Secure Browsing – powered by Citrix XenApp, Citrix XenServer Direct Inspect APIs and Bitdefender HVI

This white paper outlines the gaps in providing a secure browser, including research into data breach trends and provides a practical solution for centralizing and securing browsers. The solution includes combining Citrix and Bitdefender technologies in an innovative approach centered on new virtualization and hypervisor introspection technologies.

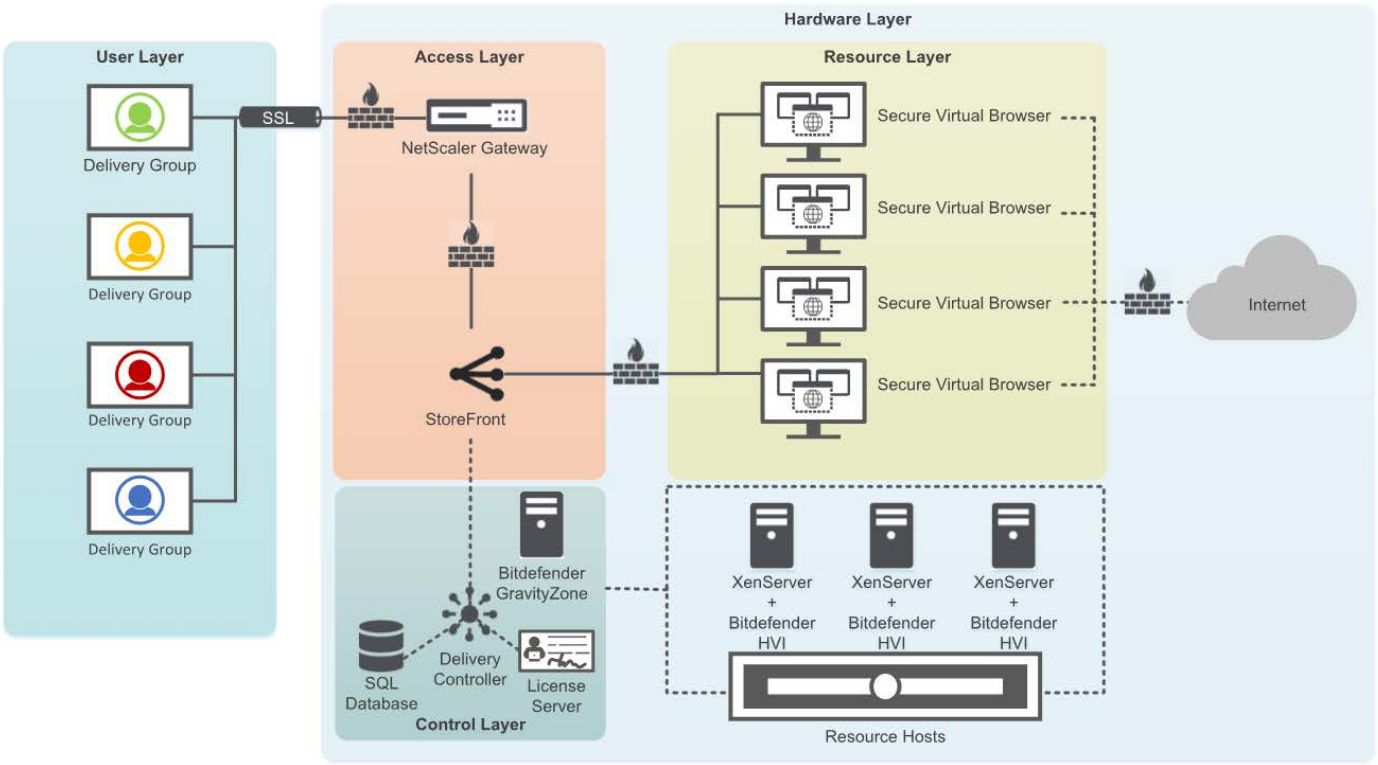


Table of Contents

Introduction

Overview

The stark reality is that browsers have become the primary vector for attacking individuals and organizations. Organizations that configure browsers without considering them as the entry-point for malware, undesired content, phishing attacks and ransomware, continue to suffer damaging breaches and browser-induced mayhem.

Contrast the "lock-down" mentality against the day-to-day reality; being a security-minded operator of datacenters has always been a difficult task. The primary mission statement is, "Make it work, and keep the technology out of the way." From email to accessing the web, from remote use of critical applications to supporting access from any web-enabled device, the pace of technology continuously challenges security. The result is a tug of war between security teams that want to lockdown browsers by removing functionality, but users want more functionality without regard to security

Organizations understand that web browsers, and their associated plug-ins, are a cause of significant security concerns. Managing different browsers across myriad endpoints and keeping plug-ins updated are challenges that cannot be addressed through legacy security approaches.

In this document, we outline the gaps in providing secure browsing, including research into data breach trends. A practical solution for centralizing and securing browsing is detailed, including combining Citrix and Bitdefender technologies in an innovative approach centered on new virtualization and hypervisor introspection technologies.

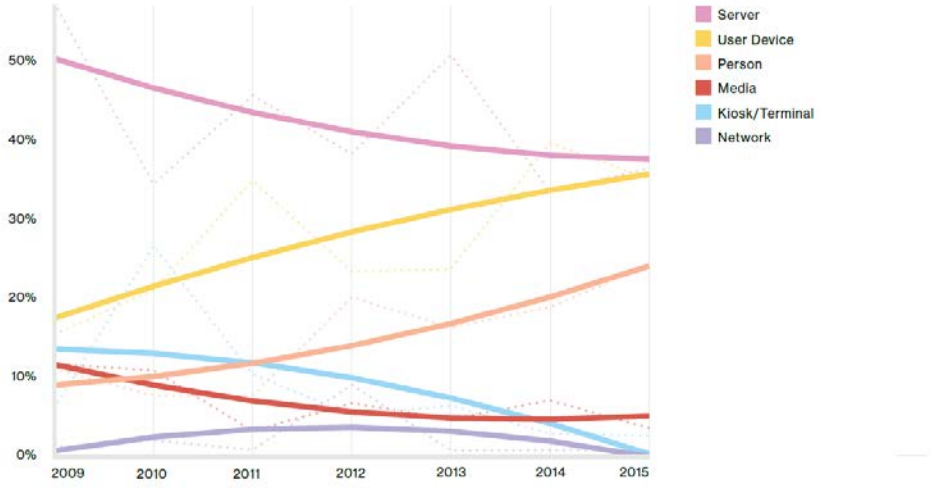
The solution proposed is different from other available solutions, such as hosted secure browsers. First, this solution is deployed on-premises and allows customers to use their existing hardware and licenses. Second, the solution leverages a technology that is unique; watching browser activity from the XenServer hypervisor, included with XenApp and XenDesktop, rather than protection by an agent installed within the operating system running an end-user system.

> "It's like deja-vu all over again."
>
> **Yogi Berra** | Baseball Legend

Data breach trends

The 2016 Verizon Data Breach Investigations Report (DBIR) that opens with the above quote report notes that, as in all nine past yearly reports, 89% of attacks are financially motived and over 80% have an external source. It further notes when looking at breaches by asset category, servers are still number one, while user devices are steadily approaching servers as the leading worst asset (or best, if one is an attacker). User devices work hand-in-glove with the people operating them, so it's a fair conclusion that end-user devices in the hands of users are a growing challenge.

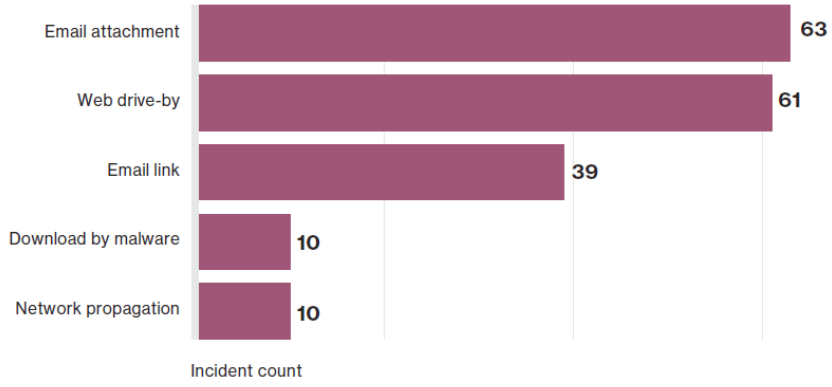
➔ Uneducated users pose risks, they can use Secure Remote Browsing and be more secure



Source: 2016 Verizon Data Breach Investigations Report

Figure 1: Percent of breaches per asset category over time

Focusing on the sources of crimeware, the DBIR provides a figure of the top five sources.



Source: 2016 Verizon Data Breach Investigations Report

Figure 2: The top five sources of crimeware (includes command and control, ransomeware, spyware/keylogger, backdoor, and data export functionalities)

Often, attacks combine phishing with drive-by downloads and include primary and secondary motives. For example, the secondary motive of compromising a web server is to facilitate drive-by downloads, which are in-turn facilitated by a primary phishing attack.

In the end, the DBIR found that malicious software was involved in 90% of cyber-espionage incidents. The first recommendation in the reports is to protect endpoints, and the first point in endpoint protection is to focus on browser and browser plug-in updates.

The overall message is clear, and should not surprise; browsers present a significant attacks surface, and persist as a top source of security incidents and data breaches.

Security Risks

The challenges in browser security are well-known. End-user education is important, yet given the sophistication of web-based attacks – demonstrated by their continued success – we know even sophisticated end-users may click on malicious links. Managing vulnerabilities in browsers and plug-ins is important, but we know – again, because of continued success – that managing browsers across organizations is problematic.

By design, browsers are excellent at parsing myriad inputs. The primary goal of browsers is providing a rich user experience, and browsers do this well. Beyond core browsers, many common plug-ins, such as Flash, Silverlight and others, are demanded by users. The result is diverse end-user systems running one or more browsers with multiple plug-ins spanning innumerable version combinations. This creates headaches for IT security teams everywhere.

Browsers have become a leading gateway for APTs (Advanced Persistent Threats). Attackers seek to compromise organizations by targeting the most vulnerable systems – often, end-user systems. These targets serve as initial footholds from which motivated attackers will diligently mine data to further attacks, and/or use as jump-points to more sensitive systems.

From email delivery to web: Browsers overachieve as a threat gateway

As far back as 2013, threat researchers and security vendors noticed primary malware delivery methods were shifting from email-based to web-based.

> "90% of fully undetected malware was delivered via web-browsing."
>
> Palo Alto, "The Modern Malware Review", March 2013

There are two primary reasons for this shift: the time difference between delivery and execution, and differing end-user experience expectations. From the point in time that a specific exploit is created, there is a race between anti-malware vendors to create and distribute detection routines, and the attacker enticing the victim to execute the exploit, by opening a malicious PDF, for example.

When delivered by email, a malicious attachment may not be opened for minutes, hours, days or longer. This time interval increases the chances of detection. Also, end-users accept delays of minutes in email delivery – indeed, when the email is unsolicited, there is no perception of delay.

These factors provide valuable time to apply in-depth analysis of email attachments, including sandboxing techniques whereby an attachment is detonated in a controlled environment, and its behavior monitored. These factors lead to wider opportunities, based on time, for security tools to update and apply rigorous inspection.

Conversely, web browsing user experience is time-sensitive. Users do not tolerate delays when accessing online content or while consuming a PDF, for instance. Since the exploit is often hosted, the attacker is also able to rapidly modify the exploit to evade detection. Attackers can even go so far as to automate these modifications. By hosting exploits which are to be executed by web browsers, attackers take advantage of the very short time-to-delivery versus time-to-execute interval, and maintain control of the exploit until moments before it is delivered.

Furthering the complexity is the consideration of third-party browser plug-ins. A Recorded Future study encapsulated the problem:

Adobe Flash Player comprised eight of the top 10 vulnerabilities leveraged by exploit kits

https://www.recordedfuture.com/top-vulnerabilities-2015/

Functionality is the goal of web browser designers and developers of browser plug-ins. Security is – at best – a secondary consideration. End-users demand seamless interaction with the wide world of content available through their browsers.

The parse-on-demand user experience demanded of browsers, along with the myriad possible combinations of devices, browsers, and plug-ins, has led to a shift from purely email-based attacks to web-based attacks. While email remains as a component of many attacks, it is most often used to deliver URLs which lead to malicious or compromised web sites.

Whether the attack is delivered by email or hosted on a web site, ultimately the goal is to exploit a vulnerability in an application to gain a foothold on the target system. For the reasons listed above, leveraging vulnerabilities in web browsers and plug-ins is increasingly the favored attack vector.

Diversity complicates browser security

Browser diversity encompasses the myriad of browser platforms, versions, extensions, plug-ins, configurations, and programming frameworks, as well as the operating systems and environments they deeply integrate with.
For most, gone are the days of a standard browser with a standard configuration on an enterprise-managed standard version of Windows. New and highly mobile operating systems, new approaches including Chromebooks and a proliferation of WebKit implementations have further driven browser diversity. In addition, browsers are asked to support an increasingly diverse set of use-cases and often conflicting security requirements.

Use cases include multiple browser types (e.g. Internet Explorer, Edge, Chrome, and Firefox), operating systems (e.g. Windows, MacOS, iOS, Android) and plugins (e.g. Flash support for videos and advertisements). Old versions of browsers are often required for compatibility, with IE7 persisting in many enterprises. In operating systems and frameworks where the browser is integral (e.g. Windows, MacOS, iOS), the browser has deep roots into the operating system and overall privileged system environment. Third-party browsers that don't have the same level of privilege benefit or suffer from the deep lack of system interface – depending on whether vulnerabilities are thwarted or enabled by this privilege arrangement. While they may look like they provide identical functionality, deep down, competing browsers are not the same.

Different combinations of extensions and plugins, and versions thereof, are required for application compatibility, which makes each device unique and hard to secure. Disabling JavaScript breaks many sites and apps, but may be desired to reduce the attack surface. Disabling Flash is highly recommended for increasing security. To add to the maelstrom, end-users often take advantage of open-ended policies to install questionable extensions.

As we can see from the diversity requirements, asking one browser configuration to support all use cases and security requirements is a losing battle that suffers user experience, support and security. We must support browser diversity through publishing individual browser instances with configurations that are specific to purpose. Fortunately, this is simple to configure and maintain using application virtualization to publish applications and use case-specific browsers.

Current approaches of securing browsers

Discussions of browser security within enterprises usually lead to the following legacy conclusion: *A standardized browser with all recommended patches, configurations and required plugins is the easiest to support and maintain for security purposes.*

The problem with the conclusion is that it is not a solution. A single browser configuration that is over-configured either leads to a poor user experience, via restrictive policies, or excessive risk via open-ended policies.

The browser at the endpoint must be a bastion of security to protect the user, endpoint, enterprise and sensitive data. But at the same time, reality demands that this "bastion of security" approach be flexible enough to support the competing demands of user experience and security control. Another approach is to provide employees with internet access through kiosks that are available on-premises. While this solution can provide a very high level of security, it is also associated with a very bad user experience that can have direct impact on the productivity of employees.

Most of the existing solutions are relying on a decentralized, architecture, where each device running inside of a datacenter needs to be properly secured. By trying to lock down all these endpoints, the IT department is directly interfering with end users' productivity and dictates how business should operate. Another challenge related to the decentralized architecture is relying on each of the endpoints to properly detect and report any malicious activity.

In-guest security tools efficacy

As part of a defense-in-depth strategy, organizations often employ several types of in-guest security controls to minimize risk. Several layers of in-guest security controls (and their network counterparts) are common in the enterprise space, including antivirus/antimalware solutions, host-based intrusion detection systems, firewall, application control modules, device control modules and others.

In-guest security controls installed within an operating system often leverage user-mode agents and a kernel-mode components (drivers). The integrity of the security control is ostensibly provided by various self-protection mechanisms which rely on operating system APIs.

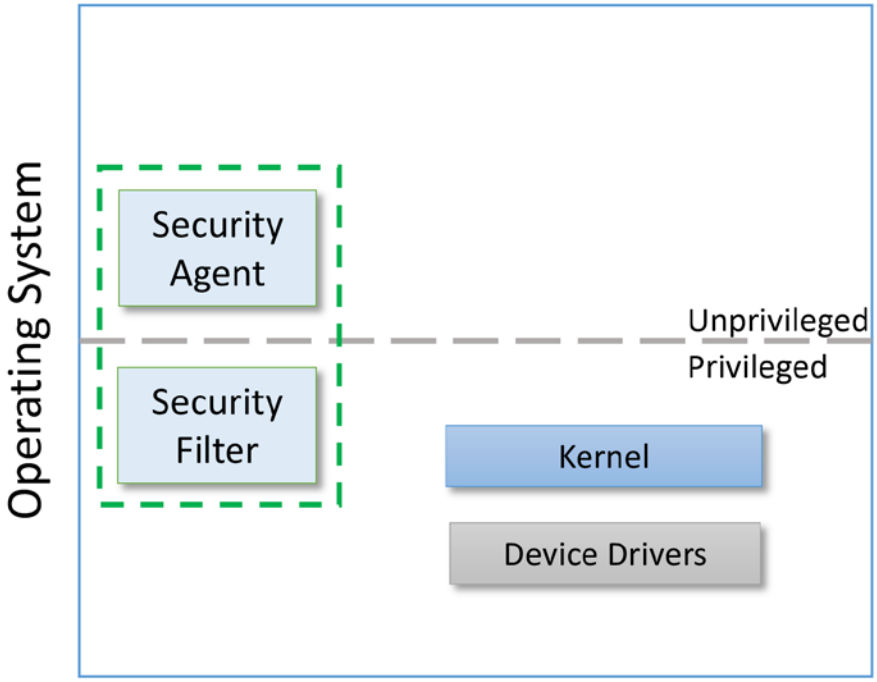


Figure 3: Security Agent Basic OS Components

Unfortunately, all in-guest security controls have a common weakness: the operating system APIs. Advanced attacks often employ elaborate evasion techniques to circumvent security controls while executing in memory. Commonly employed evasion techniques include multi-staged payloads, code obfuscation through packers and payload encryption.

When a threat is able to run in the system memory, the attack is continued with various exploits used to escalate privileges to system- or root-level privilege by abusing local vulnerabilities or misconfigurations. If the attacker achieves the ability to execute code in ring-0, in-guest security tools are at the mercy of the attacker.

As a consequence, agent-based security tools cannot guarantee detection of malicious activity, or the integrity of the system they are tasked with protecting. For example, advanced, targeted attacks may use sophisticated rootkits to defeat detection while masking command and control activity.

Security tools can also contain vulnerabilities. Security software components often run with ring-0 privileges. A vulnerability exploited in a security solution or one of its components represents a potential attack vector that with a path to full system compromise. Over the past years, several cases have been publicly reported.

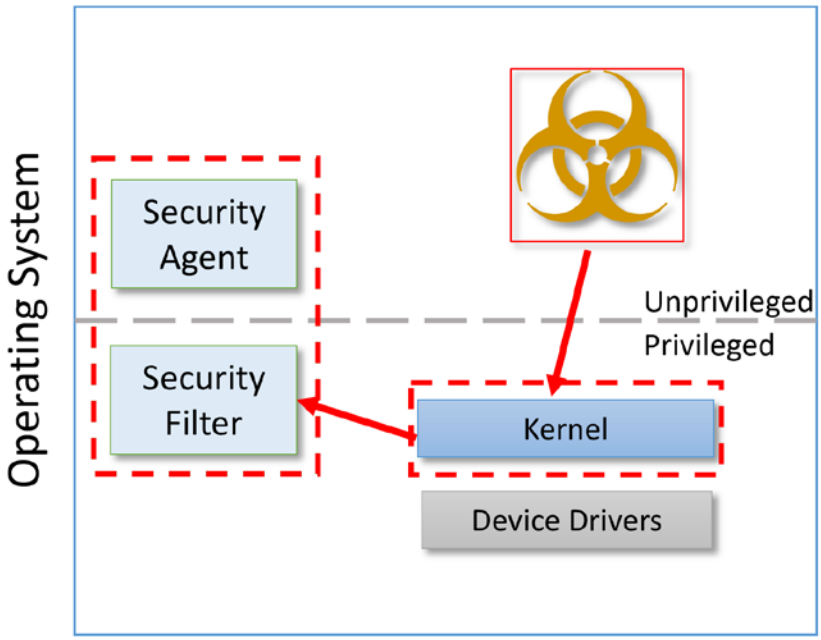


Figure 4: Security Agent Compromised by an Attack

Virtualization introduced a layer of privilege that is higher than what is available within protected endpoints. The hypervisor runs below one or more guest operating system instances, essentially as ring-minus-one. The following sections describe how this new level of privilege is leveraged to obtain stronger security controls and increased visibility.

Components of Secure Browser

Introduction to Secure Browsing

Citrix XenApp together with Citrix XenServer with Direct Inspect APIs, and Bitdefender Hypervisor Introspection (HVI) provide a method of enhancing security without sacrificing the end-user experience. The Secure Browser solution is, in concept, fairly straightforward:

- Centralize browser functionality in a XenApp site
- Run the XenApp servers on XenServer, which is secured using HVI
- Leverage HVI to provide security at the XenServer infrastructure level

There are three primary components of the Secure Browser solution. The first is XenApp, which centralizes the browser application execution on one or more host. The second is Bitdefender Hypervisor Introspection (HVI), which leverages the third component – Citrix Direct Inspect APIs in XenServer.

The novelty of the solution lies in the Bitdefender HVI technology, protecting the XenApp hosted browser. With HVI, organizations gain insight into the security posture of the hosted browser.

When designing this solution, Citrix and Bitdefender set the following goals:

- Minimize the ability of attackers to leverage web browsers as an attack vector by isolating the browser as a published application and applying security at the server publishing the browser
- Allow end-users to access Secure Browser without requiring an agent at the end-user system
- Run each end-user browser as a session for security and include configurable persistence for end-user experience
- Flexibility of applying the solution selectively—Internet versus Intranet, whitelisted URLs versus untrusted, etc.
- Take advantage of centralizing published browser by applying security layers and controls which are not available or practical at end-user systems

Citrix XenApp

XenApp is an industry leading solution for application and desktop delivery. XenApp allows you to take an application from a local machine, install it on another machine in the datacenter, and access it remotely. From the end user perspective, the experience is indistinguishable from locally installed applications, and can be configured to access the local resources, such as printers or disk drives. Access is seamless with icons that are integrated with each endpoint start menu or desktop.

Yet, applications accessed via XenApp are not actually running on the local system. The application user interface is presented on the endpoint and dynamically updated, while keyboard presses and mouse clicks are transferred to the remote session. This approach is also called application remoting or presentation virtualization.

A side benefit of XenApp to users is that the application can also be accessed from various non-Windows devices.

From a security perspective, this approach has several benefits.

- **Secure Remote Access** – You can provide simple, secure access to apps and desktops from anywhere. Instead of extending your network using SSL VPN solution for remote access, only screenshots are transmitted.
- **Data Centralization –** 1 in 10 laptops are lost or stolen. Data accessed by the application is safely stored in a datacenter and is never transferred to the endpoint. Even if an endpoint is stolen, the data is safe.
- **Access Control** – The system that hosts the application can have completely different access permissions than the endpoint that is accessing it. This allows XenApp to be used as a highly-secured bridge between two networks with a different trust levels. Instead of trying to secure every single device, you can focus your security solutions on a few access locations.

Access control allows you to separate two networks with different trust levels. Historically, this meant delimiting an external network from a local network. Today, organizations must realize the internal network must also be segmented. XenApp is often

used to separate end-users from the backend data, which is achievable with even legacy client-server applications. If users can gain access to data only through XenApp servers, rather than directly accessing systems which contain sensitive date, security measures can be concentrated on the XenApp access points (recording all sessions, implementing restrictive policies, etc.). XenApp acts as a point of managed control between trusted and untrusted network segments.

In a typical configuration, the XenApp site is hosted in a trusted environment, while the endpoints are untrusted.

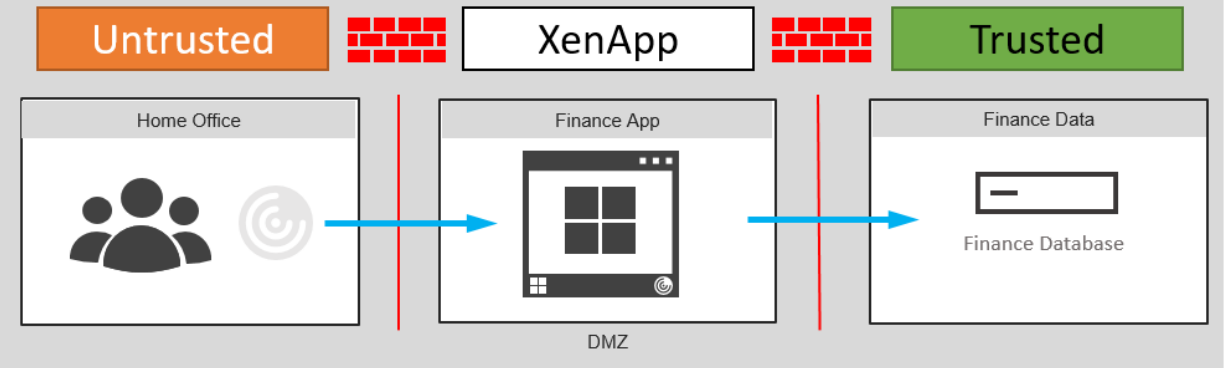


Figure 5: XenApp site hosted in a trusted zone, while endpoints are untrusted

There are however some scenarios where this trust relationship is reversed – XenApp servers are accessing untrusted data, while endpoints are hosted in a trusted network segment. While this scenario is less common, there is one use case that is a perfect match for it – isolating the browsing traffic. In this case, XenApp (hosted in DMZ without any access to the sensitive company data) is hosting browsers for the internet access and endpoints doesn't have any internet access.

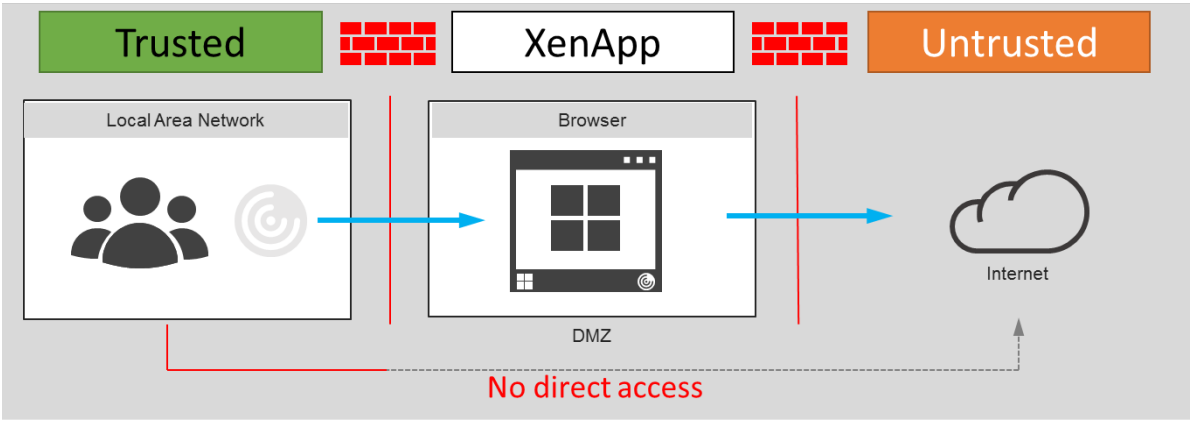


Figure 6: XenApp servers access untrusted data, endpoints are in a trusted zone

Citrix XenServer with Direct Inspect APIs

XenServer is part of the Citrix tool-stack which is used to orchestrate virtualized servers, desktops, and applications on the XenServer hypervisor. The XenServer hypervisor is based on the open-source Xen hypervisor. In the context of this whitepaper, XenServer is used to denote the Citrix version of the Xen hypervisor. Note that XenServer is included with all XenApp and XenDesktop editions.

XenServer includes a new security feature unique to the server and desktop virtualization market, called Direct Inspect APIs, which enables third party security companies to leverage memory introspection techniques from a hypervisor-layer security appliance.

Solutions, such as Bitdefender HVI (Hypervisor Introspection) integrate with these XenServer APIs working with raw memory, and without any in-guest (VM) agents. Zero-day protection through memory introspection comes from outside of the VM, enabling the

solution to even detect sophisticated unknown threats, such as APTs (Advanced Persistent Threats), intercepting and blocking them from tampering with the memory stack and injecting remediation tools if necessary.

Since an integrated solution has access to raw memory, it can be used to protect both kernel-mode and user-mode memory. However, the memory access is truly raw; it is up to the solution provider to make sense of what is provided, and apply protection.

The Direct Inspect APIs ecosystem is an open ecosystem and Bitdefender is the first company to leverage this capability.

Bitdefender Hypervisor Introspection

Hypervisor Introspection (HVI), by its very nature, operates at a level of privilege that is higher than that available in-guest. While a rootkit running in a virtual machine may run with kernel-level (ring-0) privilege, as does in-guest security software, HVI performs at the hypervisor level of privilege.

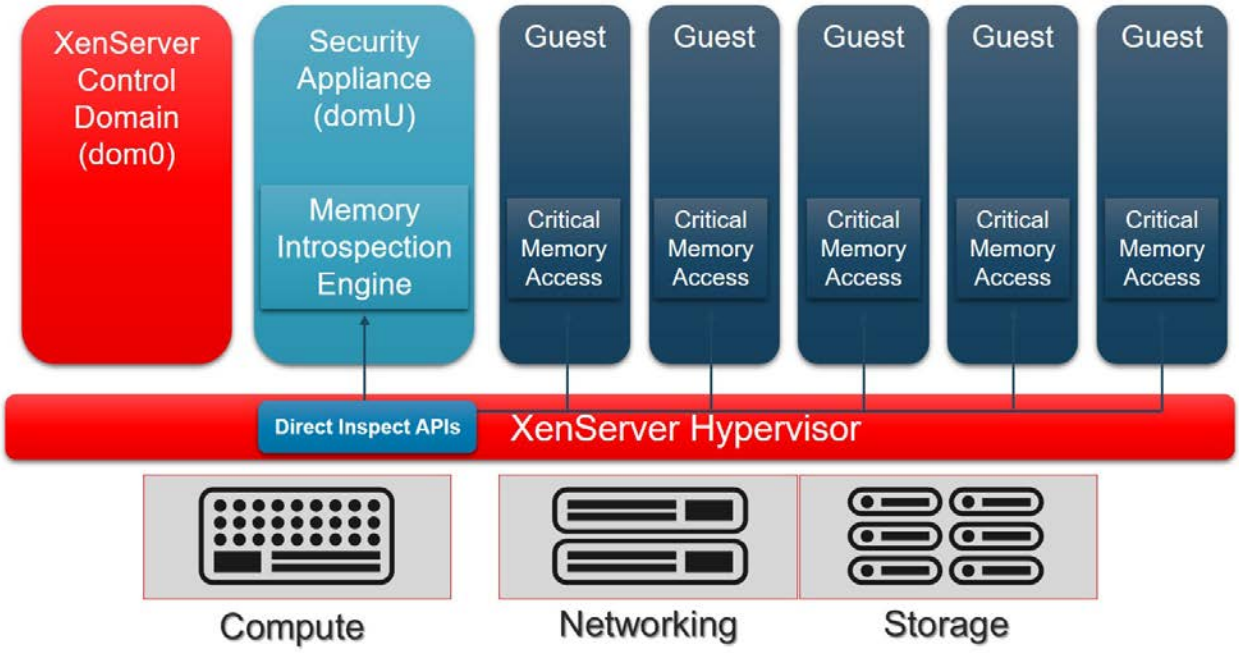


Figure 7: Simplified architecture of Hypervisor Introspection and Direct Inspect APIs

Bitdefender HVI leverages the XenServer Direct Inspect APIs. The Introspection Engine applies security rules to virtual machine memory while remaining isolated from the protected virtual machines.

Whether the protected endpoint is Windows or Linux, server or desktop, HVI provides insight at a level that is impossible to achieve within guests. Effectively, it is inspection from below the guest operating systems; ring-minus-one insight and control.

Just as the hypervisor controls hardware access on behalf of each guest virtual machine, HVI has intimate knowledge of both user-mode and kernel-mode in-guest memory. The result is HVI has complete insight into guest memory, and therefore full context. At the same time, HVI is isolated from the protected guests, just as the hypervisor itself is isolated.

Memory introspection from the hypervisor resolves the traditional isolation versus context trade-off. The hypervisor is isolated from the workloads running within virtual machines, at the hardware level.

The kernel of an operating system – the supervisor – used to be the ultimate arbiter between applications and hardware access. In virtualized environments, the hypervisor acts between the operating system kernel-mode operations and the underlying hardware. The hypervisor abstracts hardware and presents it to guest operating systems. The hypervisor acts as a gatekeeper

between guest virtual machines memory activity and physical memory, and is isolated at the CPU execution level by the design of contemporary processors.

HVI is not intended to replace in-guest security tools, such as anti-malware agents which, in part, provide file-system scanning. However, HVI can also be used to maintain the integrity of in-guest security tools. For example, in virtualized environments, file system scanning is offloaded from in-guest components to a virtual appliance. While this improves performance, it does not enhance security. HVI, for the reasons noted above, greatly enhances visibility of memory activity without an in-guest component, while also protecting in-guest components used to offload file system scanning.

The HVI technology is integrated in and managed by GravityZone, the Bitdefender endpoint protection platform.

Combining the Components to form a Solution

Secure Browser delivers benefits to both security practitioners and system administrators, enabling enterprise organizations to narrow the gap between security and operational requirements.

XenApp transforms locally managed web browsers into a centrally-managed service. Security departments can enforce configuration best-practices and tight version- and access-controls to user-groups. For example, legacy applications with specific browser requirements are delivered, according to group-based policy, to the end-users who need it, without requiring legacy browsers on end-user systems.

XenServer Direct Inspect APIs and Bitdefender HVI secure the delivery platform for the published web browser. Browser services are tightly secured, activity is monitored in memory, and security administrators receive real-time incident reports and notifications.

Secure Browser is deployed as a stand-alone solution, self-contained and leverages different integration points with the enterprise management tools.

With this approach, attacks are prevented in the early stage, before the initial breach occurs.

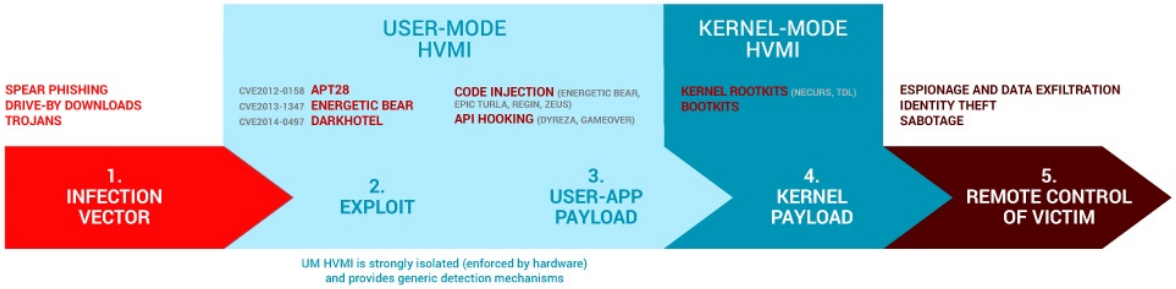


Figure 8: Generic attack process overview showing where Hypervisor Introspection acts.

Architecture of Secure Browser

The web browser is one of the weakest links in the enterprise security chain, therefore securing it is an obvious goal. This section describes the architecture of a solution for this problem. While various hardening methods and guidelines are available to improve the security of the web browser, commonly available security solutions lack a focused, practical, and scalable response to the challenge.

Solution Implementation

With the Secure Browser solution, Citrix and Bitdefender aim to provide a better response to the problem of browser security. XenApp is great at application remoting, including web browsers of any kind, hosted on Windows or Linux platforms. XenServer is used to host the farm of machines that can be quickly provisioned/de-provisioned and allows a flexible single-image management. Bitdefender HVI secures any application and the in-guest operating system, including Windows and Linux, running on XenServer.

By combining these three products, an enterprise organization takes advantage of the Secured Virtual Browser solution which allows user to browse the Internet in a free and uninterrupted fashion while the security burden is offloaded from the local end-user browser to a remotely published browser. With this simple deployment model, the user experience remains unchanged.

The following diagram represents a Secure Browser reference architecture

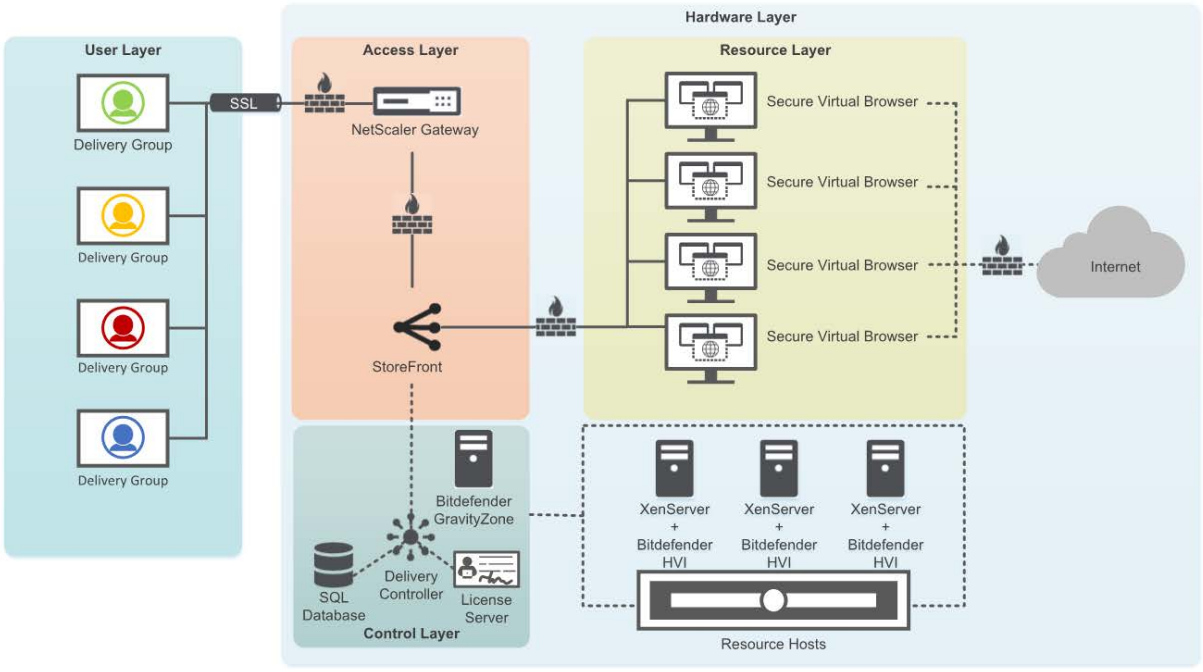


Figure 9: Secure Browser Reference Architecture

Secure Browser provides a safe method for web browsing:

- End users in an internal network access a XenApp published browser from their local systems by leveraging Citrix Receiver which connects to a Citrix NetScaler instance. For enhanced user experience, the published browser can be registered as a local default browser.
- The web browser application is published using several XenApp servers to accommodate scalability and versioning needs. The XenApp servers are non-persistent, a simple VM reboot or user log-off is enough to ensure a clean slate.

- On the infrastructure side, the XenApp servers are hosted on XenServer, and thereby protected by Bitdefender HVI. HVI constantly monitors the browser activity in memory and flags attacks or exploitation attempts in real-time.

Secure Browser is as flexible as XenApp, and can therefore be deployed as best suits the requirements of any organization.

Deployment Scenarios

The deployment architecture described in the previous chapter represents a typical enterprise implementation with all components hosted locally. With **fully on-premises** deployment, you are maintaining both control layer (infrastructure) and resource layer (application servers). A fully on-premises deployment scenario is the most common and well documented. Other possible deployment scenarios can utilize the cloud to minimize the number of components that are running in the datacenter. These various scenarios are listed in the order of likelihood – while these new deployment scenarios are still very new, they are gaining momentum and becoming more popular.

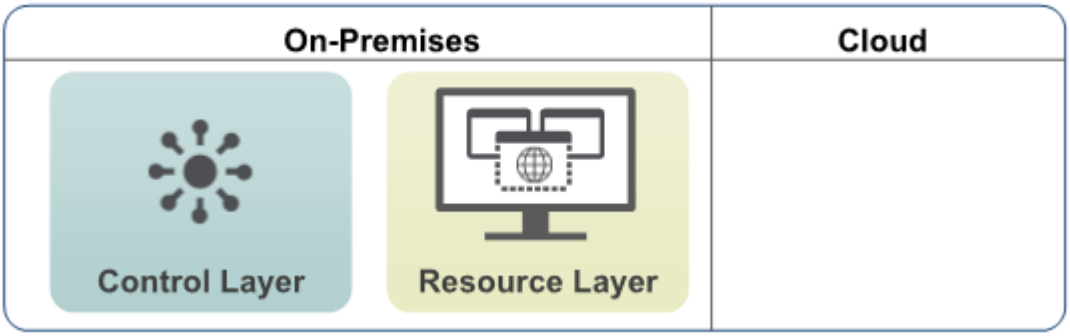


Figure 10: Fully on-premises scenario

Fully on-premises solutions require additional components – you need to manage not only physical servers, but also hypervisor, delivery controllers, SQL servers and license server. Many customers are looking for an enterprise-ready managed offering that would provide the security benefits of Citrix solution, while minimizing the complexity of deployment. Minimizing the complexity is one of the important security principles, but if not properly executed can often result in a solution that does not provide the required enterprise-grade availability. Finding the right balance can be a challenging task. Citrix is offering this service under the name Citrix Cloud. As shown in the following examples, Citrix Cloud is a flexible deployment model with different deployment scenarios.

One Citrix Cloud deployment option is to run local application servers with the management layer in the cloud. This way, you only manage the components where you need to maintain control, such as the servers hosting published browsers and security services offered by the Bitdefender HVI integration in XenServer. The broker and other control components are deployed and managed in the Citrix Cloud, which improves the security of your deployment.

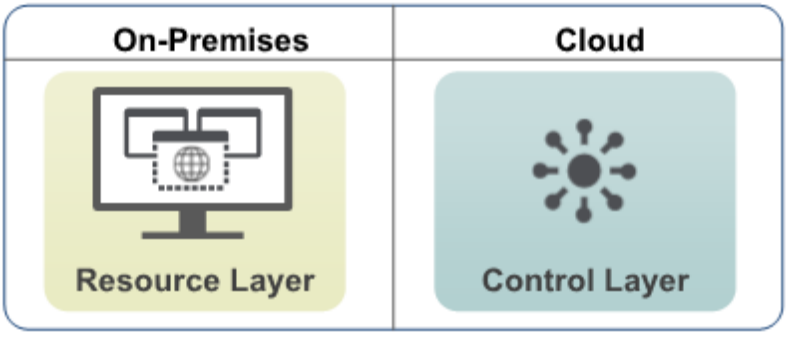


Figure 11: Local browsers with Citrix Cloud management

Another option is to completely move all the applications servers to an Infrastructure as-a-Service (IaaS) provider, such as Amazon Web Services or Microsoft Azure. This security deployment is useful when you would like to analyze potentially dangerous links, expand shortened URL links for compliance, or completely remove the browsing traffic from your datacenter. In this configuration, all application servers as well as control layer components run in the cloud. It is also possible to run the control layer on-premises, with all application servers running in the cloud, but that is not common. In either case, the published browser is isolated from the datacenter network, providing a secure environment to consume Internet content.

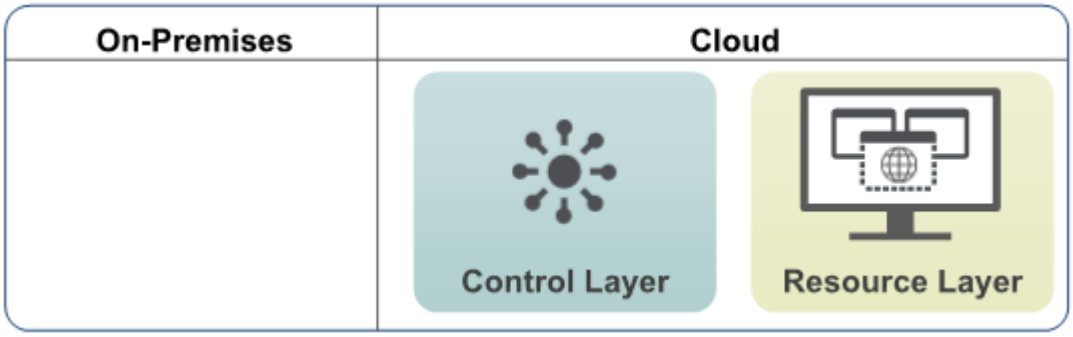


Figure 12: Browsers in cloud with Citrix Cloud management

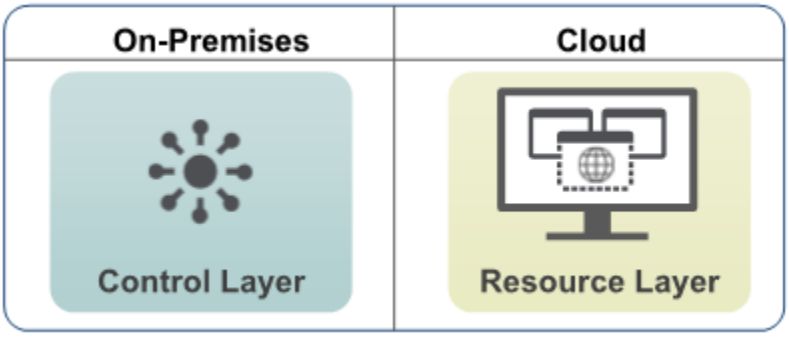


Figure 13: Browsers in cloud with local management

Finally, you may want to deploy some application servers running locally, while other application servers are running in the cloud. One example where such scenario is useful is for social media teams to use cloud-delivered browsers to access certain social media networks that are prohibited from the internal network. For other internal applications, resources are delivered from the on-premises servers. As another example, consider security teams that require access to highly-secured browser instances running in the cloud. In such cases, it is a common practice to host multiple separate environments to provide access to intranet and internet applications using completely separated networks.

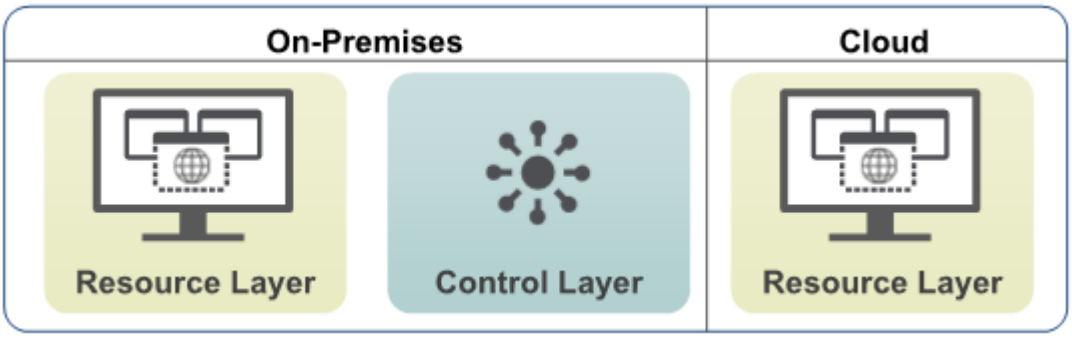


Figure 14: Flexible deployment with local management

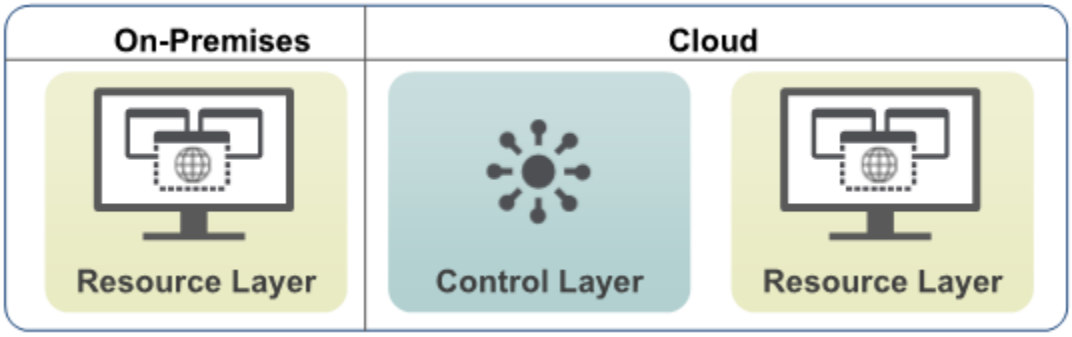


Figure 15: Flexible deployment with Citrix Cloud management

For more information about Citrix Cloud, visit www.citrix.com/cloud.

End User Experience

Over the past decade, web-based applications have become central to the daily end-user routine because the applications provide flexible, scalable and agile end-user experience in terms of accessibility, availability and usability.

Any new security layer stacked on top of existing web-based application workflows should not alter the user experience and should preserve the characteristics that contributed to the success of the application experience.

Secure Browser, through the design of its software components, respects the essential requirements:

- **Accessibility.** XenApp is designed to provide end-users access to published applications in a very simple and elegant fashion. Citrix Receiver provides access to the published XenApp applications. The administrator can leverage Receiver, either installed locally, or using the HTML 5 version, and customize end user accounts to use a published browser as the default browser.
- **Availability.** Both dedicated and non-persistent workloads can be employed. Non-persistent workloads provide a predictable system state upon reboot since any changes made when running are, by definition, not maintained.
- **Usability.** Bitdefender HVI is an infrastructure service which protects XenApp servers. While HVI protects the end-user's browser, it does so by monitoring the XenApp server, and does not require a footprint within end-user systems.

In a practical example, we're considering an on-premises deployment scenario in which the system administrator configures Secure Browser to provide a published default browser for end-users by customizing the local file type associations enforced using Group Policies, and direct Internet access from the local systems is restricted. In this scenario, Secure Browser becomes the default local browser. The workflow of this scenario is:

- An end user receives a URL via email, IM or any other communication channel.
- The end user expects to retrieve the contents of the URL in a web browser by simply clicking on the URL.
- When the user clicks on the URL, the URL is not opened using a local browser; instead, it is opened in the web browser published by XenApp and secured by HVI.

In a different configuration, the local browser remains as default browser on the system and end-users use it to access Intranet resources. Using system configurations, group policies and network controls, the administrator blocks Internet access from the local browser, allowing access to only intranet resources. External web access is allowed only through Secure Browser. In this scenario, the end-users are complying with the corporate security policy by necessity and the system administrators gain insight into potential threats that target their users without workload disruption.

While this document focuses on specific scenarios for brevity, it should be noted Secure Browser can be configured to address myriad requirements. For example, a local browser can be used for all Internet and most intranet activity, while a specific version of IE with a particular plug-in is published using Secure Browser to tightly control how a sensitive legacy web application is accessed. Or, a local browser can be used for whitelisted URLs, while Secure Browser is used for every URL not whitelisted.

The flexibility of Secure Browser allows administrators to decide if they want to apply the solution to only a narrowly defined set of users or machines, or more broadly, using Secure Browser for all browsing activity after a staged deployment.

Let's consider the security implications and benefits of Secure Browser in contrast with using a local browser:

An attacker has targeted the enterprise organization and is looking to leverage a client-side attack based on a zero-day threat which exploits a vulnerability in a browser plug-in.

Action	*Result (Local Browser)*	*Result (Secure Browser)*
End-user receives an infected URL via email and clicks on the URL	The infected URL is opened in the local browser.	The infected URL is opened in the published browser hosted by XenApp and protected by HVI
The web browser is loading the URL.	The infected payload in executed by the local browser and the attacker is able to exploit the local vulnerability to execute code.	The infected payload is executed in the hosted browser and HVI identifies the exploitation attempt before the malicious code runs in memory.
After the URL is loaded	The attacker may have remote control of the system.	The security administrator receives an incident report from HVI.

Note: A real-life scenario equivalent is represented by the Adobe Flash Player use after free vulnerability published under CVE-2015-5122 which has been successfully exploited on Mozilla Firefox and Internet Explorer running on Windows XP, Vista, 7 and 8.1.

Security industry researchers have reported this vulnerability that has been employed in advanced attacks targeting Japanese organizations.

Conclusions

Secure Browser gives organizations the ability to mitigate one of the greatest sources of risk in their environments – web browsers and associated plug-ins which execute within end-user systems. XenApp is used to deliver a remote browser which executes on the XenApp server, isolating this execution from the end-user system. This provides several benefits:

- Version control of browsers and plug-ins
- Delivery to the end-user while maintaining user experience

Since the solution runs on XenServer, the unique capabilities of the Direct Inspect APIs can be leveraged by Bitdefender HVI (Hypervisor Introspection). This layer of security is available with only XenServer, and currently leveraged by only Bitdefender.

Unlike traditional endpoint security, HVI looks for malicious activity in kernel and user-mode memory of systems running on XenServer. The advantages of HVI include:

- No footprint within protected systems (true agentless)
- Inspection of raw memory, at the hypervisor layer
- Detection of common attack techniques at the earliest stages of an attack

Together, these Citrix and Bitdefender technologies form Secure Browser – a revolutionary solution for securing web activity of end-users.

This paper outlined scenarios which are applicable to the most common circumstances. Other scenarios, which may leverage Secure Browser as a whole, or concentrate on isolating, securing, and delivering other applications following the same model, include:

- Management of arbitrary links delivered via email, social media, or other vectors
- Enforced browser process and security level segmentation
- Administrative console governance with virtual jumpboxes/bastion sessions
- Browser, or other application, forensics, testing, and patch validation

For more information

If your organization is interested in exploring Secure Browser further, below are some resources to help you get started.

Find-out more about HVI, and get a trial at www.bitdefender.com/business/hypervisor-introspection.html

Find out more about XenApp and XenServer at www.citrix.com/xenapp and www.citrix.com/xenserver

Appendix – Implementation Best practices

Choosing the right type of VDI

It is important to choose the right type of VDI to host your desktops. One of the important design decisions is the operating system that is used. When deciding for the operating system, you should consider the opportunity for security lock down and ability to reduce the attack surface – server operating systems are usually providing a smaller attack surface than desktop operating systems.

Another important design decision is whether you are planning to host multiple sessions on the same server (multi-session) or provide each user with their own machine (single-session). This design decision is based on a combination of factors – risk tolerance, licensing cost or scalability of solution. From a security perspective, single-session VDI sessions are preferred.

A final design decision is the persistency of the machine itself and single image management. From a security perspective, it is advisable to automatically reset the machine to the default stage after each session (VDI desktop provisioned by MCS or PVS). This is however possible only with a single-session machines.

Even if you've deployed multi-session hosts, single-image management with the ability to revert the changes to the machines is a strongly recommended approach. In this scenario, machines should be rebooted on a regular basis to wipe out all changes.

Seamless integration with Start Menu

If the secured solution does not provide the end users with a great user experience, end users will actively search for ways to bypass the implemented security measures. An example of poor user experience is requiring users to perform multiple steps before they can perform a quick internet search. It is therefore important to focus not only on the security, but also usability aspects.

Reducing the number of clicks to launch published applications is one of the important measures to improve user satisfaction. Citrix Receiver can integrate subscribed published application icons directly into the Start Menu. Combine this with Single Sign-on and you can provide a seamless user experience.

Administrators can auto-subscribe icons by specifying the Auto or Mandatory keywords in the published application description. Or subscriptions can be disabled for the store causing all published icons to be integrated into the Start Menu.

For more information, see the following Citrix documentation:

- Configuring application delivery
- Configure domain pass-through authentication

Reduce application launch time

Another very important user adoption metric is the time required before the browser is ready to use. Some users keep the browser running the whole day, while others will keep closing and opening it throughout the day. If a Citrix session is not already established, the first launch can be considerably slower than use of a locally installed browser. Also, after closing the browser, the session is automatically logged off and needs to be re-established the next time user launches the browser.

Citrix XenApp and XenDesktop have two features that can greatly reduce time required to launch an application. The session prelaunch and session linger features help specified users access applications quickly, by starting sessions before they are requested (session prelaunch) and keeping application sessions active after a user closes all applications (session linger).

For more information, see the following Citrix documentation:

- Configure session prelaunch and session linger
- Reduce application launch time

Recommended Citrix policies

Implementing the right Citrix Policies can have a great impact on the usability of solution. As a general rule, start with the built-in policy template called "**Security and Control**", which disables all forms of potential data transfer between the Citrix server and the Citrix endpoint.

As every environment is different, feel free to adjust the settings, especially the ones that can have a direct impact on the usability of environment:

- Ability to use client/network printers
- Ability to transfer files between endpoint and browser
- Ability to use copy & paste functionality

Another important consideration is that endpoints are more trusted than XenApp servers that are hosting browsers. As such, it is important to consider if offloading processing to the endpoint (for example Windows Media Redirection or Flash Redirection) is desired, as attacker might use these transport channels to deliver potentially hostile content to the endpoint.

Citrix SmartAccess/SmartControl functionality can dynamically adjust the policy settings based on endpoint configuration and/or endpoint location. For example, detect if the endpoint has a valid machine certificate – if a machine certificate is present, and an endpoint machine is a member of the domain, use less restrictive policies. If a machine is not domain-joined, and doesn't have a machine certificate, reject the connection, or apply more restrictive policies.

Providing seamless user experience

When properly designed and implemented, it's almost impossible to distinguish between an application installed locally, and an application hosted on the XenApp environment. Here are few recommendations on how to make sure that you provide the best user experience:

- Hide system drives that should not be accessible (e.g. the Virtual Delivery Agent's C: drive). If Client Drive Redirection is enabled (the default) from the hosted application, only client drives should be visible to the user.
- Delete all VDA printers (XPS/PDF) that are not required. If Client Printer Mapping is enabled, from the hosted application, only client printers should be visible to the user.
- Special Folder Redirection replaces the VDA's special folders (Documents, Desktop) with the endpoint's special folders. In the hosted application, if the user goes to File -> Open, the user will see the same documents in the remote session as are available on the local endpoint. Documents are saved to the endpoint machine. Special Folder Redirection requires Client Drive Mapping to be enabled.
- The appearance of the windows in the hosted application are based on the operating system of the VDA. The appearance of windows from a Windows Server 2016 VDA is identical to a Windows 10 endpoint. Group Policy can also adjust the VDA theme to match the endpoint's theme.

As a final check, you should compare commonly accessed dialogs (Save As and Print) on local application and hosted applications and see similar results.

Select the right profile solution

Choosing the right profile strategy should be aligned with the security approach that you are planning to take. For example, if you're planning to minimize the ability of users to modify their workspace environment, Mandatory Profiles would be recommended. If you're planning to allow your users to customize their browser experience (e.g. allow installation of extensions or sign-in to profile), roaming profile type would be recommended.

The same design decision applies to the location where you're planning to store the downloaded files (if any). You can either user mandatory profiles without any option to save files, use Folder Redirection as a central storage or use Special Folder Redirection to transfer all files to the endpoint.

It is important to make sure that users can access the internet as quickly as possible after clicking on the browser icon. Settings in the user's roaming profile do not have to be re-initialized after logon. Data in the user's roaming profile does not have to be synchronized after logon.

General security hardening

Multiple users can be connected simultaneously to a single XenApp server. One of those users could make a change that affects other users on the same system. Therefore it is important to properly secure all XenApp servers that are hosting browsers. Follow the recommendations from Citrix and Microsoft for operating system hardening and provide only minimum privileges to the users that are accessing the hosted browsers.

For more information, see the following Citrix documentation:

- Security documentation
- Security Resources Library

File Type Associations

For a smooth end user experience, the administrator should reconfigure the endpoint file type associations to register the Secure Browser solution as the default end user browser.

Configure the following registry settings to create the Secure Browser file type:

- System registry settings:

```
[HKEY_CLASSES_ROOT\SecureVirtualBrowser]

[HKEY_CLASSES_ROOT\SecureVirtualBrowser\shell]

[HKEY_CLASSES_ROOT\SecureVirtualBrowser\shell\open]

[HKEY_CLASSES_ROOT\SecureVirtualBrowser\shell\open\command]
@="\"C:\\Program Files\\Citrix\\ICA
Client\\SelfServicePlugin\\SelfService.exe\" -launch -reg
\"Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\storeservi-
ee876895@@XA-BrowserR.Mozilla Firefox\" %1"
```

In your environment, the bolded part of the above configuration should be obtained from a test system to which you have published the browser application. The string is easily obtainable from the Start Menu published application shortcut properties.

If you installed the 32-bit version of the Citrix Receiver on a 64-bit operating system, the registry path should contain "Program Files (x86)" instead of "Program Files."

Then configure the following registry settings to set the URL association with the Secure Browser file type:

- User configuration registry settings:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\Use
rChoice]
"Progid"="SecureVirtualBrowser"

[HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\https]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\https\Us
erChoice]
"Progid"="SecureVirtualBrowser"
```

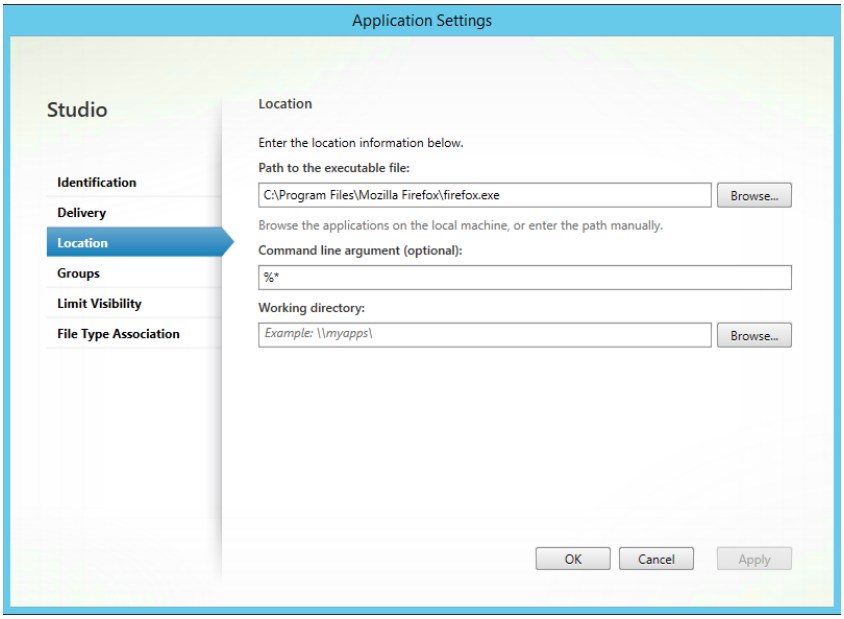
The file type associations can be configured using Active Directory Group Policies targeting the OUs containing the user desktops and user accounts.

Passing Arguments to Secure Browser

When the File Type Associations are in place, the XenApp published application needs to be configured to accept command line parameters upon launch. This way, when the end user clicks on a URL, the published Secure Browser is launched and the URL is passed as a parameter.

To configure this, follow the next steps:

- Open **Citrix Studio**
- Under **Applications**, select the browser application XenApp is publishing and click **Properties**
- In the **Application Settings** menu select **Location**
- Under **Command Line Argument** enter **%***
- Click OK to save the settings.



Bitdefender Hypervisor Introspection Configurations

The Bitdefender HVI technology is deployed to protect and monitor the memory activity of the XenApp servers that are publishing the Secure Browser. Regardless of which browser (IE, Chrome, Firefox, Opera etc.) is being published by XenApp, the HVI User Space memory protection guarantees the integrity of the running process. Customers are also advised to enable the Kernel Memory protection for the XenApp servers.

Use GravityZone Control Center (management console) to create security policies that enable the memory introspection for the Kernel Space and User Space memory. The step-by-step configuration process is described in the GravityZone Administrator Guide

In the context of Secure Browser, the administrator activates the HVI protection for all browser related processes, including any browser plugins spawned in different processes. Considering an example, the XenApp servers are publishing Mozilla Firefox as the Secure Browser; Firefox is also running the Adobe Flash Player plugin. The administrator enables the memory introspection protection for the following User Space memory processes:

- firefox.exe
- plugin-container.exe
- flashplayerplugin*.exe

NOTE: Wildcards are used to account for process name changes triggered by product updates (e.g. Flash Player binary name contains the current version number)

When a memory violation is detected in one of the monitored processes, the policy configures HVI to perform one of the following actions for each process:

- Deny – the exploitation attempt is prevented and the process continues to run
- End task – the memory introspection server will kill the subject process
- Report – the memory introspection server raises an incident event, but lets the memory violation execute
- Shut down VM – whenever a memory violation is detected, the VM itself is shut down. This action should be used with caution and only in environments where confidentiality takes precedence.

Authors

Shaun Donaldson, Bitdefender

Andrei Florescu , Bitdefender

Kurt Roemer, Citrix

Martin Zugec, Citrix

Contributors

Eric Beiers, Citrix

Mihai Dontu, Bitdefender

Chris Mayers, Citrix

Christian Reilly, Citrix

Chris Rogers, Citrix Technology Professional

Carl Stahlhood, Citrix Technology Professional

Rares Stefan, Bitdefender

Anton van Pelt, Citrix Technology Professional

About Citrix

Citrix (NASDAQ:CTXS) aims to power a world where people, organizations and things are securely connected and accessible to make the extraordinary possible. Its technology makes the world's apps and data secure and easy to access, empowering people to work anywhere and at any time. Citrix provides a complete and integrated portfolio of Workspace-as-a-Service, application delivery, virtualization, mobility, network delivery and file sharing solutions that enables IT to ensure critical systems are securely available to users via the cloud or on-premises and across any device or platform. With annual revenue in 2015 of $3.28 billion, Citrix solutions are in use by more than 400,000 organizations and over 100 million users globally. Learn more at www.citrix.com.

About Bit Defender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 West Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States