FROST & SULLIVAN

EXTENDING ENTERPRISE SECURITY ARCHITECTURE VIA THE BROWSER

How an Enterprise Browser can better secure and enable work

FROST & SULLIVAN VISUAL WHITEPAPER

By Jarad Carleton, Global Research Director, Cybersecurity and Tony Massimini, Senior Industry Analyst, Information & Network Security

CONTENTS

Introduction to the Enterprise Browser

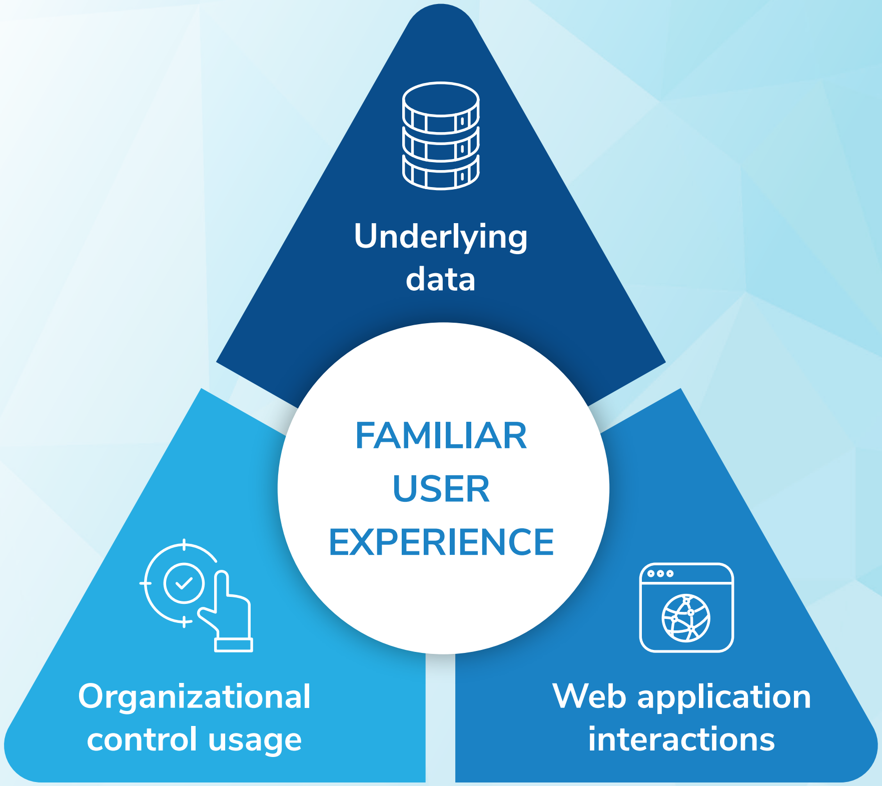
Today's web browser is a marvel of engineering: an elegant, simple, and powerful tool anyone can understand and use.

Thanks to its flexibility, capabilities, and ubiquity, the web browser utilizes a woven ecosystem of business technologies. However, managing the intersection of users, web applications, and the underlying data is difficult. Businesses need a web browser that takes a different approach than a consumer browser and delivers functions with the enterprise's needs in mind.

This new category of essential business tools is the Enterprise Browser. A successful Enterprise Browser will deliver a familiar user experience while empowering organizational control usage, web application interactions, and the underlying data. Web traffic commonly uses an encryption technology called Secure Sockets Layer (SSL), but SSL limits many inspection technologies. The Enterprise Browser maintains complete visibility of all interactions with content as a natural traffic termination point. Thus, browser-terminating encrypted traffic solves many problems with restoring full visibility.

The Enterprise Browser can function as your primary corporate browser to govern application usage, and it can be enforced and invoked only for critical applications; or, it can work alongside the consumer grade browser (such as Chrome). A browser built for the enterprise can live seamlessly alongside an existing browser.

ENTERPRISE BROWSER WILL EMPOWER:



Current browsers developed with consumers in MIND LACK THE VISIBILITY, CONTROL, and MANAGEABILITY that MODERN ENTERPRISES NEED for corporate Software-as-a-Service (SaaS) and web-based applications.

Main Concerns of a Chief Information Security Officer (CISO)

CISOs believe in the cybersecurity principle that good is not good enough. Employees spend most of their workday in a browser, accessing data and applications. The browser has become the new office and CISOs must ensure a balance between threat protection, data security, and cost.

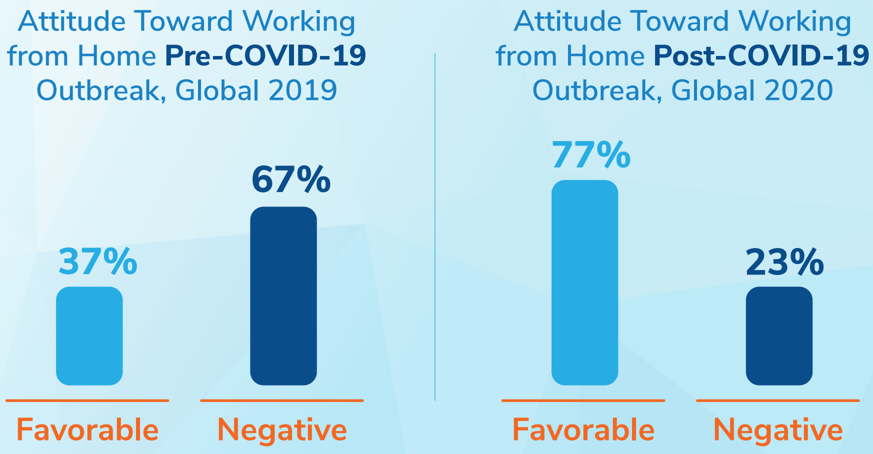
Rapid migration to the cloud and managing work from home (WFH) issues are primary enterprise issues

Organizations are migrating to the cloud as part of their digital transformations. The cost, time, and effort it will take to complement these existing investments with cloud-based services, including Secure Access Service Edge and Zero Trust Network Access, concerns CISOs.

The unprecedented transition to WFH between 2020 and 2021 requires organizations to rely on unmanaged personal devices and home networks that lack security hygiene and allow remote access to network resources. These challenges require enterprises to backhaul users with virtual private networks to protect cloud apps.

> 25% of organizations have indicated the shift to remote working is the BIGGEST BARRIER TO SECURITY.

THE PANDEMIC IS DRIVING A REVERSAL IN ATTITUDES TOWARD REMOTE WORK (GLOBAL, 2019–2020)



Attitude Toward Working from Home **Pre-COVID-19** Outbreak, Global 2019

Attitude Toward Working from Home **Post-COVID-19** Outbreak, Global 2020

Optimizing Expanding Users and Their Experiences Presents Security Challenges

Performance

The increasing number of users and the complexity of implementing many security solutions can impact performance. A solution must deliver in terms of data throughput rate and scalability. Backhauling all user traffic to secure it for remote users does not allow a native experience where users can go directly to a cloud app.

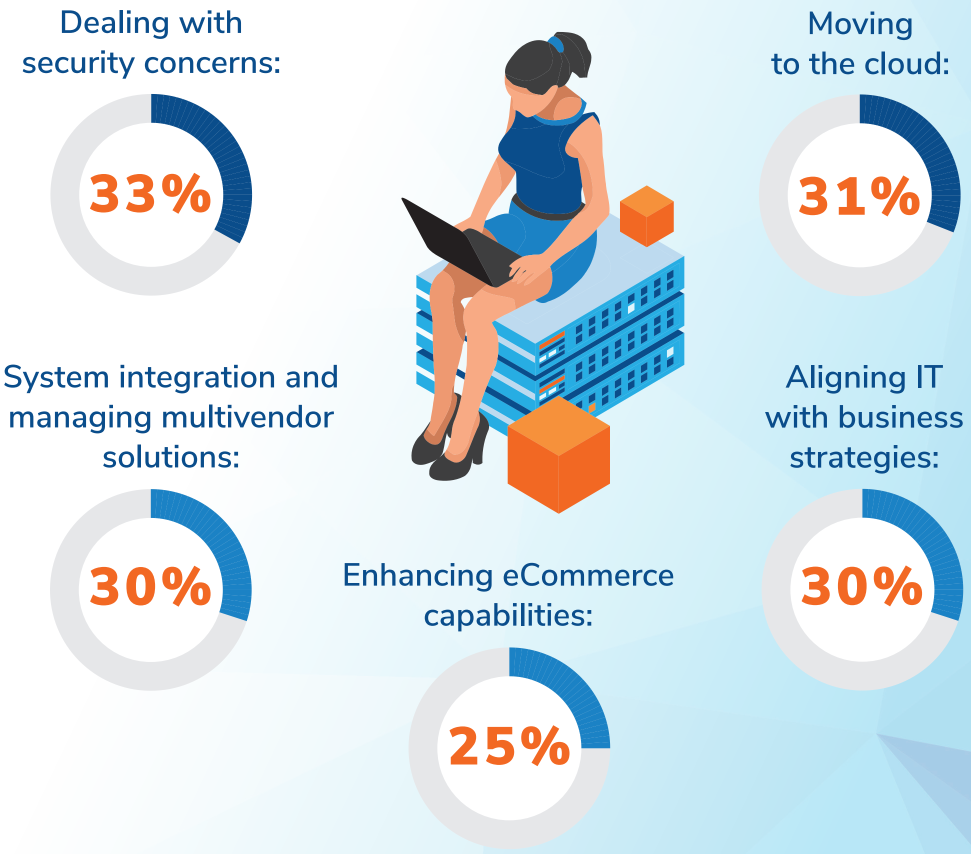
Organizations require instant scale to support traffic spikes or traffic from unexpected geographies. Large organizations have more at risk and more complex networks and internal structures than small to mid-market organizations. CISOs seek integrated solutions that will increase operational efficiencies while gaining a stronger, more comprehensive security system.

User experience

While securing business operations is important, it must not compromise productivity. CISOs want real-time threat detection and prevention. This is especially important when supporting remote and mobile users. CISOs are looking for seamless and frictionless security solutions. Users should be able to do their work with the Enterprise Browser without interruptions.

> CISOs are seeking **SEAMLESS AND FRICTIONLESS** security solutions.

TOP INFORMATION TECHNOLOGY (IT) CHALLENGES IN 2021



Survey Question: What will be the top 3 challenges your IT/Telecom department will face during the next 2 years?

Source: Frost & Sullivan 2021 Predictions—COVID-19 Accelerates CX Investments, February 2021. N=3,284 business and IT executives

Costs and Skill Shortages Dominating Operational Issues

Cost and integrating existing security solutions

CISOs must contend with the growing complexity of their security solutions and added costs to their ecosystems. They want to know how to evolve from just protecting web access to protecting all the different types of web applications and the corresponding internet-accessible data.

Shortage of skilled security personnel

A perennial shortage of qualified security personnel means organizations are resource-constrained. CISOs must examine if their current security tool investments comply with new policies and can be integrated with a broader cybersecurity tool ecosystem.

The increasing use of contracts and outsourcing inflates costs and risks access security.

Exacerbating the shortage of skilled IT workers, the "Great Resignation" of 2021 saw a record **47.4 million** **Americans leaving their employers.**

Source: US Bureau of Labor Statistics

Addressing Privacy, Government Regulations, and Compliance

Data's place in the cloud is affected by privacy concerns, government regulations, and regulatory compliance. Challenges are compounded by regularly changing laws and country-dependent data privacy regulations.

Key takeaways for CISOs

The browser has become a familiar, standard tool for accessing data and applications in the workplace. This can be leveraged for enhancing security as the Enterprise Browser.

CISOs must ensure a balance between threat protection, data security, and cost. The main drivers are performance and user experience. Security should not compromise productivity.

CISOs need a tailor-made enterprise browser that gives them the control to solve problems easily. The best browser fits a unique intersection of users, vital web applications, the underlying data, and the threat landscape.

CISOS MUST ENSURE A BALANCE AMONG:

Threat protection
Data security
Cost

Enterprise Browser Tackles IT's 2 Major Headaches

Headache #1: Accelerated Cloud Migration

Organizations have accelerated their migration to the cloud. Decentralized networks and more cloud applications are changing the way people work. Organizations continue to adopt cloud applications and storage and run more of their workloads from the cloud, thus inviting more threat vectors. They must be able to protect data and identify threats in SaaS applications. Threats that focus on web channels and the increased reliance on browsers to access applications are growing.

When working with a cloud-based service, an organization must be able to block or control access to one instance of a cloud service while allowing another. Granular policies based on the user and device profile are necessary.

The browser is a vital tool for corporate applications and services. However, the browser developed for the consumer market needs visibility, control, manageability, and governance. Organizations need additional security when users access applications through an ordinary browser.

Headache #2: Managing BYOD and BYOPC

Unmanaged devices challenge security teams, but bring your own device (BYOD) and bring your own personal computer (BYOPC) policies are often necessary organizational policies. Their implementation will only grow alongside the explosion of SaaS and an increasingly mobile and flexible workforce.

BYOD generally refers to PCs, tablets, or smartphones when the user is a contractor or another guest, whereas BYOPC refers to an organizational member's PC. These systems became prevalent when organizations needed to deploy WFH and had limited resources. It may not be possible to install an agent on these devices (particularly BYOD).

Providing an Enterprise Browser will allow remote workers and contractors to access network resources and manage security policies.

Cloud adoption will nearly double in 2022, from **42% of businesses to 85%.**

Of IT managers, **57%** say they **lack** in-house **cloud migration skillsets**.

Enterprise Browser Provides a Security Tool for IT Administrators

Security tool to alleviate shortage of skilled security personnel

Organizations need better security tools and automated systems to alleviate the shortage of skilled security personnel. IT administrators must ensure security for their organizations and cover a wide range of use cases by integrating and orchestrating several security solutions. This results in increased complexity and often security coverage gaps.

The web browser is a common element and is a woven ecosystem of technologies. IT administrators need to gain visibility and management of browser usage. Security personnel benefit from additional security tools specific to the web browser.

A robust browser management system provides a comprehensive set of tools that give IT granular analysis and the control to optimize web application use, compatibility, and security. Enterprise-class browser security tools will help protect sensitive enterprise data from security breaches and help IT administrators manage and secure browsers across networks.

ENTERPRISE-CLASS BROWSER SECURITY TOOLS WILL HELP:

Protect enterprise data from security breaches

Manage and secure browsers across networks

Leveraging Advanced Enterprise Browser Technology to Achieve Zero Trust Access (ZTA)

Managing a complex set of security solutions across a cloud environment

Organizations deploy various security technologies that are often complex, disconnected from one another, and (in many cases) have limited effectiveness. The shift to cloud resources has created risks when protecting vital resources.

The Enterprise Browser is a unique intersection point of organizational users, essential applications, and the underlying data. Administrators can more effectively protect any web application their organization uses by implementing a tailor-made browser.

The proper browser naturally integrates into an enterprise and enables the existing infrastructure to become stronger, more effective, more efficient, and completely secure. A browser that provides visibility, management, and granular policy controls achieves ZTA.

> A browser that provides **VISIBILITY, MANAGEMENT, AND GRANULAR POLICY CONTROLS ACHIEVES ZTA**.

TOP THINGS TO CONSIDER FOR A ZTA-DRIVEN STRATEGY:

- The Enterprise Browser establishes trust by assessing the posture of an installation device and dictating the appropriate policy depending upon the device type of the logged-in user.
- The Enterprise Browser ensures that advanced browser technology can manage access regardless of the device, user, network, or location.
- The Enterprise Browser can deliver last-mile control over any SaaS or internal web application anywhere with granular control.
- The Enterprise Browser gives CISOs infinite control over how users interact with information.
- The Enterprise Browser allows users to freely browse the internet with native protection from malware infiltration, credential harvesting, or data exfiltration.

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion

FROST & SULLIVAN