Multinational Consultancy Chooses WAI to Protect Against Unmanaged Device Risk

ericom security by cradlepoint

CUSTOMER PROFILE

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

INDUSTRY

IT consulting and software

CHALLENGES

- Enabling remote users to enter data on the company's applications without risk of malware on unmanaged devices spreading to enterprise resources
- Preventing exfiltration of sensitive data and PII from private corporate applications and cloud and SaaS applications
- Shielding code, APIs and other potential attack surfaces of company apps from malicious actors seeking vulnerabilities
- Enabling users to safely upload files to applications while ensuring that they are free of weaponized payloads

Background

The publicly traded, multinational provider of IT consulting and outsourcing services employs almost 260,000 software professionals as well as numerous contract workers. While the organization has over 100 development centers worldwide, many of its consultants and other professionals work at client sites or from remote locations, including from home.

Managing a Remote Workforce

While managing a remote workforce presented a new challenge for many organizations at the start of the COVID epidemic, by that time our customer had been addressing the issue for years. Their consultants--employees as well as a large contractor workforce--serve thousands of clients across tens of countries. These workers need to access enterprise applications and resources, including an attendance reporting application that was located on company servers.

Remote Connectivity at the Expense of Security

The consultancy had been using a reverse proxy solution to enable and control web access to its HR and other applications. While the reverse proxy could restrict who could reach the applications, it could not control what users did once they were in. It could not prevent them from copying data from the application functions. It could not keep data out of browser caches. And it could not protect the application, the network where it was located, or the data it held from malware that might be present on users' unmanaged personal devices.

RESULTS

- Simple, secure, clientless access to essential corporate apps from users' unmanaged devices
- Granular data sharing controls restrict uploads and downloads
- Permitted downloads are scanned with DLP to prevent data exposure
- Data approved for upload is sanitized of weaponized content
- Enterprise applications – private, cloud and SaaS – are protected from malware on unmanaged devices
- Enterprise systems are protected from malicious actors probing for vulnerabilities

When users connected to enterprise applications, they could copy sensitive information and PII contained within them. If threat actors had established persistence on the unmanaged device, they too would have access to enterprise data. And if the device were lost or hacked, even after the connection was severed, sensitive enterprise data that remained accessible in the browser cache could be exposed.

In addition, malicious content such as ransomware or downloaders that were present on users' unmanaged devices could be transmitted to the consultancy's network, where it could infect essential systems or exfiltrate sensitive data.

In addition to risk of content exposure, the organization was also concerned about possibly malicious insiders leveraging their access to gain visibility into application code and APIs, and discover vulnerabilities that could be leveraged in an attack. Threat actors who had established persistence on user devices could potentially do the same.

The Solution: Isolating Web Applications to Protect Company Assets

The consultancy's security team was familiar with Ericom's world-class remote browser isolation (RBI) solution. They approached Ericom to inquire about leveraging the company's isolation technology to protect their enterprise web applications from content on unmanaged user devices. This solution, Web Application Isolation (WAI), also applies granular sharing controls in the cloud to prevent data loss and exposure through access by unmanaged devices.

When a remote user clicks on an application in the consultancy's web portal, access is automatically routed via the Ericom Global Cloud, using the closest POP. In fact, if a user attempts to access the app directly, even with their legitimate username and password, the logon will be refused.

In the Ericom Global Cloud, all content sent from the user device to the application is isolated within a container. Only a safe stream of rendered content is sent from the isolated container to the application; any malware sent from the user device remains in the container until it is destroyed and never reaches the enterprise web application.

Within the container, granular policy-based data sharing controls are applied to restrict content uploads to and downloads from the application, block specific data from users' view, disable clipboarding functions (copy/paste/print) for application content views, and scan content with data loss prevention (DLP) to prevent exposure of sensitive information. Permitted uploads are sanitized within the container by content disarm and reconstruct (CDR) technology. Any malware that is found is stripped out before the attachment is reconstructed, with desired functionality intact, and uploaded to the application.

WAI also blocks malicious users or threat actors who have established persistence in the unmanaged devices from viewing application page source data, developer tools and exposed APIs, so they cannot identify vulnerabilities in the application surface to gain access or execute an attack.

The Impact

For the company's remote employees and contractors, accessing the applications is straight-forward and seamless – they simply open their browsers and click. Behind the scenes, transparent to users, Ericom Web Application Isolation protects the consultancy's networks and data from data exposure and loss as well as cyberattacks – even using zero days – via malware that may be present on unmanaged user devices.

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 unmanaged third party devices and user BYODs, as well as from the prying eyes of cybercriminals and malicious actors seeking attack surfaces to penetrate organizations. Like Remote Browser Isolation, Web Application Isolation is transparent to users and enables secure use of essential business applications.

Contact us for more information or to schedule a demo at **ericom.com/contact-us**