ZTEdge™
DEFEND WHAT MATTERS

Key Questions to Ask RBI Solution Providers

In the face of escalating ransomware and zero-day threats, demand for Remote Browser Isolation (RBI) is surging as organizations bolster their web and email security defenses.

Teams tasked with investigating RBI technology for their organizations quickly discover that RBI solutions are not all created equal. Key differences exist in the areas of:

- User Experience
- Performance
- Security and Policy Support
- Functionality and Applications Support

To help assure the success of your web security program, this paper outlines key questions that your IT and Security teams should be asking every Remote Browser Isolation (RBI) provider. These questions will help your team get the detailed information they need to evaluate the solutions and determine which best fits your organization's needs. The comments that accompany each question provide background information that can help you assess the ramifications of the responses.

Top 4 Questions to Ask about RBI Solutions

These 4 questions are so critical to the success of your RBI program that they deserve special attention.

Q1 Does this RBI solution provide a standard native web-browsing experience?

Does this RBI solution work with each user's usual native browser? Would they be aware of using RBI or is it transparent?

The web browser is a key productivity application for most employees, so significant changes to users' browsing experience should be avoided.

Q2 How does it impact performance?

Anything that slows down web performance, even in the name of security, will trigger user resistance. To keep isolated web traffic moving quickly, the best RBI solutions offer multiple rendering modes and leverage highly available global cloud infrastructures.

Q3 Does the solution combat phishing and credential theft?

How well will the RBI solution defend your user email and inboxes? An RBI solution's ability to improve email security is critical for minimizing the risk that phishing presents, since inboxes are the primary entry point for ransomware.

Q4 What about securing web conferencing solutions like Zoom and WebEx?

Can virtual meetings such as Zoom, Teams, WebEx and Meet be secured without installed applications, while maintaining seamless camera, microphone and screensharing functionality?

Only ZTEdge RBI has a patent-pending Virtual Meeting Isolation solution that isolates resources like cameras, microphones, and screen-sharing to keep users safe from malware. Others simply exempt web conferencing solution sites from isolation.

For your convenience, an Excel spreadsheet version of these questions can be downloaded here.

User Experience

Question	Comment
Does the RBI solution deliver a "native" web browsing experience using standard browsers such as Chrome, Edge, Safari, Firefox etc?	The web browser is a key productivity application for most employees, so significant changes to users' browsing experience should be avoided.
Will users be aware of differences from browsing via their usual preferred browser?	For best user experience, an RBI solution should be able to be transparent to users and shouldn't impact their web access and use. Offerings that use a "browser within a browser" approach or limit users to a specific web browser notably alter the user experience.
How does the application allow you to indicate to users that their session is being isolated?	The best RBI offerings provide several RBI indicator options, so each organization can choose whether to make the RBI invisible or provide an unobtrusive frame, without confusing users with a browser-within-a-browser or multiple URL layers.
Does the solution require deployment of a local client/agent?	RBI solutions should not require local agents on user devices, since installing them and keeping them updated puts a burden on IT. RBI solutions should require only that users use one or more standard modern browsers on their devices, such as Chrome, Edge, Firefox or Safari.
Does the remote browser isolation solution support web browser plug-ins? Which ones? Are there restrictions as to which may be added or additional support requirements?	Organizations typically require PDF and Flash support via browser plug-ins. Java support is also frequently needed. Installation of additional applications or software that operates within an RBI application might negate its security benefits. Make sure to check how the RBI solutions handle this issue.
Can individual users' personal preferences and settings such as home page, bookmarks, and font size be saved to persist over time?	Sessions should be reset back to a known good state, but some elements should be retained to improve usability. Cookies for frequently used sites (for example, a personal banking site) should persist, but unknown and unwanted third-party cookies should be removed, based on policies.

Performance

Question	Comment
How does the RBI solution impact website performance? Please describe how performance is managed.	Anything that slows down web performance, even in the name of security, will trigger user resistance. To keep isolated web traffic moving quickly, the best RBI solutions offer multiple rendering modes and leverage highly available global cloud infrastructures. Other less mature solutions offer only 1st-generation slow "pixel-pushing" technology with limited on-premises and cloud deployment options.
What rendering options does the RBI solution offer (e.g. vector-based rendering, DOM, pixel)?	Mature RBI solutions should include multiple rendering mode options. This allows organizations to optimize RBI policies to minimize latency and deliver excellent performance and user experience. Some less mature solutions offer only "pixel mode" which can introduce jitter or cause sluggish performance.
How is video content, such as YouTube, handled?	Good RBI solutions offer policy-based rendering options with specific modes optimized for video content. Solutions that offer only "pixel-pushing" modes are likely to deliver a jittery or sluggish high-latency experience for video and other heavy content.
Does the solution offer a full cloud SaaS service or is the RBI's cloud solution deployed using a virtual appliance through a cloud IaaS provider?	The cloud infrastructure offered should be evaluated in as much detail and with the same emphasis as the RBI service's capabilities to ensure consistent, low-latency performance from anywhere users are located. Appliances, by definition, can present challenges in terms of cost and ability to scale elastically.
If the solution is a cloud service, is its architecture "cloud-first"?	Up-to-date cloud technologies should be integrated to ensure that the RBI service delivered is resilient, scalable and highly available.
If RBI is to be provided as a cloud-based service, please describe its cloud and POP infrastructure.	The RBI cloud platform's global POP infrastructure should align with your intended usage needs and adequately cover all locations where users are likely to need access.
Does the offered cloud infrastructure automatically route user web traffic to the closest POP of the RBI solution cloud? Does it use multitenant architecture?	The global cloud infrastructure via which the RBI service is delivered is just as important as the solution's capabilities. Enterprises should ascertain whether the platform can support the service levels required for their users around the globe, whether in the office or working remotely from home or the road.
Does the RBI offering allow the organization to define what POP location a user goes to?	In some situations it is important to be able to restrict users to certain POP's or geographies.

Security and Policy Support

Question	Comment
How does the solution protect against phishing and credential theft? Please describe. How well will the RBI solution defend user inboxes?	An RBI solution's ability to improve email security is critical for minimizing the risk that phishing presents, since inboxes are the primary entry point for ransomware. When a user clicks on a questionable link in an email (as roughly 5% of users do) most RBI solutions will block all malware on the site. Your solution should also be able to identify suspicious websites and render them in isolated "read-only mode" to prevent users from entering IDs and passwords. This is a critical capability to prevent credential theft attacks.
What policy options and security controls are offered to protect against phishing?	A good RBI solution will allow suspicious sites to render as read-only so they can be viewed, but no website content can reach endpoints and users cannot enter sensitive data. The best solutions will allow choice of various policies including "read-only" and full blocking.
Can users securely download files from emails and public websites, without risk from malware that may be hidden within? Can they safely save them to their own devices with native functionality intact?	The best RBI solutions incorporate CDR for disarming documents. Unlike "preview mode" or similar actions that disable native file functionality, CDR allows downloaded documents to function as expected (e.g., spreadsheet, word processor, pdf, slides, etc.) with dangerous code removed. If CDR is recommended by the RBI provider, is enabling safe "deconstruction" of malicious content built into the offering? If so, once completed, users should have full access to material that is benign. Alternatively, content can be scanned for viruses by AV and/or sandboxed before being moved to the local device. The best offerings provide both CDR and AV/sandboxing.
Does the solution offer policy-based controls to limit browser data sharing functions? Can the following functions be selectively allowed/disabled? • **Cut & paste (clip-boarding)** • **Print functions** • **Download and upload of data and documents** **Can policies be based on criteria such as users, groups and/or domains? Please describe.**	The web and cloud apps are significant channels of data loss, either through unintentional actions or via intentional activity by malicious insiders. RBI can help "lock down" data leaks with web browser sharing controls. Make sure that restrictions are policy-based, so required functionality is not impaired.
Can users bypass isolation by using a different web browser? If so, please describe how that is prevented.	All web activity from an endpoint device needs to be channeled through RBI to ensure consistent and reliable policy enforcement. Some solutions are configured per browser app, allowing risky sites to be accessed by using a different browser.

Security and Policy Support (continued)

Question	Comment
Can the RBI solution be used “in reverse” to isolate enterprise apps and data from unmanaged devices?	This emerging use case is becoming increasingly important to organizations that want to protect their web apps from attack via an unmanaged or compromised device, or to prevent their websites from being co-opted to stage malicious content.
Can users bypass RBI by browsing outside of working hours? Or by browsing from other locations?	To ensure that policies are consistently and reliably enforced, all browsing activity from endpoints that are ever connected to the business network must be channeled through RBI. Some solutions can be (mis)configured to allow risky sites to be accessed outside of business hours and/or when the user is in a different location.
Are RBI policies easy to manage? Is the policy creation console easy to navigate? Does it offer the ability to create very granular isolation policies? Please provide examples.	Policy creation and system configuration can be a time sink, so look for a management console that makes it simple to set flexible, granular policies based on website categories, individual URLs, users, groups, location, and more.
Can the RBI solution operate independently of the provider’s SWG or NGFW? (e.g., “will we be able to switch SWG or firewall vendors while retaining the current RBI solution?”)	Some vendors only offer RBI as an add-on for their SWG or NGFW and do not license the RBI solution independently. As a result, those solutions can’t integrate with and are not interoperable with the broader security vendor ecosystem. This places undue restrictions on organizations that wish to maintain flexibility to implement a best-in-class set of solutions (SWG+NGFW+RBI). It also locks in organizations that may wish to switch their SWG or firewall while retaining their RBI solution.

ZTEdge™
DEFEND WHAT MATTERS

Impact on Frequently Used Applications

Question	Comment
How are virtual meeting/web-conferencing applications such as Zoom, Teams, and WebEx handled? Can virtual meetings be seamlessly secured, without installing applications?	Virtual meeting solutions have become a workplace staple for business professionals worldwide. But their web portals expose business users to the same risks as all other websites. An effective RBI solution should allow virtual meeting resources like cameras, microphones, and screen-sharing to be used within an isolated environment. This allows the power of RBI to be extended to virtual meeting apps to prevent hackers from using them to launch attacks. Watch for RBI solutions that simply exempt web conferencing sites from isolation.
Explain how the remote browser isolation solution supports SaaS applications. Does it support O365, ServiceNow, Salesforce, and G-Suite? **Does the RBI solution recommend whitelisting SaaS apps such as those?**	Some RBI solutions have not "tuned" their solutions to optimize performance and usability with SaaS applications. If the user experience with common web-based applications is poor, users will find ways to bypass the RBI solution, increasing risk of exposure to threats. Whitelisting, of course, similarly increases risk.
Does the RBI solution enable safe downloading of files from apps such as Excel, Word, PPT, PDF and others? How does it ensure that the files are safe?	A good RBI solution will offer the ability to sanitize files that are being downloaded using Content Disarm and Reconstruct capability, so the file will be available to users immediately, with its native functionality intact. The best RBI solutions offer AV as well as CDR. Rudimentary/less mature solutions will offer a preview mode, allowing a user to view only static content.