SURF

Join

Don't just browse, SURF.

THE PROBLEM

The first thing employees in the morning do is open a consumer-grade, unsecured browser.
As threats become more sophisticated, traditional security tools grow increasingly complex.
Cumbersome firewalls, VPNs, and a multitude of single-purpose solutions hinder productivity and
user experience. In their quest for safety, businesses often create friction, leading to compromised
data and a stifled workforce.
According to Gartner: 25% of enterprises will be using enterprise browsers by 2026, up from less
than 10% today. By 2027, it will be a central component of most enterprise super app strategies. By
2030, enterprise browsers will be the core platform for delivering workforce productivity and
security.

THE SURF SECURITY SOLUTIONS

Surf Security understands that true security doesn't exist at the network perimeter. It begins where
users and threats interact – the browser. Our innovative solutions reimagine cybersecurity by
focusing on protecting the individual user and their digital journey.

> Surf Security Enterprise Browser: A revolutionary browser built from the ground up with security
> at its core. It employs proactive threat detection, zero-trust access principles, and a familiar user
> interface. This combination empowers businesses to operate confidently and efficiently,
> especially for unmanaged devices where organisations cannot risk security gaps by using
> optionally removable extensions.
> Surf Security Extension: Our powerful extension transforms existing mainstream browsers into
> secure endpoints. It seamlessly integrates intelligent security layers, protecting users without
> disrupting their preferred browsing experience. Ideal for managed devices where corporate
> profiles can enforce the extension's use.

FEATURES	EXTENSION	BROWSER
Type of client	Managed	Unmanaged
BYOD Support	No	Yes
> **Advanced Protection**		
Dev Tools Access Control Limit usage of development tools in the browser for security purposes	Yes	Yes

FEATURES	EXTENSION	BROWSER
Just-in-Time (JIT) Access Management Reduce Browser based zero day vulnerabilities	No*	Yes
ADMX Rules	No*	Yes
Domain Age Verification Limit access to websites based on their domain registration date	Yes	Yes
Weak Password Alert Check password strength during registration and send an alert for weak passwords	Yes	Yes
Malicious Processes Disarm Define custom list of authorised processes	Yes	Yes
Safe Browsing Control Decide whether to scan untrusted sites or bypass the checking process altogether	Yes	Yes
IFrame Content Script Control Controls whether content scripts will be executed within IFrames	Yes	Yes

> **Audit**

	EXTENSION	BROWSER
Alert Tracking Track alerts for security incidents	Yes	Yes
Malware Tracking Track malware incidents	Yes	Yes
Performance Tracking Track browser performance metrics	Yes	Yes
Navigation history Track user navigation history	Yes	Yes
AI tools usage Track usage of AI tools	Yes	Yes
Application Statistics Reports Track application usage and ShadowIT	Yes	Yes
Multi-Factor Authentication (MFA) Enforcement Require multi-factor authentication at login	Yes	Yes
Transactional MFA Enforcement Require multi-factor authentication on selected pages	Yes	Yes
Session Duration Limit	Yes	Yes
Personal Credential Controls Control the usage of personal credentials for authentication	Yes	Yes
Auto-Hibernate Logout Enforcement Set maximum idle time for user disconnect	Yes	Yes

FEATURES	EXTENSION	BROWSER
Passwordless Login Leverage RPA for passwordless login	Yes	Yes
Keylogging Protection	Yes	Yes
Login Enforcement Enforce authentication after browser restart or IDP/App logout.	Yes	Yes

> **Bookmark Management:** Browser Extension Controls

	EXTENSION	BROWSER
Allow list	Yes	Yes
Extension Risk Scoring	Yes	Yes

> **Browser Monitoring**

	EXTENSION	BROWSER
Session Recording	Yes	Yes
Application Usage (including ShadowIT)	Yes	Yes

> **Data Loss Prevention (DLP) Controls**

	EXTENSION	BROWSER
Copy Protect from copying content	Yes	Yes
Paste Protect from pasting content	Yes	Yes
Print Protect from printing content	Yes	Yes
View Source Code Protect from viewing the source code	Yes	Yes
Cross Browser Redirect Enabled Redirect users to the SURF browser for accessing content with unsupported policies	Yes	Yes
Watermark Apply a customisable watermark to the user's view	Yes	Yes
Database Injection Block Database injection in input fields	Yes	Yes
PII Masking Customisable PII masking based on Regex	Yes	Yes
Email Sending Controls (Office 365) Limit permissible domains for outbound emails using the web version of Office 365	Yes	Yes
Upload Management Restrict file uploads	Yes	Yes

FEATURES	EXTENSION	BROWSER
Sensitive Data Anonymization Anonymize sensitive data on specific applications	Yes	Yes
GenAI Character Limit Limit the number of characters a user can copy, paste, and type within GenAI	Yes	Yes
Read only WebSites Disable user interactions, including clicks and keyboard inputs	Yes	Yes
DLP recording Capture screenshot on selected actions	Yes	Yes
Screen Capture Prevention Block screen capture from the device	Yes	Yes

› **Device Compliance Enforcement**

FEATURES	EXTENSION	BROWSER
AV Detection Check for antivirus on the device	Yes	Yes
Disk Encryption Check for active disk encryption on the device	Yes	Yes
Registry Keys Check for specific registry keys in device	Yes	Yes
File-Exists Check for specific files on the device	Yes	Yes
Certificates Check for specific certificates on device	Yes	Yes

› **Download Management**

FEATURES	EXTENSION	BROWSER
Corporate Storage Enforcement Download files to company's remote storage	Yes	Yes
Download Restrictions Set restrictions based on file types and web pages	Yes	Yes
File Download Alert Notify when for files are downloaded	Yes	Yes
Download File Encryption Choose file types for automatic encryption upon download	Yes	Yes
Web scraping Block data scrapping from web pages	Yes	Yes
Download Malware Scan Automatically scan downloads for malware threats	Yes	Yes

FEATURES	EXTENSION	BROWSER
› **Phishing Protection**	Yes	Yes

FEATURES	EXTENSION	BROWSER
Protection Method Set phishing policy protection methods	Yes	Yes
Protection Scope Set coverage areas for the protection methods	Yes	Yes
› **Proxy Access Management** Route global traffic or specifc applications via a proxy	Yes	Yes
› **Session Kill Switch** Block user session and clear all session data	Yes	Yes

› **Web Content Filtering**

	EXTENSION	BROWSER
Access Request Define if the user can request access to blocked content.	Yes	Yes
Category-Based Web Filter Control access by content categories	Yes	Yes
Custom Rules Control access by manual definitions	Yes	Yes
Keywords Filtering Restrict access based on specific keywords	Yes	Yes

KEY BENEFITS
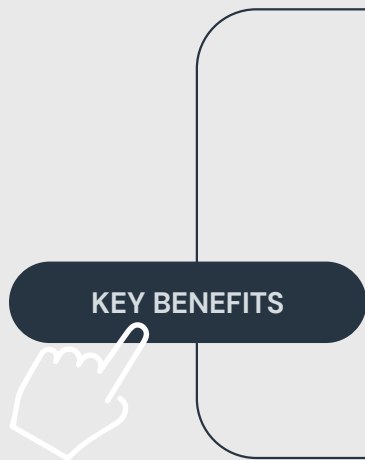
› **ZERO Trust Security:**

Secure & protect your users from inside the browser.

› **ZERO infrastructure costs:**

No Proxy or cloud infrastructure required.

› **ZERO performance impact:**

Faster than any enterprise and most consumer browsers.

› **ZERO Trust Browser & Extension:**

Chromium-based for a private & familiar user experience.

› **Security-Conscious Organizations:** Industries handling sensitive data (finance, healthcare, government) in need of robust protection without hindering operations.

› **Productivity-Driven Businesses:** Companies looking to enhance collaboration, enable remote work, and drive agility with security as an enabler.

› **IT-burdened Teams:** Organizations seeking to reduce security tool complexity and empower users to work safely.

* Can be configured via the MDM solution for managed devices

Contact Surf Security Today

Join the secure browsing revolution.