Forcepoint

Use Case

# Remote Browser Isolation For Government Agencies

Powered by Ericom

## Challenge

- Working in defense, security and protection for the internal network is paramount. Agencies must be able to give selected users access to websites based on category and implement a cloud-based, "targeted user" web access environment to eliminate security risks.
- Stop phishing and sero-day threats from compromising endpoints, delivering ransomware, and stealing credentials.
- IT support overwhelmed with web access exception and change requests.

## Solution

- Cloud-based "targeted user" environment.
- Allow selective users access to websites by category.
- Block phishing attacks.

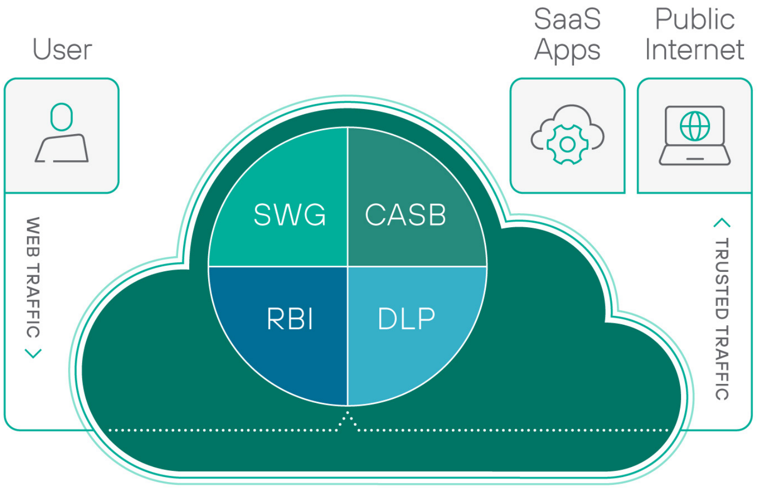
## Results

- Improved productivity and reduced costs without impacting network security.
- Protecting the C-level and other high risk users.
- Preventing data loss.

## Introduction

A large European defense contractor, recognized as one of the world's foremost players in **aerospace**, **defense**, and **security**, chose Forcepoint Remote Browser Isolation (RBI) powered by Ericom to protect employees' devices and network resources from malicious web-based attacks.

The partnership integrates Ericom's remote browser isolation capabilities across Forcepoint's Dynamic Edge Protection cloud-native SASE solution.



## Challenges

The European defense contractor recognized a need for an RBI solution after encountering ongoing costs related to providing access to legitimate websites that had been blocked by their existing technology. With the older approach, the website blocking was restrictive, impacted user productivity, and created a negative user experience. The IT security and management teams, overwhelmed with exception and change requests, decided they needed an alternative solution that provided the following benefits:

- → Enabling broader web browsing access for end-users without increasing risk
- → Protecting the organization's network and applications from malicious attacks
- → Offering protection from zero-day attacks
- → Minimizing need for IT support

A broad review of security solutions from a number of cybersecurity vendors in the market was conducted and the contractor decided that an RBI solution would be the best fit for its network architecture. A short list of vendors was finalized and an RFI was issued. Three vendors were selected to perform an in-depth, technical-led, POC-driven response by the head of IT security and his team. The following results were sought:

→ **Implement a cloud-based, "targeted user" environment:** The remote RBI policy is applied to users only when the selected category of website is triggered, ensuring a seamless user experience.

→ **Allow selected users access to websites (by category):** Working in defense, security and protection for the internal network is paramount.  This contractor was already using Forcepoint Secure Web Gateway (SWG) to manage policies and user access, but access to many sites was statically blocked by policy.

→ **Block phishing attacks:** Stop phishing from compromising endpoints, delivering ransomware, and stealing credentials.

Following the extensive process and review, the company chose the Forcepoint RBI Powered by Ericom solution as it offered the highest level of protection against web-based cyberthreats without curtailing web access or hampering employee productivity. Just as importantly, the feature-rich solution offered the strongest value proposition.

Forcepoint RBI Powered by Ericom offered the defense contractor the following value:

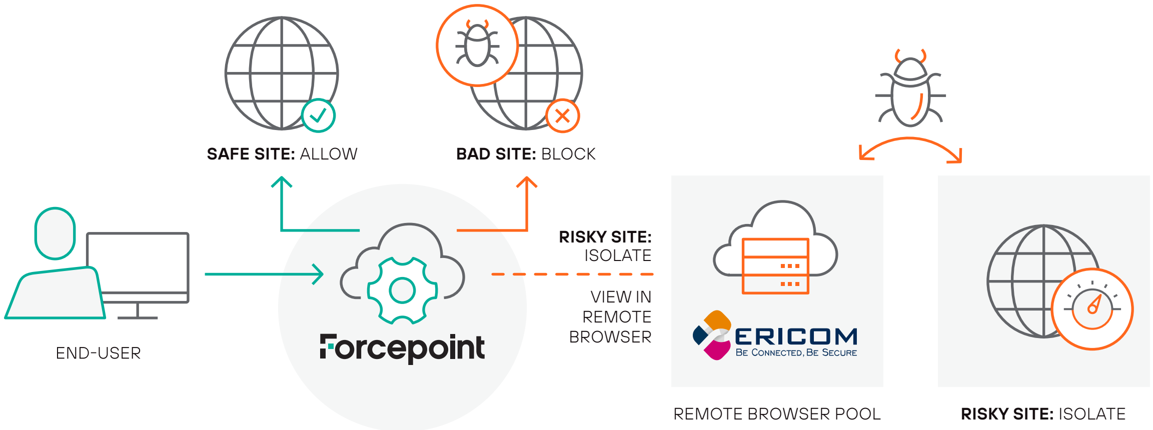
→ The best, most seamless user experience to maintain end-user productivity

→ Ease of cloud deployment with minimal impact to current infrastructure

→ The most advanced level of protection for document downloads beyond simply blocking them

→ An easy-to-implement extension to existing Forcepoint infrastructure

## Targeted Remote Browser Isolation



Forcepoint Web Security ecosystem and Ericom Shield remote browser integration protecting browser environments from malware threats.

## POC Use Case

→ **Cloud based "targeted user" environment:** The remote RBI policy is invoked to those users only when the selected category of web site is triggered ensuring a seamless user experience.

→ **Allow selective users access to websites (by category):** Working in defense, security and protection for the internal network is paramount. This contractor was already using Forcepoint Secure Web Gateway (SWG) to manage policies and user access but with access to most sites blocked by policy. By utilizing RBI in conjunction with the Forcepoint SWG it became possible to improve productivity and reduce costs without impacting on Security moving from a restrictive based approach to an enabling based approach.

→ **Block phishing attacks:** Stop phishing from compromising endpoints, delivering ransomware, and stealing credentials.

## Results and Outcomes

The combination of Forcepoint SWG and Ericom's Zero Trust browsing security framework, Forcepoint RBI executes active web content in a remote, isolated container. An interactive media stream representing the website is sent to the endpoint browser, providing a safe, seamless user experience. The contractor improved productivity and reduced costs without impacting network security when they moved from a restrictive approach to an enabling approach.

File downloads can be disabled but the contractor opted to instead pass files through the Content-Deconstruct-Reconstruct (CDR) engine. This process removes any active content without impacting the readability of the file. This was seen as one area of tremendous value given the nature of defense work which required file downloads.

The approach ensures that advanced web-borne threats cannot impact devices and networks.

## Future Use Cases

The second phase of the Forcepoint RBI Powered by Ericom solution implementation includes some additional uses cases which have been identified and which will be implemented to bring additional value to other areas of data security where current practices are inhibiting user productivity or simply to better address cybersecurity threats. The second phase objectives include:

→ **Protecting C-Level and Other High-Risk Users.** Protect users with elevated privileges by air-gapping their endpoints from web threats.

→ **Preventing  Data Loss.** Keep sensitive web app data out of browser caches; limit user data-sharing activity on websites.

### About Ericom

Ericom Software is a leading provider of Zero Trust secure access solutions that protect organizations from advanced cybersecurity threats. Leveraging innovative browser and application isolation capabilities, Ericom solutions enable simple, secure policy-driven access to mission-critical cloud and on-premises business systems and resources, including the public Internet, without impacting end-user productivity.

### About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

**forcepoint.com/contact**

[Remote-Browser-Isolation-for-Govt-Agencies-Use-Case-EN] 15Oct2020