The Defender browser enforcement gap: what Microsoft's own documentation says.

Every claim below is a direct quotation from Microsoft Learn, current as of August 2026, with a link to the source page. This isn't a theoretical gap — it's documented, intended behavior of Microsoft Defender for Endpoint's Network Protection component.

1 Full URL-path blocking is Microsoft Edge-only, by design

Defender for Endpoint's custom indicators let you block a specific **URL path** — not just a domain — for example `https://contoso.com/block`. Microsoft's own documentation is explicit that this only works in one browser:

> "To block a specific URL path, specify the URL path (for example, `https://contoso.com/block`). This indicator matches resources under the /block path on contoso.com. Note that **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**

The same constraint is repeated, word for word in effect, on the indicator-configuration page:

> "HTTPS fully-qualified domain names (FQDN) can be blocked in non-Microsoft browsers **(indicators specifying a full URL path can only be blocked in Microsoft Edge)**."
>
> **— Create indicators for IPs and URLs/domains, learn.microsoft.com/en-us/defender-endpoint/indicator-ip-domain**

2 Why: Network Protection only ever sees the domain, never the path

This isn't a licensing restriction — it's a structural limit of how non-Edge browsers are protected. Outside Edge, Defender relies on **Network Protection**, which inspects traffic below the browser, at the network layer:

> "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** that occurs after a TCP/IP 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 plain terms: Network Protection reads the hostname from the unencrypted part of the TLS handshake (the ClientHello / SNI field) before the encrypted session starts. The actual URL path and query string travel *inside* that encrypted session and are never visible to a network-layer control — in any browser other than Edge, where SmartScreen sits inside the browser itself and sees the request before it's encrypted. Microsoft's Web Content Filtering documentation states the practical consequence directly:

> "Web Content Filtering is based on Network Protection. Blocking in third-party browsers requires required browser configuration for content inspection. **Because full URLs are not available in third-party browsers**, blocking access to certain web applications may require creating a custom block indicator for the application's login page."
>
> **— Web content filtering, learn.microsoft.com/en-us/defender-endpoint/web-content-filtering**

3 Two more conditions stand between "documented" and "enforced"

QUIC & ENCRYPTED CLIENT HELLO

Even domain-level blocking in Chrome/Firefox requires QUIC and Encrypted Client Hello to be disabled in those browsers — otherwise the SNI itself is encrypted and Network Protection has nothing to read. (network-protection, Microsoft Learn)

NETWORK PROTECTION MUST BE IN "BLOCK" MODE

Custom indicators and Web Content Filtering only apply to non-Edge browsers when Network Protection is explicitly enabled in block mode on the device — audit mode or default-off leaves non-Edge browsers unprotected. (network-protection, Microsoft Learn)

On macOS and Linux, the gap widens further:

> "On Windows, network protection doesn't monitor Microsoft Edge. ... On Mac and Linux, **the Microsoft Edge browser only integrates Web Threat Protection**." — meaning even Edge on macOS/Linux doesn't get the same indicator and Web Content Filtering enforcement it gets on Windows.
>
> **— Use network protection to help prevent connections to malicious sites, learn.microsoft.com/en-us/defender-endpoint/network-protection**

4 The indicator ceiling

Separately from browser scope, the entire custom-indicator system has a hard cap:

> "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**

Duplicate indicators still count against that ceiling, and large threat-intel feeds or IR engagements can exhaust it quickly — at which point new IOCs silently fail to enforce rather than raising an error.

What this adds up to

An organization can invest fully in Defender for Endpoint P1/P2, Sentinel, and curated threat intelligence, and still have zero URL-path enforcement the moment a user opens Chrome, Firefox, or Safari — not because the intelligence is wrong, but because the enforcement point (Network Protection) was never designed to see inside an encrypted request outside of Edge. Cybereinforce closes exactly this gap: a native browser extension enforces the same Defender IOC policy at the point where the URL is still visible — inside the browser itself — across Chrome, Firefox, Safari and Edge, on Windows, macOS, Linux, iOS and Android, and offloads volume beyond the 15,000-indicator ceiling to tenant-level hosting.

5 Sources cited in this brief

#	CLAIM	MICROSOFT LEARN PAGE
1	HTTPS URL-path indicators only match in Microsoft Edge	learn.microsoft.com/en-us/defender-endpoint/indicators-overview
2	Full URL path indicators can only be blocked in Microsoft Edge	learn.microsoft.com/en-us/defender-endpoint/indicator-ip-domain
3	Network Protection reads only the TLS ClientHello / FQDN, not the URL path	learn.microsoft.com/en-us/defender-endpoint/network-protection
4	Full URLs are not available in third-party browsers	learn.microsoft.com/en-us/defender-endpoint/web-content-filtering
5	QUIC / Encrypted Client Hello must be disabled for non-Edge FQDN blocking	learn.microsoft.com/en-us/defender-endpoint/network-protection
6	Network Protection must be in block mode for non-Edge enforcement	learn.microsoft.com/en-us/defender-endpoint/network-protection
7	15,000 indicator-per-tenant limit, no increases supported	learn.microsoft.com/en-us/defender-endpoint/indicators-overview

All sources retrieved August 2026 from Microsoft Learn (learn.microsoft.com). Quoted for accuracy; Cybereinforce is not affiliated with Microsoft. Documentation is subject to change — verify current behavior against the live pages before relying on this brief for a compliance submission.