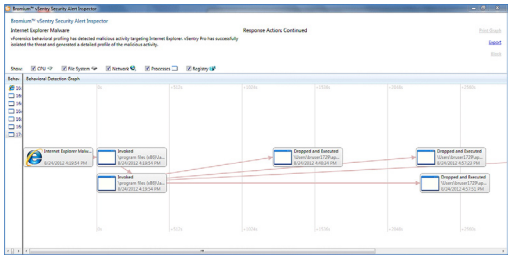


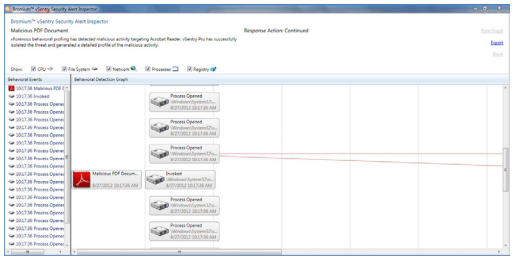
vSentry includes a powerful behavioral inspection and analysis engine that uses per-micro-VM introspection and instrumentation at a granular level: Rather than focusing solely on the first two stages of the malware lifecycle, like today's detectors that have to detect early in order to be of value, vSentry can gather data across the entire lifecycle of an APT, even allowing malware to execute to "completion". A memory exploit, execution of a new task, an attempt to access the shell, file persistence, and attempts by malware to connect to external command/control centers or bot-nets, or to propagate into the Intranet – are all visible to vSentry and explicitly controlled by the Microvisor. Moreover the Microvisor is in control of time – as seen by the task – and has the benefit of a fully instrumented Windows system call interface – which is not possible for legacy detection systems because of Microsoft PatchGuard.

vSentry offers IT a configurable interface for visualization and analysis, that allows the security team to trade off the benefits of early alerts versus full post-attack analysis. Attacks that have been identified by vSentry are presented via the vSentry management console, permitting IT to quickly understand the specific threats to which the enterprise is exposed.

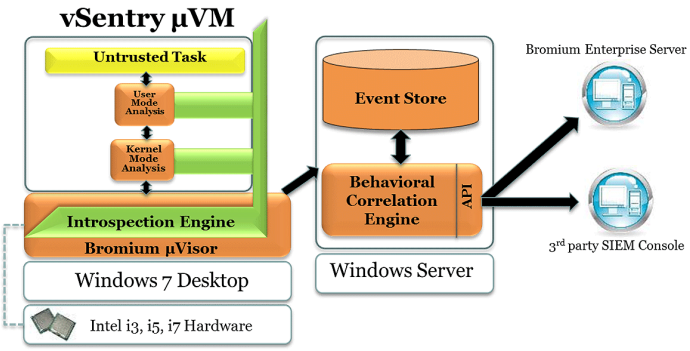


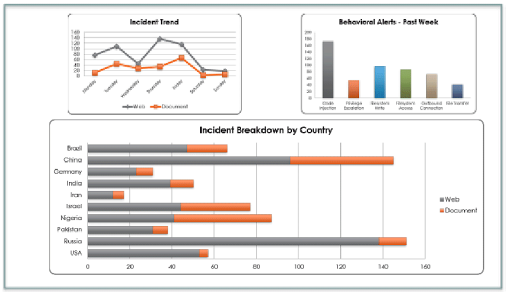
When malware strikes, vSentry provides the full execution trace for the compromised task, enabling IT to gather information on the vector, target and methods used by the attacker. Full details of the attack are preserved including network traffic, file signatures and all changes that malware attempts to make to the operating system and/or file system. Since the specific context in which the attack arrived at the desktop is available, together with the task state for the micro-VM, IT can pinpoint the origin of the attack and its vector into the enterprise, and identify the specific assets targeted by the attacker. vSentry automatically computes cryptographic digests of key components of the attack such as persisted files, which can be used as signatures in existing network infrastructure protection systems to achieve defense in depth.

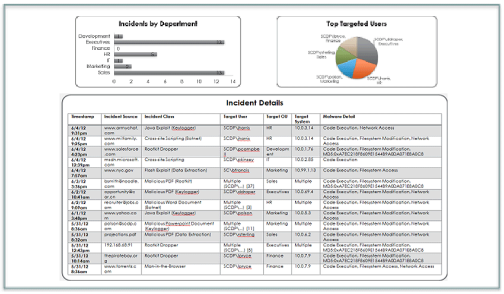




vSentry captures all relevant details for live attack visualization and analysis, and delivers this information to a centralized event store – the Bromium Management Service or BMS – where correlation analysis across all desktops in the enterprise can be efficiently computed to deliver an enterprise-wide view of trends in attack behavior. Alternatively, the vSentry BMS can deliver data to 3rd party SIEM consoles or to an IT data store such as Splunk®, permitting custom applications to be built for visualization of attacks across the enterprise. For more information on vSentry event processing, please consult the relevant product documentation.







Conclusion

Bromium vSentry protects enterprise data and networks *by design* – a design that relies on hardware isolation to defeat unknown attacks, and enables it to deliver ground-breaking live attack visualization and analysis *without* false alarms. It eliminates labor-intensive, costly and non-strategic desktop practices, enabling IT to focus on its core mission of empowering users to be productive, no matter how or where they work. With vSentry, IT can

- Be confident that advanced malware will be isolated and defeated, even if desktops have not been patched against the latest vulnerabilities
- Obtain actionable insights including signatures for otherwise undetectable attacks, in real-time, permitting rapid defense in depth
- Avoid the cost and downtime of remediation. Malware is automatically discarded, keeping users productive
- Automate complex, expensive, manual investigations by the Incident Response team. Malware cannot penetrate the enterprise infrastructure to persist hidden attacks.

Bromium HQ
20813 Stevens Creek Blvd, Suite 150
Cupertino, CA 95014
info@bromium.com
+1.408.598.3623

Bromium UK Ltd
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

#Bromium-wp-vSentry-1212e