SURF Security Zero Trust Enterprise Browser® & Extension

INDEX

SURF Security
Zero Trust
Enterprise Browser®
& Extension
Sales Brochure

Introduction

Enterprise security teams are on the back foot. A cybercrime underground worth trillions annually[i] provides malicious actors with all the tools and knowledge they need to launch sophisticated attacks, a long with a readymade market for the sale of stolen data. One vendor blocked over 161 billion attacks[ii] in 2023 alone.

Many more will slip under the radar as the same organisations struggle to enforce policy across a heterogenous set of remote working endpoints – including personal devices which may be missing anti-malware protection and the latest software updates. Limited IT budgets and cyber skills shortages compound the challenge. The world is short of four million cybersecurity professionals, by one estimate[iii].

"Ransomware has become an existential threat for some companies, impacting an estimated **75%** of organisations"

The business risks are real[iv]. The average cost of a data breach today is nearly $4.9m[v]. But aside from the direct costs, serious security breaches take an unquantifiable reputational toll in customer churn and erosion of brand value. Ransomware has become an existential threat for some companies[vi], impacting an estimated 75% of organisations[vii].

Against this backdrop, IT and security leaders need a new approach to endpoint security—a more reliable, consistent way to enforce policy, meet regulatory compliance requirements and effectively mitigate cyber risk. But one that will enable them to consolidate and streamline existing controls, without needing to radically rethink security posture. They need a zero trust enterprise browser.

"One vendor blocked over **161 billion** attacks in 2023 alone."

"The world is short of **4m** cybersecurity professionals, by one estimate"

"The average cost of a data breach today is nearly **$4.9m**."

Why your business needs SURF

The potential risks to any enterprise are significant, but key stakeholders within an organisation are concerned with specific issues.

CIO: The post-pandemic distributed workforce presents many challenges. You're looking for ways to optimise employee productivity and streamline workflows in as cost effective and secure a manner as possible. That's especially true at a time of budget tightening and persistent economic uncertainty.

Your go-to solution might be a Secure Access Service Edge (SASE) platform, which combines SD-WAN, secure web gateway, firewall-as-a-service, zero trust network access and cloud access secure broker (CASB) technology. SURF can provide all of that functionality and more, in a way that's more efficient, cost-effective and easy-to-deploy.

"SURF will enforce posture checks, limit malicious and negligent behaviour, and protect users from third-party threats."

CISO: Endpoint security continues to evolve, with major implications for enterprise cyber-risk management. In a world where remote workers are no longer the exception, it becomes increasingly challenging to ensure consistency of policy enforcement across managed and unmanaged endpoints. When employees are logging on to cloud resources remotely, how can you ensure the device they're using is secure?

SURF is the answer. By ensuring all employees log on from a zero trust enterprise browser, it doesn't matter what device they're using, SURF will enforce posture checks, limit malicious and negligent behaviour, and protect users from third-party threats.

DPO: Your business operates in an era of potentially huge fines and the threat of reputational damage hanging over every security incident. Malicious actors have a wealth of tactics, techniques and procedures (TTPs) at their disposal to breach networks and find customer and employee data stores.

SURF offers several layers of protection at the endpoint—to keep bad stuff from getting in and important data from leaking out. SURF's Zero Trust Enterprise Browser can also help mitigate risks stemming from employees, offering defence-in-depth to stop social engineering in its tracks. And in the worst-case scenario, the implementation of SURF into your security stack shows regulators that you have put in place appropriate technical safeguards.

A new endpoint for a new era

> "SURF is designed for the modern, distributed workplace. 99% of threats come from the internet and employees access corporate resources via work and personal devices."

SURF offers a range of benefits over traditional endpoint/network-layer security solutions, which tend to redirect employee traffic to the vendor's back-end cloud systems for decryption and inspection. This adds extra cost and latency, and potential security coverage gaps if there are cloud outages.

SURF is designed for the modern, distributed workplace. A place where 99% of threats come from the internet and employees access corporate resources via work and personal devices. In this context, it makes far more sense to secure the browser, which is the conduit for almost all employee activity. SURF scans and protects before threats can even execute. It's a faster and smoother experience, with no cloud-based, single point of failure. And it works with any device – whether managed or unmanaged – providing a sandbox environment to protect all company resources without the need to deploy hardware-based endpoint security.

SURF doesn't enhance endpoint security. It is the secure endpoint.

SURF puts your business back in control, by monitoring every interaction between users and applications running through the browser, detecting and preventing security breaches and providing security teams with centralised visibility and control over key policies. Users authenticate on startup, with access to corporate resources and SaaS/on-premises apps controlled based on identity and device posture. Copy, paste, print and screen-share privileges can be enabled or revoked in a few clicks, and files for download can be encrypted, watermarked and scanned for malware.

Zero trust, maximum protection

Sensitive personal, business and customer information can be masked as it renders on the page and prevented from being pasted into GenAI and other apps. Strict policies and permissions can be used to prevent unauthorised access, transfer or modification, while audit logs/reporting accelerate breach response. The environment within the browser is sandboxed to guard it from malware, ransomware and other local/web-based threats on the endpoint. Even deepfake audio can be flagged as fraudulent. All traffic is encrypted end-to-end to protect data in transit.

Securing a distributed workforce

Your remote and home working employees face cyber risk on all sides. Here's where the attack surface is most exposed, and how SURF can help:

Vulnerability exploitation: Unpatched corporate and personal (unmanaged) devices represent an acute threat for organisations given their access to company data and resources.

- SURF offers just-in-time access management to mitigate browser-based zero-day vulnerabilities.

Social engineering: Most breaches last year involved a "non-malicious human element", meaning an employee made an error or fell victim to a social engineering attack. Phishing and BEC attacks are the main risks.

- SURF eliminates social engineering threats through multiple checks and whitelisting, including web reputation, SSL certificate and trusted domain checks.

Stolen or guessed credentials: Credentials were the top initial action type in data breaches last year.

- SURF enforces multifactor authentication and passwordless logins, and flags when weak passwords are attempted on registration.

Supply chain risk: Third-party software may contain malware and vulnerabilities, while individuals including contractors may expose the organisation through unprotected devices and weak credentials.

- SURF offers easy-to-use zero trust-focused controls for user authentication and device posture. It enforces customised security and control policies for every type of contractor role, network access point, and device without affecting productivity, ensuring devices are free from malware.

Malicious content: Malware is everywhere and could be downloaded unwittingly by employees onto their devices, putting corporate assets at risk.

- SURF blocks malware downloads and supports granular web content filtering.

Malicious insiders: Breaches stemming from deliberate malice rather than employee negligence are more expensive to remediate and harder to detect.

- SURF monitors for suspicious employee activity and provides a session kill switch.

Enhance and replace your existing security

SURF works to simplify and consolidate your security stack into a single, optimised security tool. It brings together:

Web isolation: An isolated work environment on the endpoint itself. Local browser isolation (LBI) replaces traditional, cloud-based remote browser isolation (RBI).

MDM for browser: Eliminates the need for an additional device management tool.

Web filter: Category-based filtering within the browser.

Web DLP: Because everything is happening inside the SURF browser, it can monitor every click and prevent data leakage.

VDI replacement: Providing continuous, high-performance, friction-free and secure access to all SaaS and on-premises applications—eliminating the need for VDI.

VPN replacement: Via a proxy from within the browser, SURF provides more granular control over traffic than a traditional VPN.

SaaS visibility and discovery: CASB-like ability to show what users are doing in the browser, what apps they're using and navigation history.

Web and malvertising: Protects against phishing based on web reputation and whitelisting, and blocks use of company/personal credentials.

Extension management: SURF can control what browser extensions users install.

LLM security: Blocks uploads of sensitive data into apps like ChatGPT.

Beyond SASE

At a time when the corporate attack surface continues to expand, SASE helps many organisations to mitigate cyber-risk in a scalable and relatively simple manner. But it's not a silver bullet. SURF can help organisations achieve the same benefits and go beyond, in a more affordable, easier-to-implement and simpler-to-use way.

SURF offers several enhancements over SASE, most notably:

Disaster recovery

SURF supports user productivity and maintains protection even during SASE outages.

Hosting

SURF offers a more seamless experience than SASE (which is cloud based) thanks to an edge compute-based model, with no reliance on cloud except for policy updates.

Unmanaged devices

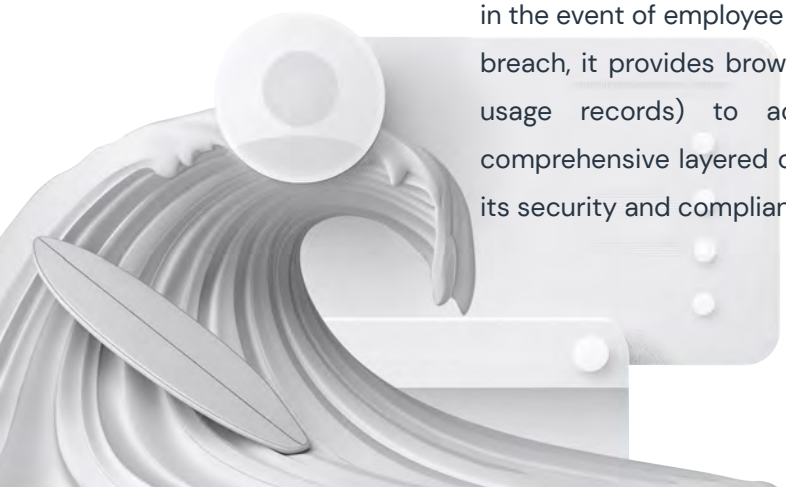
SASE only works on managed devices, whereas the browser-based SURF works across managed and unmanaged devices.

Supporting data privacy and compliance

Organisations are buckling under the weight of multiple regulatory mandates – from NIS2 and HIPAA to GDPR. But SURF supports industry best practices that cut across many of these regulations, by controlling:

- What employees can access and download
- Who is authenticating
- What data can leave the organisation
- Device security posture

SURF provides an extra set of eyes, ears and controls to mitigate compliance risk in the event of employee negligence or malicious behaviour. And in the event of a breach, it provides browser monitoring (session/DLP recording and application usage records) to accelerate remedial action. For regulators, SURF's comprehensive layered controls provide assurance that your organisation takes its security and compliance obligations seriously.



Keeping end users happy

Too often, security is the enemy of productivity. Almost half (48%) of younger workers claim corporate tools are a hindrance . SURF is different. The SURF enterprise browser is built specifically to make the user experience better, without compromising on security.

SURF monitors user activity in the background, blocking malicious content and preventing risky behaviour that breaks policy. But otherwise, it allows employees to work as normal. And because it's based on Chromium, there's no need for them to learn a new UI or modify their workflows. A familiar look and feel puts users at ease. And it works across all devices, whether managed or unmanaged. It's also significantly faster and more responsive than traditional VDI or VPN infrastructure.

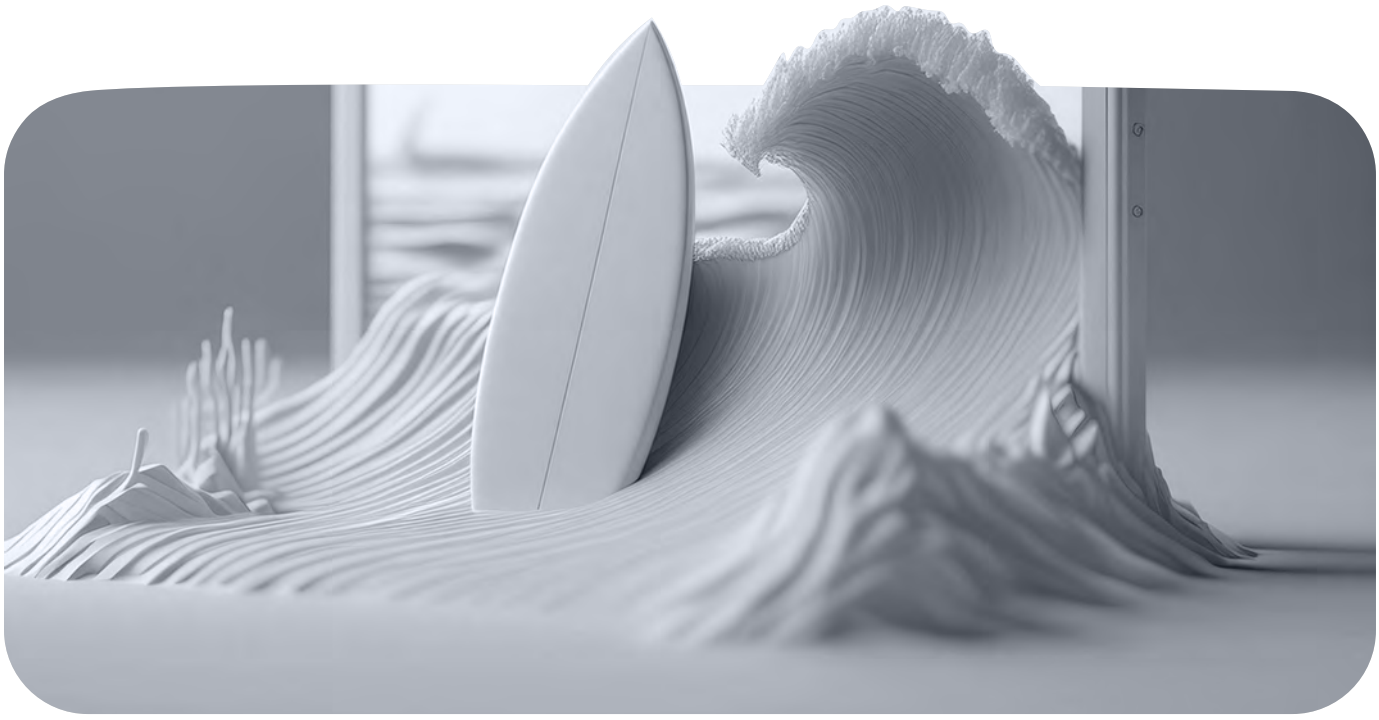
Getting started with SURF

SURF is simple to deploy.

1. **For managed devices:** Deploy the browser extension via your preferred MDM.

2. **For unmanaged devices:** Invite users via the admin portal. They will receive an automated email to download SURF like any other browser.

Once the browser is downloaded, users simply authenticate and they will be presented with a personalised view according to company policy and role. Admins can manage SURF across all users from a centralised cloud-based portal. (There's also an option to host in their own datacentre).



Keeping end users happy

Enterprise browsers are gaining significant traction in enterprise security. But not all products are created equal. Here's what to look for:

Policies

Configurable down to a single user level or group, applicable globally, and supporting Role-Based Access Controls (RBAC). Recommended policies available based on real-world user behaviour.

Traffic filtering

Supports rich media such as images, videos and documents. Blocks traffic by country, expressions, keywords and binary patterns.

Traffic inspection

Inspects all traffic before encryption and before leaving the browser. Filters content based on domain, URL, contents, and keywords and alerts on C2 traffic, obfuscated traffic and data exfiltration.

URL filtering

Based on categories and domains.

Transit encryption

Ensures all data-in-transit is encrypted.

Intrusion detection/prevention

Realtime, inline detection/blocking of malicious content and prevents malicious content from accessing resources.

Endpoint security

Blocks malicious processes and scripts; scans downloaded files with multiple malware engines. Executes files for inspection in sandbox for isolation. Ability to kill session and revoke user access if account is compromised.

Data loss prevention

Blocks copy / paste and screenshots. Prevents sensitive data download, uploads and transfers. Blocks / obfuscates sensitive data. DLP policies can be customised based on user's role, group, location etc.

Identity and access management

SAML/Active Directory integration. Support for multifactor authentication (MFA), Single Sign-On and password managers. Can import policies from IAM solutions.

Visibility and monitoring

Session recording, compliance reports and admin dashboards. Visibility into URLs accessed, downloads / uploads and private sessions.

Anomaly detection

Baseline behaviour profiles and abnormal behaviour detection based on time of day, location, URLs accessed, keystroke cadence, downloads and more.

Threat intelligence

Integration with variety of IP, domain and file reputation services.

Social engineering

Detects and blocks access to known phishing sites, and heuristic analysis to detect new social engineering attempts.

Malware protection

Scans for and blocks malicious content including downloads.

Man-in-the-Middle (MitM)

Ensures secure connections and monitors for suspicious activities indicating MitM interception.

Web filtering

Blocks access to inappropriate/harmful websites.

Anonymisation

Protects browsing activity data from being tracked and/or exposed.

Deepfake detection

Capabilities to flag use of voice generation software and stop fraud and misinformation in its tracks.

Use cases

GenAI security

Managed and unmanaged device support

Contractors

VDI (Virtual Desktop Infrastructure) replacement

VPN replacement

RBI (Remote Browser Isolation) replacement

Distributed workforce protection

Endpoint protection

Social engineering protection

Compliance

Insider threat & cyber espionage

Helpdesk support

FAQ section

Keen to find out more?
The following may help to answer any burning questions:

What's the difference between an enterprise browser and SASE?

An enterprise browser focuses on securing web browsing activities at the endpoint level. It provides a controlled environment for users to access the internet with features like centralised management, content filtering, and data loss prevention.

SASE, on the other hand, is a typically a cloud-delivered architecture that converges networking and security services and is less tailored to protecting the endpoint/clients. The SURF Security Enterprise Zero Trust browser provides the same or better capabilities than endpoint-SASE solutions

Do I still need anti-virus/malware on my endpoints?

Malware and viruses can infect your computer via many methods, including USB drives, the network, and other browsers. So it is recommended. In fact, SURF's Policies can be tailored to only run the browser if the right protections are in place.

Do I still need to use a VPN solution?

This is up to the network administrator.

Why is an enterprise browser better than a browser isolation solution?

An enterprise browser stands out as a superior choice over browser isolation solutions, mainly because it sidesteps the pitfalls of remote infrastructure dependency, offering improved performance with reduced latency and costs. Additionally, it offers stronger integration possibilities with Zero Trust security models, enabling granular access control and proactive threat detection.

Why deploy a full enterprise browser and not an extension?

A full browser is the best choice for unmanaged devices, whilst we recommend that managed devices use the extension.

Does an enterprise browser integrate with SIEM solutions or similar?

Yes, enterprise browsers often integrate with SIEM (Security Information and Event Management) solutions or similar log aggregation and analysis platforms. This integration enables organizations to collect, centralize, and analyse security-related events and logs generated by the browser, providing valuable insights into user behaviour, potential threats, and security incidents.

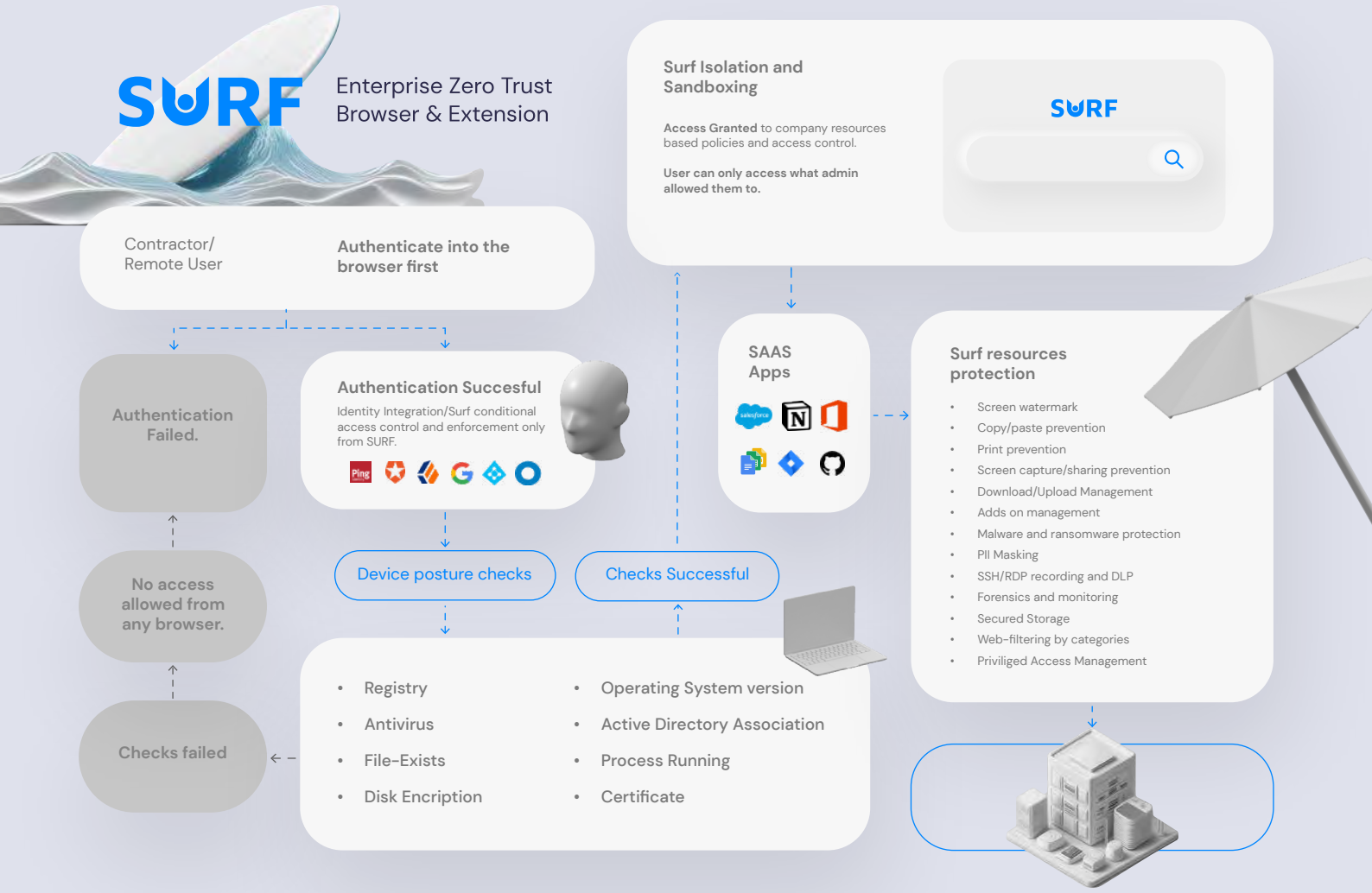
Can you disconnect users at the click of a button?

Yes, our 'Kill Session' feature is design for just this purpose.

Appendix

Other relevant documents

- LinkedIn Company Page
- Compliance Paper
- SURF Security Browser & Extension Features
- Zero Trust, Zero Fear Whitepaper
- Say Goodbye to VDI Paper
- GenAI Paper
- Stats & Facts Infographics
- How does Surf Work- Infographic
- LinkedIn Newsletter
- www.surf.security



The Surf Security Solutions

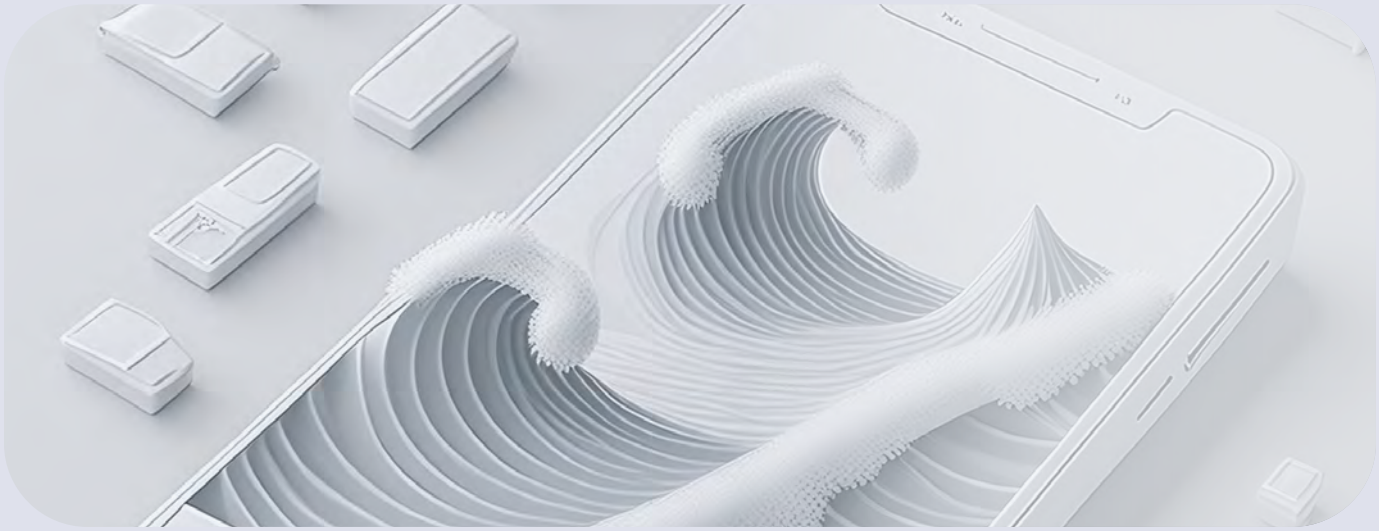
Surf Security understands that true security doesn't exist at the network perimeter. It begins where users and threats interact – the browser. Our innovative solutions reimagine cybersecurity by focusing on protecting the individual user and their digital journey.

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
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

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

FEATURES	EXTENSION	BROWSER
Type of client	Managed	Unmanaged
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
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		
Allow list	Yes	Yes
Extension Risk Scoring	Yes	Yes
› Browser Monitoring		
Session Recording	Yes	Yes
Application Usage (including ShadowIT)	Yes	Yes
› Data Loss Prevention (DLP) Controls		
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

FEATURES	EXTENSION	BROWSER
Type of client	Managed	Unmanaged
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
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 screenshots on selected actions	Yes	Yes
Screen Capture Prevention Block screen capture from the device	Yes	Yes
› Device Compliance Enforcement		
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		
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

FEATURES	EXTENSION	BROWSER
Type of client	Managed	Unmanaged
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
› Phishing Protection	Yes	Yes
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 specific applications via a proxy	Yes	Yes
Session Kill Switch Block user session and clear all session data	Yes	Yes
› Web Content Filtering		
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

Founded in London, UK in 2022, SURF Security is an endpoint protection Browser-SASE (secure access service edge) cybersecurity company that has created the world's first enterprise zero-trust browser and extension with security at its core. These two products capitalise on the rise of both the working-from-home phenomenon, and 'software as a service' or SaaS platforms that are used through a browser. SURF secures the browser itself, either replacing or augmenting consumer browsers such as Chrome, Edge, or Safari. This approach helps ensure compliance, defends organisations from breaches and protects users from social engineering attacks such as phishing—all on the user's device. **www.surf.security**

- https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
- https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/calibrating-expansion-2023-annual-cybersecurity-threat-report
- chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
- https://www.idtheftcenter.org/publication/2023-data-breach-report/
- https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
- https://www.bbc.co.uk/news/uk-england-northamptonshire-66927965
- https://www.infosecurity-magazine.com/news/75-orgs-ransomware-2023-1/#:~:text=Three%2Dquarters%20(75%25)%20of,t%20experience%20any%20ransomware%20attacks.
- https://threatresearch.ext.hp.com/wp-content/uploads/2021/09/HP_Wolf_Security_Rebellions_and_Rejections_Report.pdf