CYBEREINFORCE

WHITEPAPER

Closing the Browser Enforcement Gap.

How Cybereinforce extends Microsoft Defender-grade threat intelligence — and stands alone where Defender isn't present — across every browser, every operating system, and every team that depends on it.

August 2026 · Cybereinforce Threat Enforcement, a Cybeurope product

Enforcement has to happen where the URL is still visible.

Every organization that relies on Microsoft Defender for Endpoint has already made the right investment in threat intelligence. The problem this whitepaper documents isn't a gap in that intelligence — it's a gap in where it gets *enforced*. Microsoft's own documentation confirms that full URL-path blocking is a Microsoft Edge-specific capability: outside Edge, Defender's Network Protection component can only ever see the domain a browser is connecting to, never the path or query string, because that detail stays encrypted inside the TLS session until it reaches the browser itself.

Cybereinforce closes that gap with a native browser extension that enforces the same indicator policy — Defender-sourced or Cybereinforce's own curated threat feed — at the one point the full URL is still visible: inside the browser, before the request is ever sent. The result is one enforcement engine that serves five distinct audiences without five different products.

Edge-only	**5 browsers**	**5 frameworks**	**< 10 min**
Where Defender enforces full URL paths, per Microsoft Learn	Chrome, Edge, Firefox, Safari, Chromium — one policy	ISO 27001, NIS2, NIST CSF, DORA, SOC 2 evidenced by one control	Time to first protected device

✓ Who this is for

01

Defender & Sentinel teams

Close the Edge-only enforcement gap and offload volume beyond the 15,000-indicator ceiling — without replacing anything already deployed.

02

Small & growing businesses

Enterprise-grade browser protection with no SOC, SIEM, or existing Microsoft stack required — Cybereinforce ships its own curated threat intelligence.

03

MSPs & MSSPs

A new managed revenue line, structured as Pay-As-You-Go revenue share or prepaid Credits with a locked-in discount.

04

Compliance & audit teams

One enforced control that produces standing evidence across ISO 27001, NIS2, NIST CSF 2.0, DORA and SOC 2.

05

Mobile & IT fleet teams

The same policy extended to iOS Safari and Android Firefox — no separate mobile product or SKU.

What Microsoft's own documentation confirms.

Defender for Endpoint's custom indicators can block a specific URL path — not just a domain. Microsoft is explicit that this level of precision is Edge-specific:

> "HTTPS URL paths will only be matched in Microsoft Edge; HTTP URL paths can be matched in any browser."
>
> **— Overview of indicators in Microsoft Defender for Endpoint, learn.microsoft.com/en-us/defender-endpoint/indicators-overview**

Outside Edge, enforcement falls to **Network Protection**, which inspects traffic at the network layer — below the browser, after encryption has already begun:

> "In non-Microsoft Edge processes, Network Protection determines the fully qualified domain name for each HTTPS connection by examining the content of the TLS handshake... This requires that the HTTPS connection use TCP/IP (not UDP/QUIC) and that the ClientHello message not be encrypted."
>
> **— Use network protection to help prevent connections to malicious sites, learn.microsoft.com/en-us/defender-endpoint/network-protection**

In practice: Network Protection reads the hostname from the unencrypted ClientHello/SNI field before the encrypted session begins. The URL path and query string travel *inside* that encrypted session and are invisible to any network-layer control. Microsoft's Web Content Filtering documentation states the consequence directly: **"full URLs are not available in third-party browsers."**

Two further conditions narrow enforcement even for domain-level blocking outside Edge: QUIC and Encrypted Client Hello must be disabled in the browser (otherwise even the domain is encrypted from view), and Network Protection must be explicitly running in **block mode** — audit mode or default-off leaves non-Edge browsers unprotected. On macOS and Linux, Edge itself "only integrates Web Threat Protection," narrowing the gap further still.

Separately, the entire indicator system has a hard ceiling:

> "There's a limit of 15,000 indicators per tenant. Increases to this limit aren't supported."
>
> **— Overview of indicators in Microsoft Defender for Endpoint, learn.microsoft.com/en-us/defender-endpoint/indicators-overview**

An organization can be fully invested in Defender P1/P2, Sentinel, and curated threat intelligence, and still lose URL-level enforcement the instant a user opens Chrome, Firefox, or Safari — not from a licensing gap, but a structural one in where the enforcement point sits.

Enforce at the one point the URL is still visible.

Cybereinforce is a native browser extension. It doesn't sit on the network, and it doesn't wait for a TLS handshake to guess at a hostname — it enforces policy inside the browser process itself, where the full request, path and query string included, is available before it's ever sent.

1 Sync or self-source

Ingest an existing Defender IOC policy in real time, or run entirely on Cybereinforce's own curated feed of 500,000+ known malicious domains and 100,000+ targeted phishing URLs — no Microsoft stack required to start.

2 Enforce in-browser

The extension blocks the full URL — path and query string included — the moment it's requested, on any Chromium-based browser, Firefox, or Safari, on desktop or mobile.

3 Report everywhere

Every block is logged with device, user and timestamp. Events push to Microsoft Sentinel via the CybereinforceCTE_CL pipeline, or export directly for organizations without a Sentinel workspace.

✓ Coverage

OPERATING SYSTEM	SUPPORTED BROWSERS
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

Bypassing the 15,000-indicator ceiling

Volume beyond Defender's native cap offloads to tenant-level Cybereinforce hosting — preserving native Defender capacity for file and IP indicators while maintaining 100% URL enforcement coverage.

One engine, five ways teams put it to work.

01 Defender & Sentinel teams

Real-time ingestion of existing custom indicators closes the Edge-only enforcement gap without re-authoring anything. Overflow beyond the 15,000-indicator ceiling offloads to Cybereinforce hosting, and every block lands in Sentinel as an investigation-ready event.

02 Small & growing businesses

No SOC, SIEM, or Microsoft E5 licence required. Cybereinforce's own curated threat intelligence enforces from the moment the extension is installed — deployable via MDM or a self-serve join link in under 10 minutes.

03 MSPs & MSSPs

Partners choose **Pay-As-You-Go** — a revenue share starting at 25% and rising to 50% at 60,001+ managed licenses, with zero upfront commitment — or prepaid **Credits**, which lock in the volume discount immediately and hand partners full self-service control over client licensing. Credits convert at 1× for Standard, 1.5× for SME, 2× for Corporate, and 3× for Enterprise+, so the same 60,000-credit purchase covers 60,000 Standard licenses or 20,000 Enterprise+ licenses at the same locked-in discount.

04 Compliance & audit teams

FRAMEWORK	CONTROLS / ARTICLES EVIDENCED
ISO 27001	A.5.9, A.5.23, A.8.7, A.8.15, A.8.20
NIS2	Art. 21(2) — incident handling & supply-chain risk
NIST CSF 2.0	PR.PS-05, DE.CM-01, DE.CM-09
DORA	Art. 9 — ICT risk protection & prevention measures
SOC 2	CC6.1 (logical access), CC7.3 (detection)

Detection alone doesn't satisfy a control — enforcement does. Every block event is timestamped, attributable evidence, not a policy document.

05 Mobile & IT fleet teams

The same policy extends to iOS/iPadOS via a native Safari extension and Android via a Firefox mobile extension — deployed through the same MDM, reporting to the same dashboard, with no separate mobile SKU.

Deployment, licensing, and next steps.

✓ Deployment in under 10 minutes

STEP	WHAT HAPPENS
1. Install extension	Deploy via MDM or browser policy — no agent replacement, no network changes
2. Enroll device	Automated silent enrollment
3. Import IOC	Instantly sync existing Defender rules, or activate the curated Cybereinforce feed
4. Enable Sentinel	Activate the telemetry pipeline (optional for standalone deployments)

✓ Licensing tiers

TIER	RETENTION	EVENT LOGS	RULE LIMIT	BEST FOR
Standard	0 days	None	500	Deterministic blocking only
SME	30 days	Up to 500	1,000	SOC-ready visibility
Corporate	90 days	Up to 1,000	2,000	XDR-ready, curated CTI included
Enterprise+	365 days	Up to 2,000	5,000	Compliance-grade, analyst-backed

Secure your endpoints today.

2 weeks completely free — up to 100 rules and 50 devices unlocked immediately, no credit card required.

Start free trial →

Sources: Microsoft Learn — indicators-overview, indicator-ip-domain, network-protection, web-content-filtering (learn.microsoft.com/en-us/defender-endpoint/), retrieved August 2026. ISO/IEC 27001, NIS2 Directive (EU) 2022/2555, NIST Cybersecurity Framework 2.0, DORA Regulation (EU) 2022/2554, and AICPA SOC 2 Trust Services Criteria referenced for framework mapping.