WEB APPLICATION ISOLATION
IT CONSULTING AND OUTSOURCING

Multinational IT Consultancy Chooses Ericom Web Application Isolation to Shield HR Apps

Customer profile

A leading multinational provider of IT consulting and outsourcing services with almost 260,000 employees

Industry

IT consulting and software

Challenge

- Enable remote users to enter data on the company's HR apps without risk that malware on unmanaged devices will be transmitted to enterprise networks
- Shield the code, APIs and other potential attack surfaces of company apps from malicious actors seeking vulnerabilities
- Enable remote users to safely upload files to the apps, ensuring that they are free of weaponized payloads

Background

The customer is a publically traded, multinational enterprise that provides IT consulting and outsourcing services. It employs almost 230,000 software professionals as well as numerous contract workers and has over 100 development centers worldwide.

Managing a Suddenly Remote Workforce

With the onset of the COVID pandemic, tens of thousands of employees and contractors who had previously worked onsite, in company offices, moved to working from home.

The transition to remote work, of course, posed many challenges for organizations worldwide. Among numerous challenges our customer faced was enabling remote workers – including contract workers -- to access internal human resources (HR) systems, such as an attendance reporting application that was located on company servers.

Remote Connectivity at the Expense of Security

Immediately following the transition to remote work, the enterprise implemented a reverse proxy to enable and control web access to its HR apps. While the reverse proxy helped control who could reach their app, it could not protect it – and the network where it was located -- from malware that might be present on the unmanaged personal devices of users and contractors working from home. When users connected to the HR app, malicious content such as ransomware or downloaders on their devices could be transmitted to the company network and move laterally to infect essential systems or exfiltrate sensitive data.

Given the huge number of employees and contractors, the organization was also concerned about malicious insiders leveraging app access to gain visibility into the app code and APIs, and discover vulnerabilities that could be leveraged as an attack surface.

The Solution: Isolating Web Apps to Protect Company Networks

The company's security team approached Ericom with an interesting request: Rather than using remote browser isolation (RBI) to protect endpoints, they wanted to isolate the enterprise's web application from content on user devices, a use case known as Web Application Isolation (which uses RBI in an inverted way).

When a remote user clicks on an HR app in the organization's web portal, access is automatically routed to the reverse proxy via the closest POP on the Ericom Global Cloud. In fact, if a user attempts to access the app from any IP address that is not on the Ericom Global Cloud, by for instance, typing in the address in a browser rather than choosing the app from the enterprise portal, the connection request will be refused.

Results

- Users can easily access essential HR apps and upload relevant files from unmanaged devices without danger of infecting enterprise networks and systems with malware
- Enterprise systems are protected from view of malicious actors seeking a vulnerable surface to attack

In the Ericom Global Cloud, all content from user devices is routed by Ericom Web Application Isolation to a container located in the cloud. Only a safe data stream is sent from the isolated container to the local user's browser; any malware on the users' local device cannot touch the actual webpage of the HR app at all. Moreover, potentially malicious employees or 3rd-party users cannot see any of the application code or identify vulnerabilities in the application surface, and therefore cannot leverage application access to plan or execute an attack.

Because users sometimes need to upload files to the company's HR apps, Ericom Web Application Isolation integrates Content Disarm and Reconstruct (CDR) technology. Documents that users upload are first inspected in the cloud-based container and sanitized of any malware found within. The documents are then reconstructed before being transmitted to the app to make sure that no infected content reaches enterprise networks.

The Impact

For the company's employees and contractors, accessing the HR apps is straight-forward and seamless – they simply open their browsers and click. Behind the scenes, transparent to users, Ericom Web Application Isolation protects enterprise networks and systems from all ransomware and malware – even zero days – that may be on user devices, while enabling communication of essential employee and contractor data.

Conclusion

Just as Remote Browser Isolation prevents ransomware, zero day exploits and malicious content from penetrating endpoints from the web and phishing emails, Ericom Web Application Isolation protects websites and applications from malware on the endpoint devices that access them, as well as from the prying eyes of cybercriminals and malicious actors seeking attack surfaces that will enable them to penetrate organizations. Like Remote Browser Isolation, Web Application Isolation is transparent to users and enables secure use of essential business applications.

About Ericom Software www.ericom.com

Ericom Software provides businesses with secure access to the web and corporate applications, in the cloud and on-premises, from any device or location. Leveraging innovative isolation capabilities and multiple secure access technologies, Ericom's solutions ensure that devices and applications are protected from cybersecurity threats, and users can connect to only the specific resources they are authorized to access.

Americas:
T +1 (201)767-2210
E-mail: info@ericom.com

UK & Western Europe:
T +44 (0)1905 777970
E-mail: ukinfo@ericom.com

Worldwide:
T +972-2-591-1700
E-mail: info@ericom.com

Follow us