TALON

POINT OF VIEW

Why Secure Enterprise Browsers are Emerging as an Alternative to VDI

By Reuven Eliyahu
VP of Customer Success

Due to the rise in distributed work, the need to provide a way to connect employees and third parties back to their SaaS and web-based business applications had grown. The optimal solution would maintain seamless and flexible working environments no matter where users are.

These solutions, however, have the potential to create a multitude of challenges for organizations of all sizes. They create environments that are complex, expensive, risky, and perhaps most prominently, deliver poor, inconsistent user experiences to your workers.

Thankfully, modern VDI alternatives can address the shortcomings of these solutions for a variety of use cases, helping organizations enable secure access to corporate applications and data in a way that is non-invasive, and delivers exceptional user experiences.

Why VDI solutions aren't the answer for distributed work security and support

Some businesses use VDI solutions to secure their distributed workforce, which could include third-parties and employees who are using their own devices as part of BYOD programs. VDI is a virtualization solution that leverages virtual machines to provide and manage virtual desktops. Essentially, VDI solutions host desktop environments on a centralized server, and deploy them to end-users, who access them over a network via their endpoint.

Because of this, VDI solutions are tough to scale, as the scalability of the hosting IT infrastructure is a difficult matter to tackle. Think about it like this: as an organization adds more users and creates more virtual desktops for workers to access, they also need to add more compute, storage, and networking resources to support the VDI workloads. As the infrastructure grows, this becomes incredibly complicated, expensive, and difficult to deliver consistent user experiences for workers.

Along with introducing operational complexity, VDI also raises some security concerns. Common factors like stolen credentials can expose an organization to a multitude of threats. For example, virtual desktops are often left unpatched and don't have sufficient security software installed, making them incredibly vulnerable to threat actors.

All that said, the concept of VDI is valid and has a place in modern businesses. Organizations must find a vehicle to provide secure access to corporate applications and data for distributed workforces. Employees, contractors, and other workers within enterprise environments need to be able to connect back to the business in a secure manner regardless of their physical location.

Distributed work empowers the business to move at the speed needed to be successful. The trick that IT and security leaders need to tackle is providing access in a way that is inherently secure, doesn't break the bank and delivers consistent user experiences that allow work to flow.

Analyzing how work is conducted

To address the challenges of VDI, security and IT leaders need to take a step back and understand the trends that are changing how users work.

For starters, SaaS and web-based application usage have sharply risen, with the average IT team responsible for managing and securing over 110 SaaS applications, according to data from BetterCloud. More and more applications are moving to the web, leading to more work being done in the browser itself.

The browser has emerged as the new workspace, where users access critical applications and data. Because of this, it represents the most natural vehicle to connect workers back to the business in a secure manner.

The emergence of the secure enterprise browser

Thanks to the standardization of Chromium, the open-source foundation of popular browsers like Chrome and Edge, new enterprise browsers are able to deliver consistent user experiences, and robust security features, and have emerged as a viable solution to reduce and replace the use of VDI.

Essentially, the browser combines the user experience that users know with enterprise-grade security features and controls for IT and security leaders. Rather than placing security around the browser, it is baked directly in, acting as a secure access point back to the business for distributed workers.

Unlike VDI solutions that host desktop instances remotely, an enterprise browser is able to isolate web traffic locally on the endpoint, preventing things like malware spread and data loss without adding latency or impacting the user experience.

Plus, enterprise browsers are easy and cost-effective to deploy, administer, and support, since they do not have the expensive licenses cost or the IT management overhead that comes with VDI solutions. In fact, enterprise browsers can deliver up to 80% savings compared to VDI.

From a security and control perspective, an enterprise browser:

- Is easy and cost-effective to deploy, administer, and support, and requires no admin privileges
- Provides secure access to SaaS solutions and internal web apps running in public or private clouds
- Isolates web traffic locally on the endpoint, providing a native user experience
- Supports a wide variety of endpoints and operating systems
- Addresses a wide range of users including employees, contractors, business partners, and third-party IT service providers

The bottom line?

As the adoption of SaaS and web-based applications continues to rise, enterprise browsers offer a modern solution to ensure users are able to work freely, while maintaining the enterprise-grade security posture needed in today's environment.

With an enterprise browser powering your distributed workers, they benefit from improved and consistent user experiences, while security and IT teams gain the granularity and visibility to properly defend against modern attacks.

About Talon Cyber Security

Talon Cyber Security is modernizing security programs and improving user experiences for hybrid work by delivering the first secure enterprise browser. Built on Chromium, the TalonWork browser provides customers with consistent user experiences, deep security visibility, and control over SaaS and web applications needed to simplify security for the future of work. Talon was named the Most Innovative Startup of 2022 at the prestigious RSA Conference Innovation Sandbox Contest. For more information, visit talon-sec.com.

About Reuven Eliyahu

Reuven is VP of Customer Success at Talon Cyber Security, where he is responsible for ensuring that Talon's team and product delivers unmatched value and support to organizations throughout the customer lifecycle. Prior to Talon, Reuven was VP of Products at Argus Cyber Security, the world's first automotive cybersecurity company. Previously, he held product and R&D management roles at leading organizations, including Palantir, IntSights, Intelitek and Thales. Reuven holds a bachelor's degree in computer science from Reichman University.