Guidance

Browser Security Guidance: Enterprise Considerations

Published

Contents

1. Protecting against malware
2. Separating enterprise data from Internet content
3. Sensitive data storage
4. Plugins

This section discusses some of the wider considerations an enterprise might wish to resolve when deploying web browsers. The considerations given here are common to several of browsers discussed in this documentation.

1. Protecting against malware

The browser and End User Devices security frameworks note the importance of reducing the risk from malicious software and content based attacks. This is more important to get right as there is a higher chance that the user will access untrusted content which may be malicious. The most effective protections will use the native security features of the underlying platform as well as protecting against specific web threats.

1.1 Anti-virus software

Anti-malware and anti-virus software is available on a number of platforms. It monitors Internet content as well as software running directly on the platform. Threats from the Internet may be traditional malware that attacks the browser and platform, but also may be in the scripts that attack other web services such as online banking or enterprise web-apps.

Organisations can implement this monitoring on their enterprise web gateway, particularly if anti-malware software is not running on their End User Devices. This will only be effective if the web gateway includes an SSL/TLS interception proxy, otherwise the anti-malware software will be unable to detect threats on encrypted sites. Organisations should consider the privacy implications of decrypting all secure sites, as they may contain personal data from staff members accessing online banking or personal email.

1.2 Cloud-based reputational services

Some browsers have built-in security features that aim to protect against phishing websites and malicious downloads. They work by sending information about the page being visited to the cloud, which responds with a warning if the link being accessed is known to be malicious.

These cloud-based reputational services can be highly effective as they are always up to date, and they are usually backed by search engine heuristics. The amount of information sent to a cloud service to decide whether a link is malicious varies depending on which browser is being used. Organisations should consider the trade-off between privacy and security when using these services.

1.3 Sandboxing

A successful attack against a browser is less likely to compromise the rest of the platform if it is contained inside a sandbox. The separation provided by a sandbox helps protect against the theft of sensitive enterprise data and makes it more difficult for malware to keep running after the browser is closed. The level of protection provided depends on the underlying platform integrity and application sandboxing as well as which of the available security features that a browser chooses to implement.

The most effective sandbox is one that is implemented for the entire browser including its plugins. This approach ensures that the system has protections for all types of potentially untrusted code. Some browsers do not automatically sandbox all plugins, or allow data to be automatically passed to other applications that do not run inside a sandbox. Organisations should consider the increased exposure to malware when enabling plugins that do not run inside a sandbox, and consider restricting them so that they can only be used by trusted Intranet web-apps.

Some platforms that include sandboxing technologies treat some browsers differently to other applications installed on the device. This can mean that the browser sandbox is weaker and potentially easier to attack than would otherwise be expected on that platform. Organisations should consider the strength of the sandbox in use, particularly when considering which other anti-malware technologies to deploy.

1.4 Updates

Browser vendors regularly release updates to add features and fix security issues. As the attack surface of browsers is very large, and the chances of encountering malicious code is high, these security updates must be installed regularly and quickly following their release.

Some browsers may only offer security patches when installing the latest version of the browser. Browser updates may remove web standards that are no longer in common use on the Internet but may be relied on in the enterprise. Some vendors release an early preview, or beta, of their browsers to allow for compatibility testing. This allows organisations to resolve any compatibility issues before patches (that also fix security issues) are applied to the enterprise estate.

2. Separating enterprise data from Internet content

Browsers permit the concurrent browsing of Internet and Intranet web pages in separate tabs. This may mean that the browser process is processing untrusted code and sensitive data at the same time, and the browser is required to enforce separation between the two domains. This presents a large and rich attack surface to the

tab running untrusted code and the browser must therefore be robust to attacks from that code.

Some browsers can be configured to treat sites from an enterprise Intranet differently to those from the Internet. This may include a sandbox to ensure that untrusted sites cannot access sensitive enterprise resources which protects against data theft from Intranet sites that are vulnerable to cross-site-scripting and cross-site-request-forgery attacks.

Browsers may allow different settings to be applied to Intranet sites and Internet sites. Older and potentially vulnerable plugins may be needed to access some corporate tools. Configuring the browser to only use them on Intranet sites will protect against attack by a malicious Internet website.

3. Sensitive data storage

3.1 Device storage

Browsers may cache previously-viewed web pages on disk. This places a reliance on the device to protect that information at rest. Whilst platforms with full volume encryption would normally encrypt the browser cache, platforms with file-based encryption may not, and sensitive information from web pages may be written unencrypted to disk.

Browsers may cache credentials by offering to save passwords submitted to websites. Similar to the cache above, organisations should ensure that they are content with how this information is protected on the device, or disable any information caching functionality.

3.2 Cloud sync

Some browsers allow the user to synchronize their web browser to the cloud so that they can get the same experience on all of their devices. This usually includes bookmarks and currently open tabs, but may also include more sensitive data such as saved passwords and personal details. Organisations should consider the impact of automatically uploading enterprise data into the cloud. Sensitive data may be stored unencrypted in an untrusted cloud and a user may choose to sync that to an unmanaged device.

4. Plugins

Third-party plugins such as Adobe Flash and Oracle Java are often required to access certain types of web content, including enterprise web-apps. Modern browsers often allow the user to install plugins to personalise their browser or provide easier access to things they do regularly. Plugins are usually user-controlled and so they should not be relied upon to enforce security controls as they will not be effective if disabled.

Most browsers allow plugins to access all web pages that are currently being accessed. They can read and alter the content of pages, move content between tabs and windows or upload it to the cloud. This can reduce the separation that usually exists between pages in different tabs, some of which may be sensitive enterprise data.

Plugins become part of the browser and so they need to have security patches applied with the same priority

as the browser itself. Like the browsers, plugins may add extra functionality in newer versions. New features may be introduced that work against the security principles, such as automatically synchronising data to an untrusted cloud service or disabling security to increase compatibility. Malicious plugins may start out offering useful features and later introduce malware through an update. While patching should be considered a priority, enterprises should continue to monitor plugins after initial installation to ensure that they do not have undesirable features.

The use of plugins does not have to carry any more risk than using built in-browser features if the plugins being used are known to be safe. Plugins that run inside the browser sandbox are preferred as this maintains the separation in place between untrusted Internet content and the underlying platform. Unsandboxed plugins used to access enterprise services should be configured so that they can only be used on trusted Intranet sites.

Organisations should consider the security balance of maintaining an allow-list of known patchable plugins compared to allowing the user to install arbitrary plugins from the Internet.

Legal information