Forcepoint

Solution Brief

Forcepoint Remote Browser Isolation

How the healthcare industry can ensure productivity and web security with Forcepoint RBI

Features

- Real-time web content analysis
- Native browsing user experience
- Easy deployment and management
- Seamless integration with other security solutions
- Zero Trust Content Disarm & Reconstruction (CDR)

Benefits

- Keep users productive without sacrificing security or performance
- Prevent malware infections, phishing attacks and other web-based threats
- Easy policy management and configuration allow admins to focus on value-add tasks
- Stop data theft via steganography and sanitize all downloaded files
- Maintain regulatory compliance

Digital transformation and cloud adoption has propelled the healthcare industry to the forefront of digital customer service and patient care. Healthcare providers now regularly meet patients virtually via web-based video conferences, leverage IoT devices such as self-serve kiosks at branch locations to facilitate patient check-in, and seamlessly integrate with third-party apps to increase administrative efficiencies.

As patients and employees enjoy the benefits of digital experience, cybercriminals continue to explore ways to exploit these new vectors.

The cyber-attack on Ireland's healthcare system in 2021 left the country's healthcare providers and patients in chaos, as hackers reportedly stole and published more than 500 private records relating to patients[1].

And it all began with a simple email.

During the same year, more than 40 million patient records[2] were compromised in the United States, mainly from web-based threats.

According to Verizon's 2022 Data Breach Investigations Report[3], basic web application attacks and insider threats are the number one and two top threat vectors respectively for the healthcare industry. So how can the healthcare industry continue to deliver the best possible customer service while maintaining security efficacy? With Forcepoint Remote Browser Isolation (RBI).

Forcepoint RBI prevents web threats by transferring the user web request from the local browser to an isolated environment that performs fetch, execute and render functions remotely. With Forcepoint RBI, active code is never sent to the endpoint as all web-based instructions are run in an isolated, purpose-built environment designed to remove malware.

Healthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns[1].

An overlooked security risk located at the branch site is the self-serve kiosk stations patients use to check in, reschedule appointments and perform other tasks. These kiosks are often connected to the internal network, and the SaaS-based app used for patient check-in is connected via an active web session.

A cybercriminal can weaponize a kiosk by accessing a risky site and downloading malicious code onto the device. Once the complete, the malware will infiltrate, encrypt and execute files, often without being detected until the damage is done.

Administrators can avoid this potential threat with Forcepoint RBI, by extending Zero Trust and creating a policy to automatically send risky or uncategorized web requests to an isolated remote session.

Any attempt to download malware in a remote session will be ineffective as malicious code will be stripped from the content, ensuring the security of the device and the network. Forcepoint RBI intelligently optimizes performance with security based on risk policy. For high-risk user groups Forcepoint RBI can render the page in read-only mode to ensure credentials or other sensitive information cannot be entered.

Another commonly overlooked technique used by inside threat actors to steal data out of the network is steganography. This method embeds stolen data into an image file such as JPEG, then the image file is sent out of the network, usually via email.

Steganography has gained popularity in recent years as traditional antivirus is ineffective, as there is no malware to set off alerts. Forcepoint RBI prevents steganography with Zero Trust CDR capability. Unlike traditional AV tools that scan files for malware, Zero Trust CDR automatically sanitizes all files at download to strip active content and then rebuild the files safely from scratch using only benign elements.

How Zero Trust CDR works:

- → Rather than identifying known malware, Zero Trust CDR takes the data and extracts the useful information from it.
- → The extracted information is transformed into an intermediary format and verified.
- → This advanced threat protection process makes sure no threats or attacks can reach the next stage.
- → The original data is stored or discarded along with malware, known or unknown. Brand new data is then built in a normalized way, containing the verified information.
- → The new data replicates the original data, without the threat of embedded malware and is now guaranteed safe.

Allow safe access to risky sites without compromising security. Gain Zero Trust web security with Forcepoint RBI.

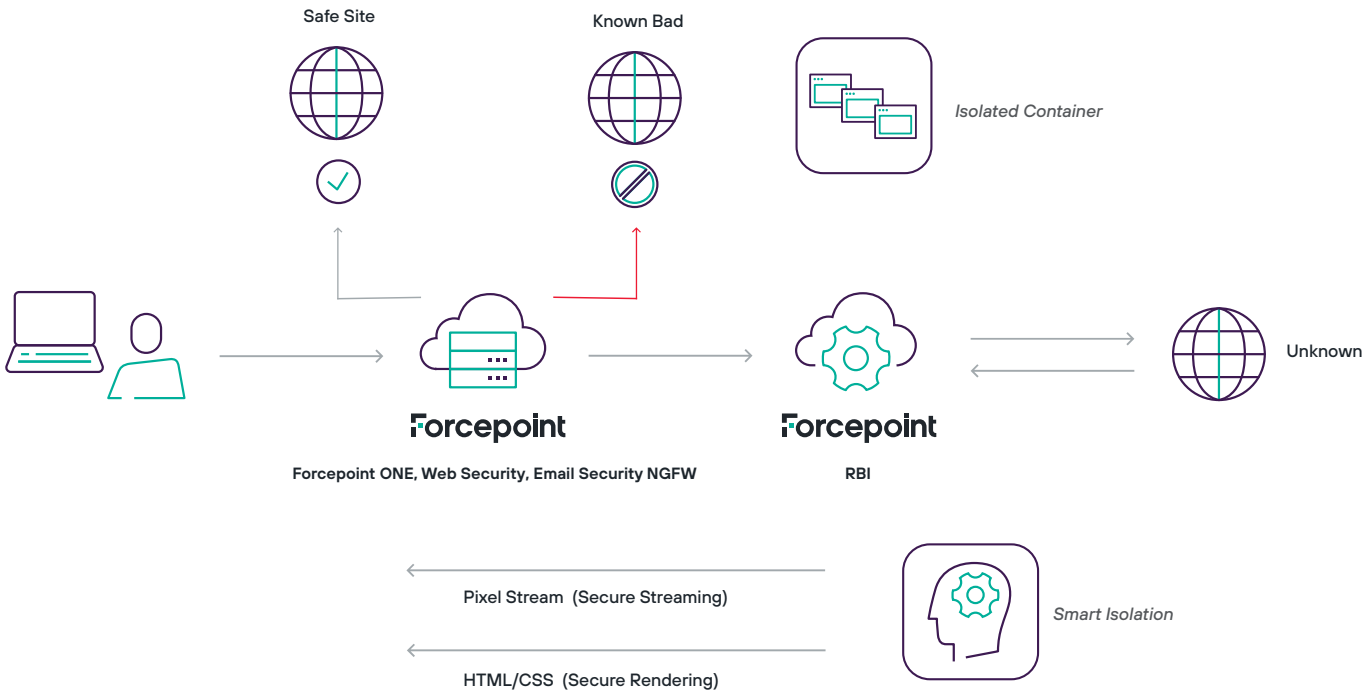

Figure 1. Forcepoint ONE ecosystem with Smart Isolation technology automatically adjusts between two rendering modes based on potential risk or verified trust.

Learn more about Forcepoint RBI here →

1. Health Service Executive ransomware attack - Wikipedia
2. https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021
3. Verizon's 2022 Data Breach investigations report

forcepoint.com/contact

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners
[FP-RBI Healthcare Solution Brief] 23Mar2023