eBook

Remote Browser Isolation - The Ultimate Guide

Table of contents

Remote browser isolation:

What it is, how it works, and why it matters for your organization

Cyber threats are no strangers in our digital world. Every day, we face increasingly sophisticated tactics designed to target unsuspecting users.

97% of organizations have seen an increase in cyber threats since 2022. - Accenture

About 60% of attempted breaches from outside an organization succeed. - Accenture

As these threats grow, our protections must keep up—and that's where remote browser isolation (RBI) comes in.

Let's explore exactly how RBI keeps users safe—and what its role looks like as cybersecurity evolves.

Explore the possibilities of RBI with Parallels Browser Isolation, built for simpler onboarding and better experiences. Try it for Free

What does RBI mean today?

Remote browser isolation technology is—or should be—a major component of modern cybersecurity. It acts as a buffer between users and the dangers of the internet. It stages every site a user visits in a secure environment in the cloud. This way, threats get isolated and neutralized before they ever get through to the user.

Protections like RBI are becoming increasingly important as cyber threats rise.

Malware and ransomware, phishing, and zero-day browser vulnerabilities all pose a danger for users through their web browsers—sometimes even if they don't click.

To add to the issue, shifts like remote work and bring-your-own-device policies create wider attack surfaces and bigger risks for organizations.

- **Less oversight for IT:** When devices aren't in one centralized place, it's harder for IT techs to monitor, manage, and oversee their use.
- **Unauthorized use:** BYOD policies carry the chance of people using devices for personal activities that put the organization at risk—but it can happen with remote work, too.
- **Higher vulnerability to social engineering:** Employees scattered around the globe may not know one another, making them more susceptible to impersonation scams.
- **Public places:** Employees may work from public or unknown networks, especially in places like coffee shops. This makes them vulnerable to network and physical threats like drive-by downloads.

In this guide, I'll explore ways organizations can use modern RBI technology to protect themselves, their employees, and their sensitive data from web-based threats.

Web-based threats are on the rise

Both the frequency and complexity of browser-based attacks have increased in recent years.

In a 2025 survey, 94% of organizations said they've seen an increase in multi-channel attacks in the last year.

That's not to mention that global cybercrime damage costs will likely hit $10.5 trillion USD in 2025—up $7.5 trillion from a decade ago.

This increase is mainly due to the increasing attack surface organizations face. Decentralized IT infrastructures and distributed workforces, along with increases in web traffic, have created more pathways for attacks. Multi-channel attacks target people through multiple channels like email, text messages, social media, and even voice and video calls.

These channels have become more accessible due to vulnerabilities introduced through remote work and BYOD policies.

Since the pandemic, employees have experienced blurring lines between work and personal lives. This further exposes organizations to the risks of web-based threats.

For example, in 2021, it was found that of employees surveyed:

- 50% used work devices for personal purposes
- 40% used work devices for online education
- 27% let other people use work devices
- 27% used work devices to play games
- 36% used work devices to stream content

What does this mean?

In addition to lower IT oversight of company devices, employees are being lax with their security. This just adds to the already-increasing attack surface for organizations.

> "Imagine a vice president receiving a call from the 'CEO' asking them to execute an urgent action, followed by a confirming message on another medium like Teams or Slack. The call creates urgency, and the follow-up adds credibility. Who wouldn't do as advised?"
>
> – Sascha Giese, tech evangelist at SolarWinds
> Originally cited on ITPro

Why security starts with the browser

Many web-based threats rely on network or browser connections to find their targets. They also rely on browser vulnerabilities to extract information from their targets.

Because browsers are the first line of access, they should also be the first line of defense.

That's why modern cybersecurity starts with protecting users' browsers through cloud-based web isolation.

Local browsers	Cloud-based browsers
Are easy to use and access but vulnerable to malware and malicious code	Isolate devices from potential threats, creating a protective shield
Can expose information on devices to attackers	Run remotely to protect other data on the device from attacks
Can create issues with zero-day vulnerabilities that open gateways for attacks	Negate zero-day vulnerabilities and isolates web browsing from happening directly on the device

Your organization's security starts with a browser experience that knows how to keep you safe.
See how it works today with Parallels Browser Isolation. Try it for Free

Where organizations run into issues with RBI

There are four major challenges associated with RBI as a cybersecurity measure.

Bandwidth use Because of the complexity of RBI, some solutions can overload network systems. This can negatively impact performance.	**User experience** Poor loading times and delays between a user's interaction and result can prevent user adoption and discourage use.
Integration issues Some solutions can run into problems integrating with existing systems or security tools. This creates bottlenecks for users.	**Perception issues** Due to issues like these, users often feel that RBI slows them down rather than helping them work faster and more securely.

How RBI has evolved to solve challenges

Cyber threats are becoming more common and sophisticated. Users are less cautious with devices. Remote work and BYOD open up new pathways for attacks. And RBI, a key point of cyber protection, can run into issues.

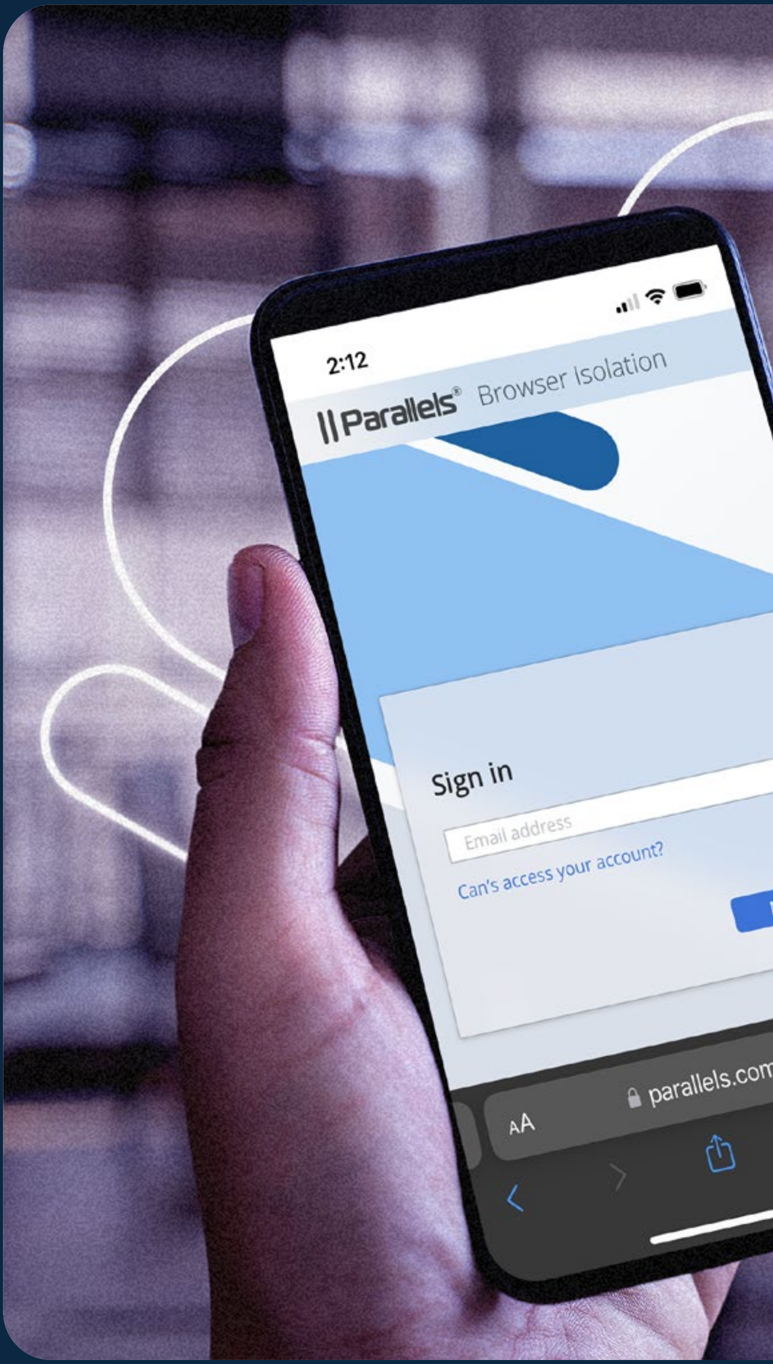
What's an organization to do?

Luckily, RBI has evolved to keep ahead of the threats it protects against. As organizations shift to cloud-based ecosystems to centralize scattered workforces and struggling IT infrastructures, RBI has evolved to become the virtual centralization system they need.

- It's become lightweight, with architecture that doesn't require as much bandwidth.
- It's learned to integrate with enterprise security frameworks.
- It's gained intuitive designs that keep users' workflows on track and minimize interference.
- And for that, it's becoming a core component of organizational security measures.

Just consider that the RBI industry, worth $0.7 billion USD in 2024, is projected to reach $8.26 billion USD by 2033. That's a lot of growth, and it reflects both the increasing need for it due to cyber-attacks and the rate at which organizations will adopt the technology. Protect your organization against cyber threats—and low-latency RBI—with Parallels Browser Isolation.

Try it for Free



Managed or on-prem?

Another way that RBI technology is evolving is by considering what the organization really needs.

This often shows in the decision between managed and on-prem systems. While a remotely managed system can benefit companies with lower IT capacities, an on-prem system can work for one with higher IT capacity.

Because on-prem RBI runs within an organization's network, it can handle security needs through a tighter integration with existing IT infrastructure. It can also run customized functions, including monitoring in-house apps and meeting diverse regulatory requirements.

This ultimately gives organizations more overall control over their security.

Managed RBI	On-prem RBI
Entirely cloud-based	Runs browser sessions in a cloud-based environment but is handled on-premises
Policies handled for the company by vendor	Policies handled by the company in-house
Requires non-SaaS in-house apps to be managed through a VPN	Can manage non-SaaS in-house apps

How organizations are using RBI

As threats evolve, organizations are using RBI in all sorts of ways to protect their clients, their employees, and their data and intellectual property.

Stop multi-channel phishing attacks

By isolating sessions in impenetrable cloud environments away from an organization's network and devices, RBI protects against phishing attempts. This is especially important as multi-channel phishing becomes more prevalent.

Insulate users from malware

RBI runs users' browsing sessions in separate browsers away from the device itself. This allows it to act as an air gap between the device and the network, preventing the spread of ransomware and spyware between devices.

Isolate contractors and high-risk users

Sometimes, contractors and other external users need to access company files. RBI gives organizations a way to do this without exposing those files—or their network—to external devices.

Minimize the risk of zero-day browser vulnerabilities

Because RBI separates browsing activity from the browser itself, it helps organizations avoid risks of vulnerabilities that haven't been patched yet.

Improve cost efficiency and scalability

RBI solutions can improve an organization's cost efficiency and ability to scale by controlling endpoint infections and reducing the costs of removing malware.

Different types of RBI also have other ways of managing costs and scalability.

Cloud-based RBI brings lower upfront costs and simple scaling to the table, so it's simple for hybrid workforces to grow.

On-prem RBI integrates with existing networks, giving larger organizations flexibility to control sensitive data, integrate with existing systems for cost management, and expand over time.

How to decide if RBI is right for your organization

If you're considering the benefits of RBI for your organization, there are a few steps to take.

1. Assess your current exposure to web threats and vulnerabilities

Do you have lots of files or devices that need to operate outside of your central IT structure? Have you had run-ins with browser-based threats before?

While employee education can help, it's worth considering if a proactive approach would go farther for you.

2. Research and identify RBI solutions that match your goals

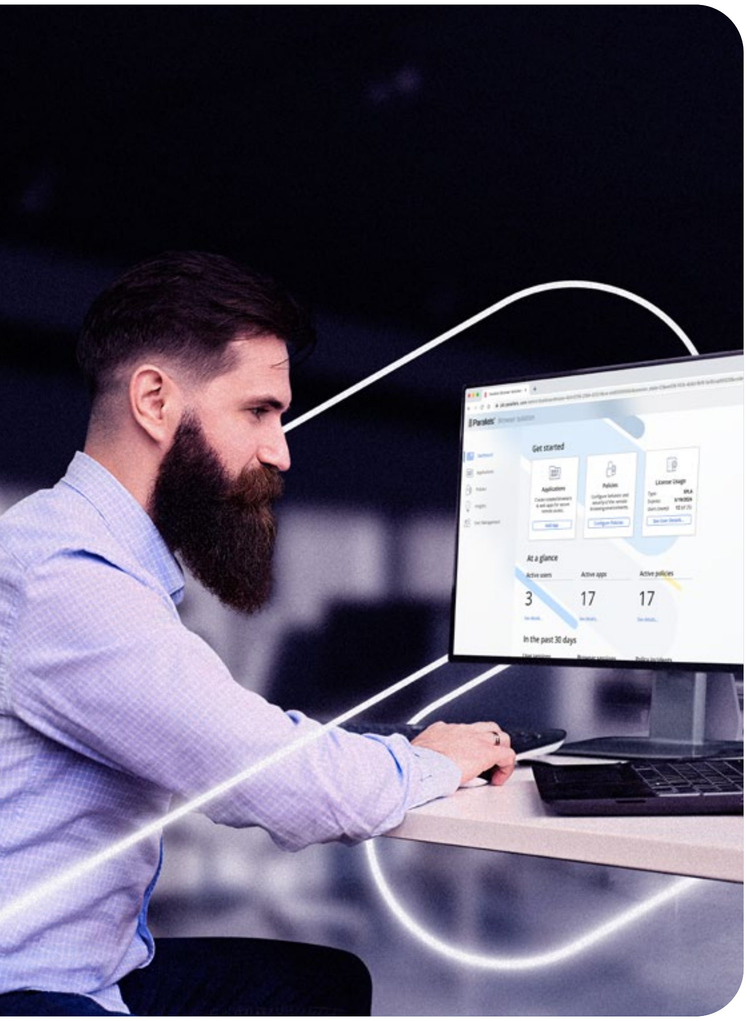
Each RBI solution out there does things a little differently. Identify which ones best fit your organization's needs and address your current exposure the best.

3. Run a pilot with your RBI solution

Once you've chosen your candidate, run a pilot test within a segment of your business. Be sure to collect data on performance, scalability, compatibility with other solutions, and ease of use for your employees.

4. Roll out your RBI solution company-wide

When you're satisfied that the pilot went well, roll it out across the company. Keep an eye on its behavior in your broader cybersecurity framework.



It's time for better cybersecurity

Cyber threats aren't going away—and RBI is an essential tool for organizations to protect themselves, now and in the future.

As the industry grows and cyber threats increase in sophistication, now is the time to establish your organization's security structure.

Now is the time to consider scalable solutions that will grow as you do, keep productivity high, and protect your data from the dangers of malware.

Show cyber threats the door—not the way in

Cyber threats are always looking for the easiest way into your organization. Parallels solutions and Parallels Browser Isolation are designed from the ground up to keep them out.

From contractors and vendors to remote workers, BYOD policies, and everything in between, set your organization up for security with Parallels Browser Isolation.

Try it for Free