Closing the Microsoft Defender Browser Security Gap

Enforcing URL-level threat intelligence blocks outside of Edge across all platforms, operating systems, and ecosystems.

THE DEFENDER SECURITY GAP

Microsoft Defender for Endpoint reliably enforces granular, URL-level threat mitigation **only within Microsoft Edge** When users or external contractors migrate to alternative browsers, sessions become unprotected because network-level TLS encryption masks full URI visibility.

Standard network-layer components can only inspect top-level domains [cite: 3]. This leaves your SOC blind to subdirectories and precise attack paths, rendering strategic investments in Microsoft Threat Intelligence completely ineffective once an active workspace moves away from Edge.

THE CYBEREINFORCE ADVANTAGE

Cybereinforce functions as a native browser extension to close this Defender gap natively.By operating where the traffic is fully decrypted, it dynamically bridges policies across your complete software and contractor ecosystem:

- **Universal Engine Compatibility:** If a browser is Chromium-based and permits web extensions, Cybereinforce guarantees protection.
- **Bypassing the 15,000 IOC Ceiling:** Seamlessly offloads heavy URL indicator databases to tenant-level Cybereinforce hosting, preserving native Defender capacity for file/IP indicators.
- **Customized Governance:** Allows enterprises to define personalized brand identity templates with custom `blocked.html` landing files.

PROACTIVE THREAT INTELLIGENCE LAYER

Beyond immediate custom tenant indicators, Corporate+ plans include a dynamic armor layout protecting endpoints from over **500,000 known malicious domains** and **100,000 targeted URLs** without taxing manual SOC input.

Deployment: Installs via MDM in under 10 minutes. Devices securely onboard via `cybereinforce.com/join` using hostnames for telemetry heartbeat signals.

CROSS-PLATFORM SUPPORT ARCHITECTURE

Operating System	Supported Fleet / Extensions
Windows, macOS, Linux	All Chromium-based browsers, Firefox
macOS (Native Desktop)	Safari, Firefox, All Chromium Frameworks
iOS & iPadOS	Safari Native Extension
Android	Firefox Mobile Extension

SOC VALUE & ECOSYSTEM INTEGRATION

- **Defender Integration:** Automatically synchronizes rules to ingest Indicator of Compromise (IOC) matrices in real-time
- **Microsoft Sentinel Ingestion:** Automatically generates investigation-ready incident structures inside the existing tenant workspace via the custom `CybereinforceCTE_CL` data pipeline
- **Supply-Chain Protection:** Enforces enterprise policies inside partner, consultant, or third-party browsers without requiring full tenant migration or endpoint takeover

COMPLIANCE MATRIX

Standard	Controls Met & Regulatory Impact
ISO 27001	A.5.9, A.5.23, A.8.7 (Malware), A.8.15, A.8.20 (Web)
NIS2	Proactive supply-chain risk reduction & attack discovery
DORA	ICT risk reduction via deterministic URL protection
SOC2	Fulfills CC6.1 (Logical Access) & CC7.3 (Detection)

✓ **ISO/IEC 27001 Certified SaaS Operations**

EVALUATION MATERIALS & TECHNICAL VALIDATION

PoC Demonstration	Produktvorstellung	Threat-Intel Case 1	Threat-Intel Case 2
Video Walkthrough	**Technical Deep-Dive**	**Attack Path Block**	**Automated IOC Sync**