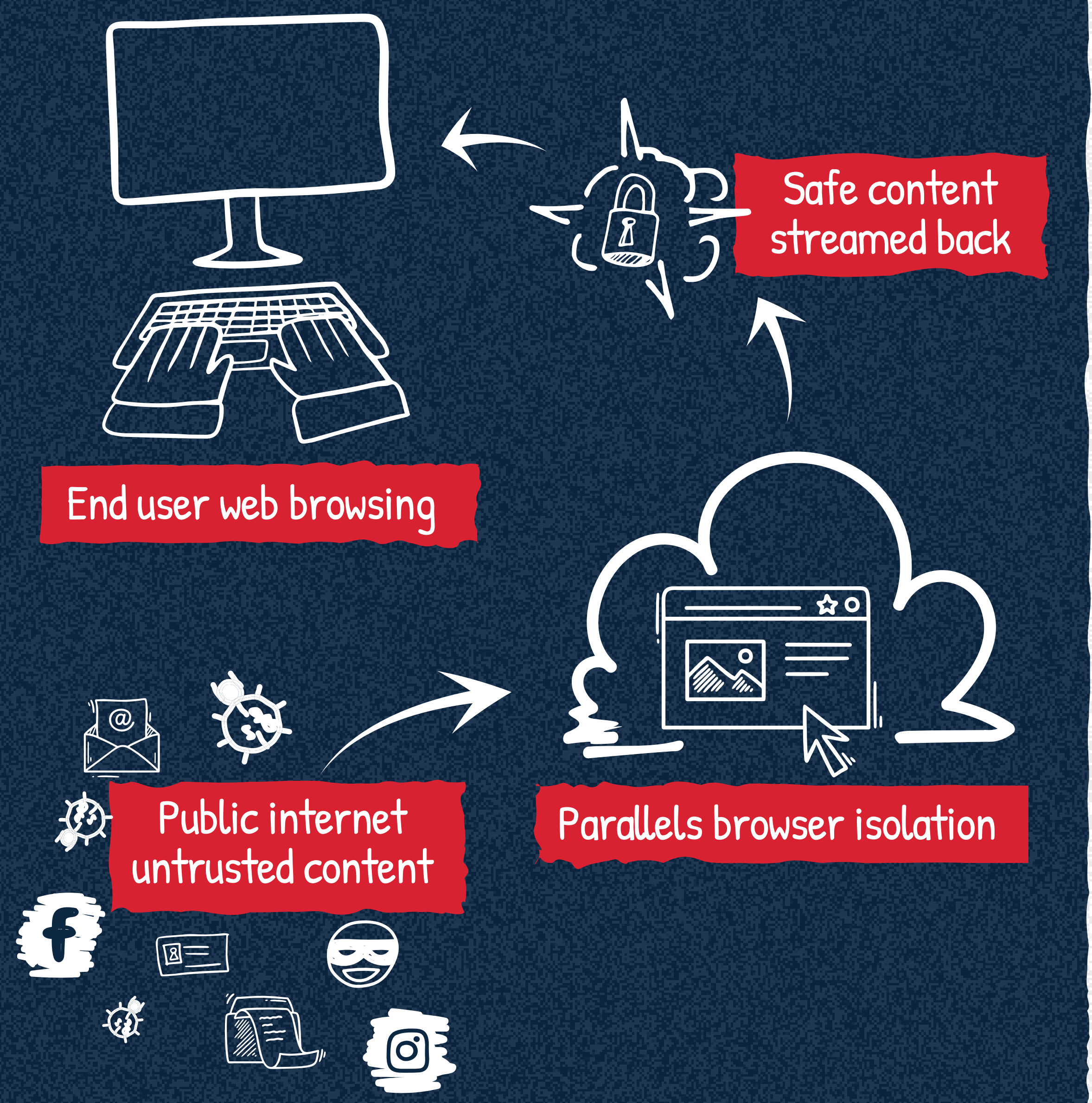
Secure web access with Parallels Browser Isolation

Parallels Browser Isolation is a secure, cloud-based web access solution that modernizes digital workspaces and addresses emerging cyber threats.

This technology streamlines secure browsing, providing essential defenses and facilitating easy access to web and SaaS applications.


Safe content streamed back
End user web browsing
Public internet untrusted content
Parallels browser isolation

Web browsing challenges

1. **Web security:** Organizations face significant risks from malware, ransomware, and phishing attacks originating from unsafe web browsing.
2. **Data breaches:** Sensitive data is at risk from potential web-based attacks, impacting compliance and customer trust.
3. **Compromised endpoints:** Endpoint devices are frequent targets for cyber threats, acting as gateways to organizational networks.
4. **Device and date risk:** Managed and unmanaged devices face risks from cyber threats and data leakage, compromising organizational security.
5. **Lack of transparency and control:** Organizations with remote/hybrid workforces may struggle with overseeing user activities and effectively enforcing security policies.

Benefits of Parallels Browser Isolation

1. **Customizable security:** PBI enables tailored security settings, including content filters and policy controls, based on user roles and domain permissions.
2. **Predictable costs:** Flat-rate, clear pricing for easy budgeting.
3. **A comprehensive solution:** The Parallels ecosystem includes a wide range of solutions for desktop, enterprise, legacy, SaaS, and web applications, boosting productivity and seamless integration.
4. **Real-time insights:** PBI delivers real-time and historical data on user and admin activities for informed decision-making.
5. **Seamless integration:** Compatible with leading external identity providers like Microsoft Entra ID, Okta, and Ping, simplifying user access management.

Key use cases for Parallels Browser Isolation

1. **SaaS app security:** Protecting data across public SaaS solutions.
2. **Security & compliance first:** Meet industry standards for protecting against web threats.
3. **Contractors and external vendors:** Secure, limited access to web resources or SaaS apps.
4. **Global collaboration and remote working:** Protected browsing from anywhere, using any device.

Parallels