Kasm
WORKSPACES

PROTECT
THE ENTEPRISE

▷ ▷ ▷ ▷ ▷ ▷

INTRODUCING THE KASM
ENTERPRISE BROWSER

I will tell you
Why it is important

93%

Windows Apps

Browsers

1997   2014   Today

Browser usage over time
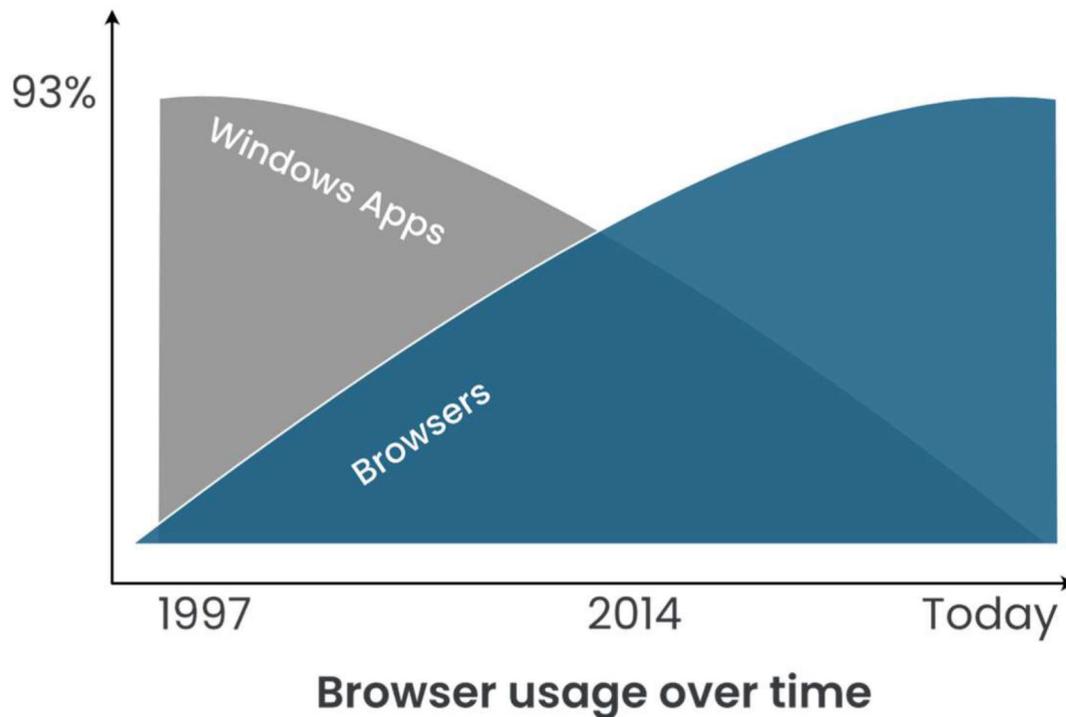
In 1995, the first commercial internet browser started taking shape. Within one year, the browser wars began. By 2000, corporations took advantage of the benefits of the browser, shifted away from applications installed on desktops, and began webifying their applications.

Today **more than 93% of all corporate activity** is done through an internet browser. We know the names: Chrome, Safari, Firefox, MS Edge, and Opera to name a few.

The value of webifying business applications for corporations is clear. However it opened the door to lots of other headaches.

The main culprits are **hacking, malware, and ransomware**

Kasm's enterprise browser is designed to meet these culprits head on.

Our motto **"SAY YES"** to new security techniques and corporate compliance.

Internet	Network	Laptop
WiFi	Office	Browser

Old ways are
Hard to change

Monitor for attack, "if found" delete it, get a new patch to monitor the next attack.

Our IT departments work diligently to protect their internal customers' work products from attacks that come from many angles. Many hackers are technology experts and make it their business to find new ways, or vulnerabilities, to use to attack end users on their devices. These corporate devices are subject to two main angles of attack: the device and the browser.

"If found" are the two key words everyone lives by today. With our close communities, it only takes a matter of minutes for 1 virus to infect 50% of the community. And as the attackers become more savvy, their viruses learn to wait for the opportune moment. Bringing down whole corporations.

Corporate Device

For a hybrid worker, their laptop is everything. And the same defense models from the 1990s are still the ones in use today.

Browsers

How does one stop social engineering? Once the browser allows in the virus, the potential to create widespread infection is very high. Locking down the browser causes numerous other problems. So a balance has been reached within corporations; use the browser, but use it carefully. And we, IT, will revert to above model to protect the corporate device..

The virtual session simply appears as a tab or window within your local browser. No worries about infecting your local device. No worries about infecting the corporate network. The virus has no place to go. It is stuck in the container.

Feel safe blending

work and person life activities together.
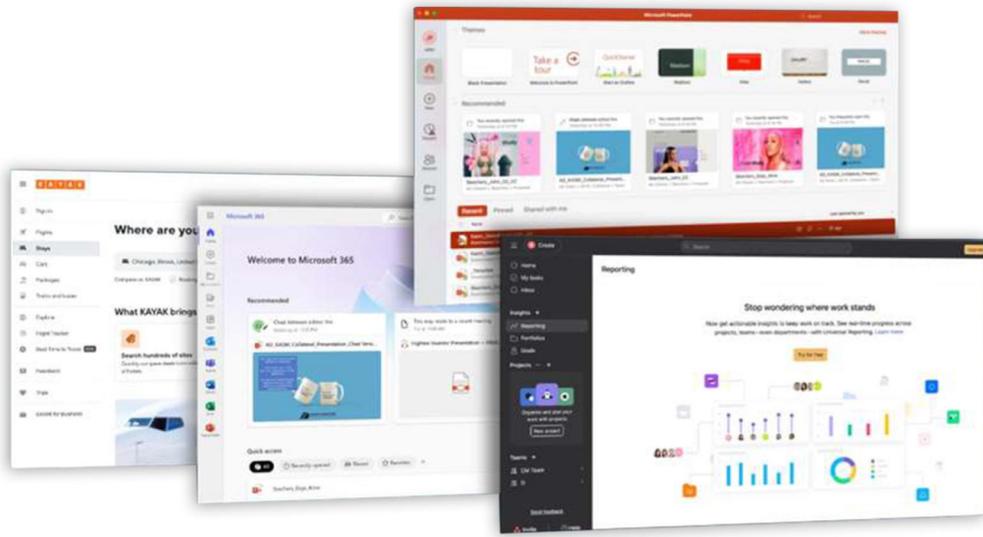
There is a Better Way

▷ ▷ ▷ ▷ ▷ ▷

We have call it, **"Virtual Browsing."** Kasm's container strategy isolates all the activity away from the device and places it in the cloud.
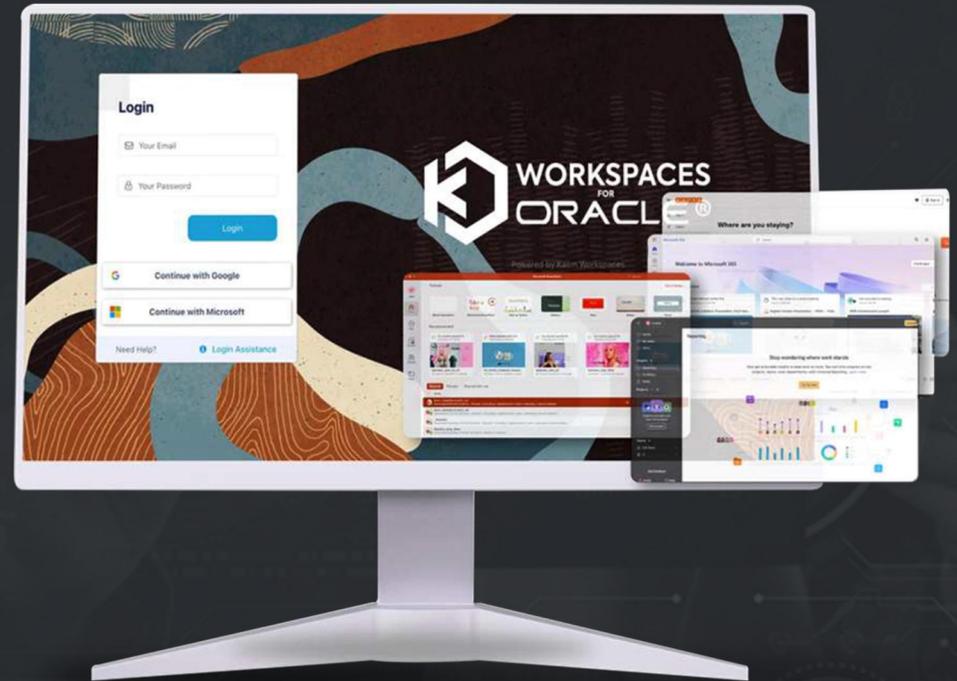
We believe
Containers have Super Powers

Do you want to access your data or do you want to protect it?

Many existing remote access systems are designed with access architecture at their core. In the 1990s, that was necessary. However in todays worlds, it creates opportunities for hackers, malware, and data theft.

At Kasm, the container approach, steeped in security, makes for a winning combination between access and protection. **"Say Yes to Both – Access and Protection!"**

Armed with Virtual Browsing, your end user's devices are safe. IT no longer has to worry about end user's getting hacked and their corporate environment infected. The Enterprise Browser has cybersecurity features built-in.

Secure Access

- ⊘ Zero-Trust Architecture
- ⊘ Two-Factor Authentication
- ⊘ Single-Sign-On with Corporate Identity Access Management
- ⊘ Agentless Web-Native Remote Access

Active Protections

Web Application Firewall (WAF)
Zero-day Vulnerability Mitigation and Malware Prevention
Advanced Rate Limiting for brute force and DDoS protection
Nightly Builds to Automate Patching/Upgrades
Data Loss Prevention