Cybeurope

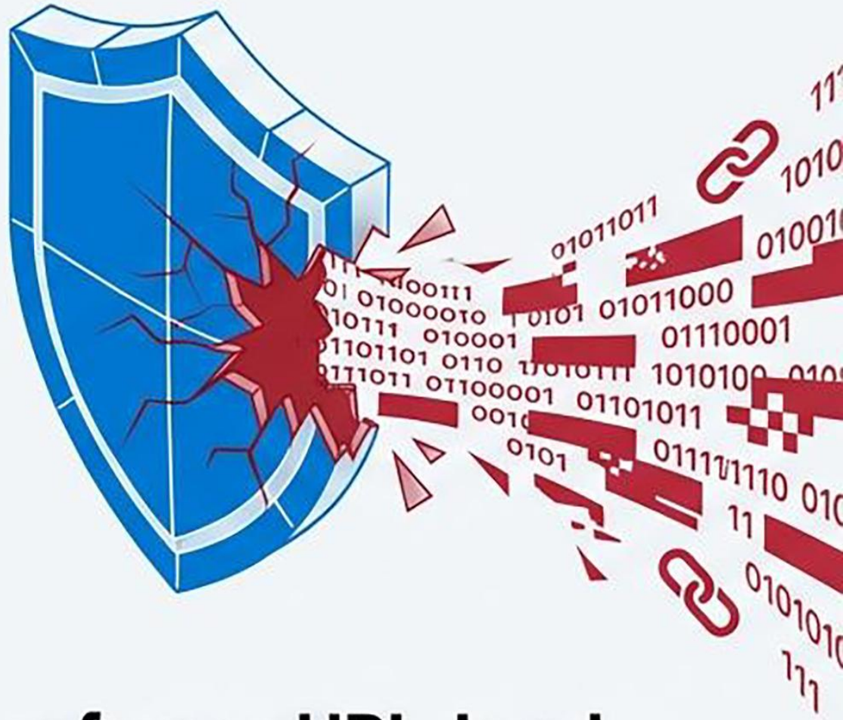
Total Browser Enforcement for Microsoft Defender

Closing the invisible URL gap across all platforms, devices, and contractor ecosystems.

April 1, 2026

Defender blocks malicious domains everywhere.

Comprehensive protection stops threats at the domain level across all applications and interfaces.



But it enforces URL-level blocks only in Microsoft Edge.

Critical URL-level protection is limited to the specified browser, leaving others vulnerable.

Your users on Chrome, Firefox, and Safari are exposed.

Alternative browsers lack the same granular URL filtering capabilities.

Unmanaged iOS, iPadOS, and macOS devices bypass URL indicators.

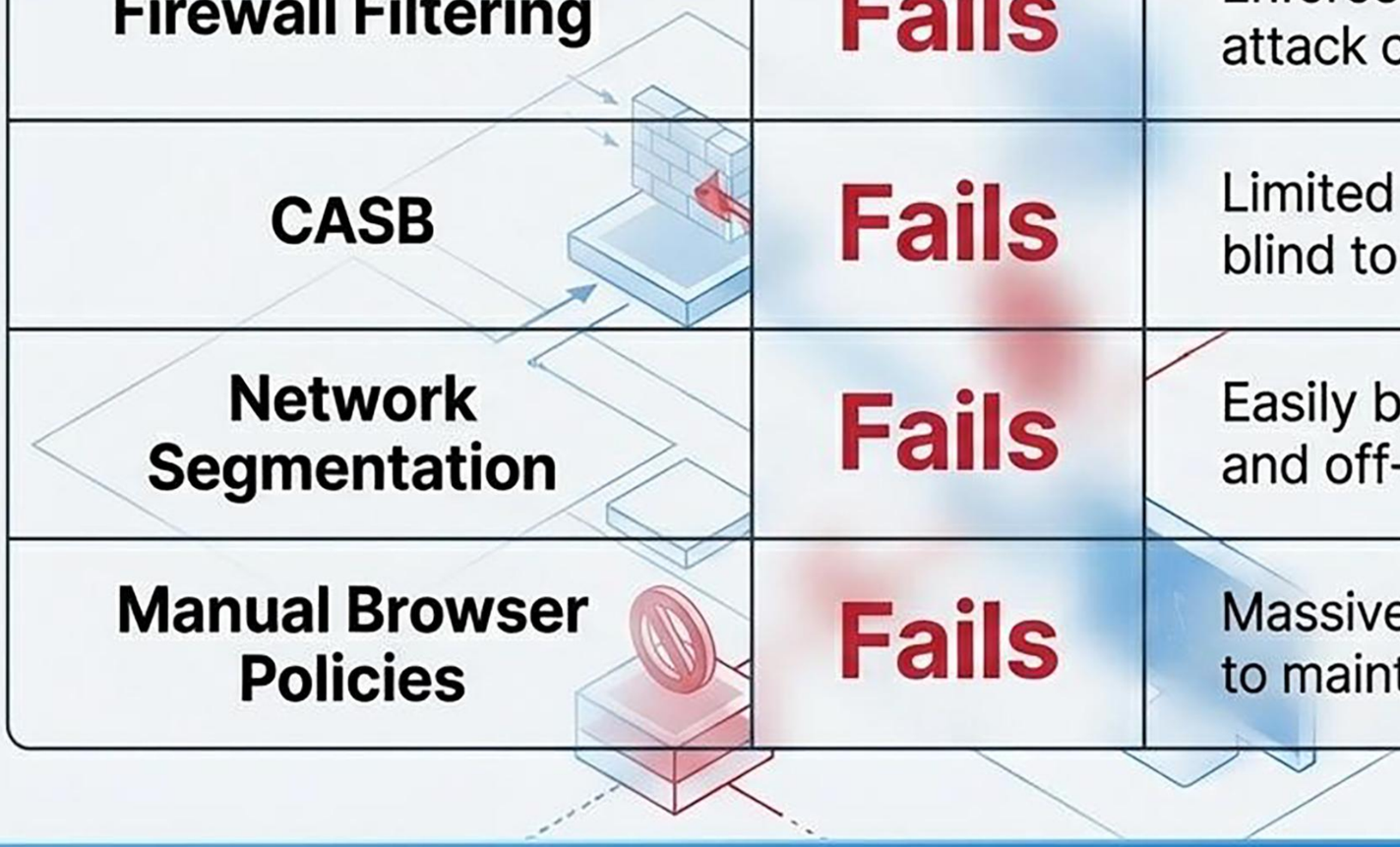
Devices outside your management purview do not respect URL-level restrictions.

Credential-harvesting URLs slip past network-level domain blocks.

Sophisticated phishing links can evade broader domain-based blocks.

Why Current Workarounds Fail

Firewall Filtering	**Fails**	Enforcement happens too late in the attack chain; useless for remote workers.
CASB	**Fails**	Limited scope to specific cloud apps; blind to direct malicious links.
Network Segmentation	**Fails**	Easily bypassable by mobile devices and off-network endpoints.
Manual Browser Policies	**Fails**	Massive operational overhead; impossible to maintain across unmanaged devices.



Only native, browser-level enforcement stops modern credential harvesting before the payload executes.

Ubiquitous Enforcement, Zero Exceptions

Windows & Linux

All Chromium Browsers
Firefox

macOS

All Chromium Browsers
Firefox, Safari

iOS & iPadOS

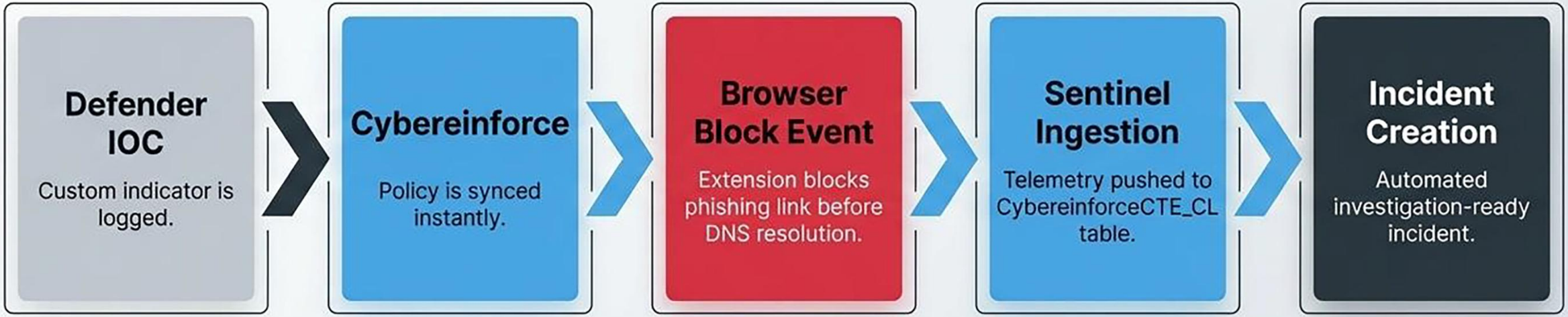
Safari

Android

Firefox

One centralized Defender IOC policy, enforced simultaneously across every operating system and every major browser via a lightweight, native extension.

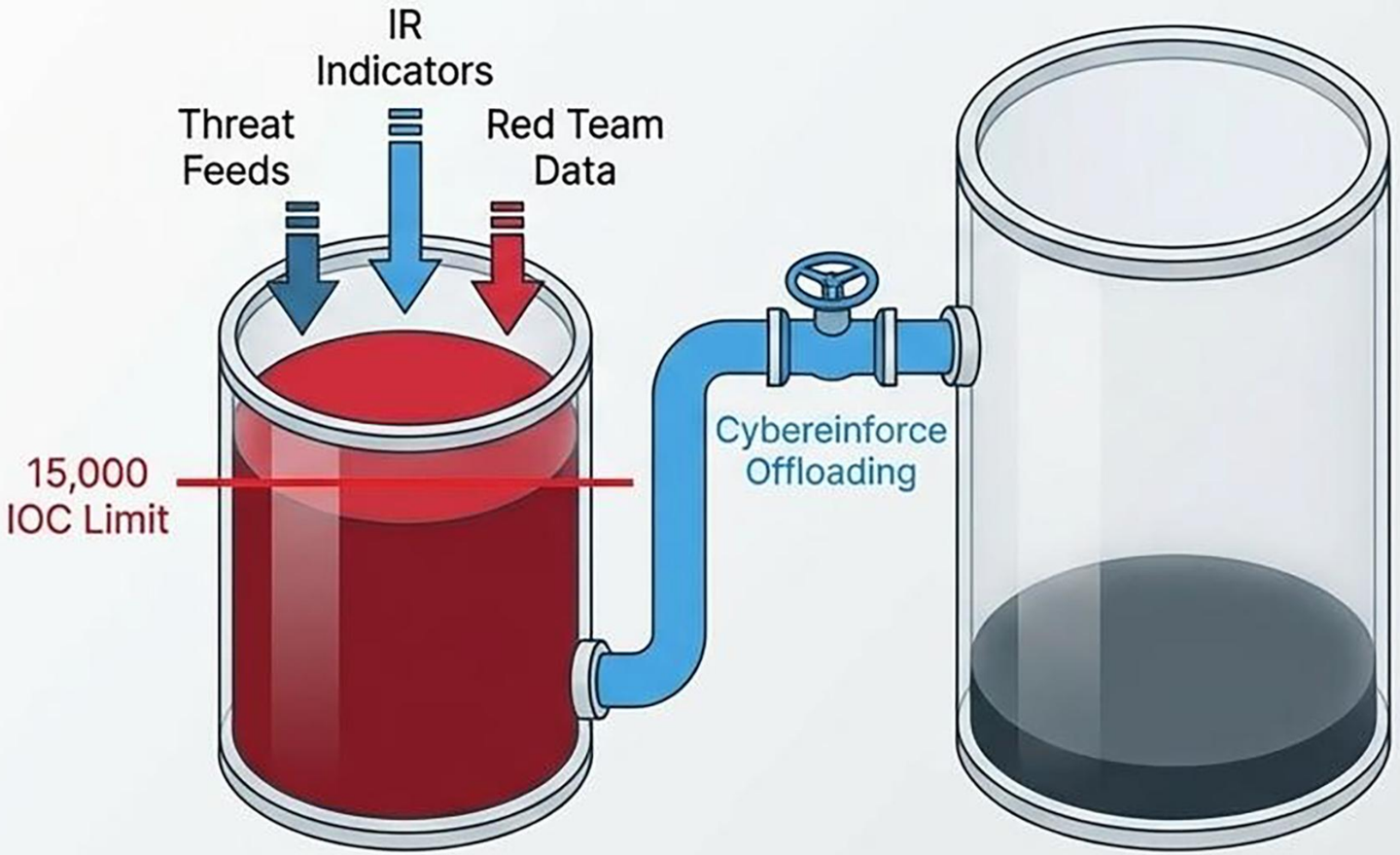
The SOC Visibility Advantage



Cybereinforce

The SOC Visibility Advantage: Traditional DNS filtering blocks the threat but leaves the SOC blind. Cybereinforce ensures the SOC sees every blocked click in real-time.

Bypassing the 15,000 Indicator Ceiling

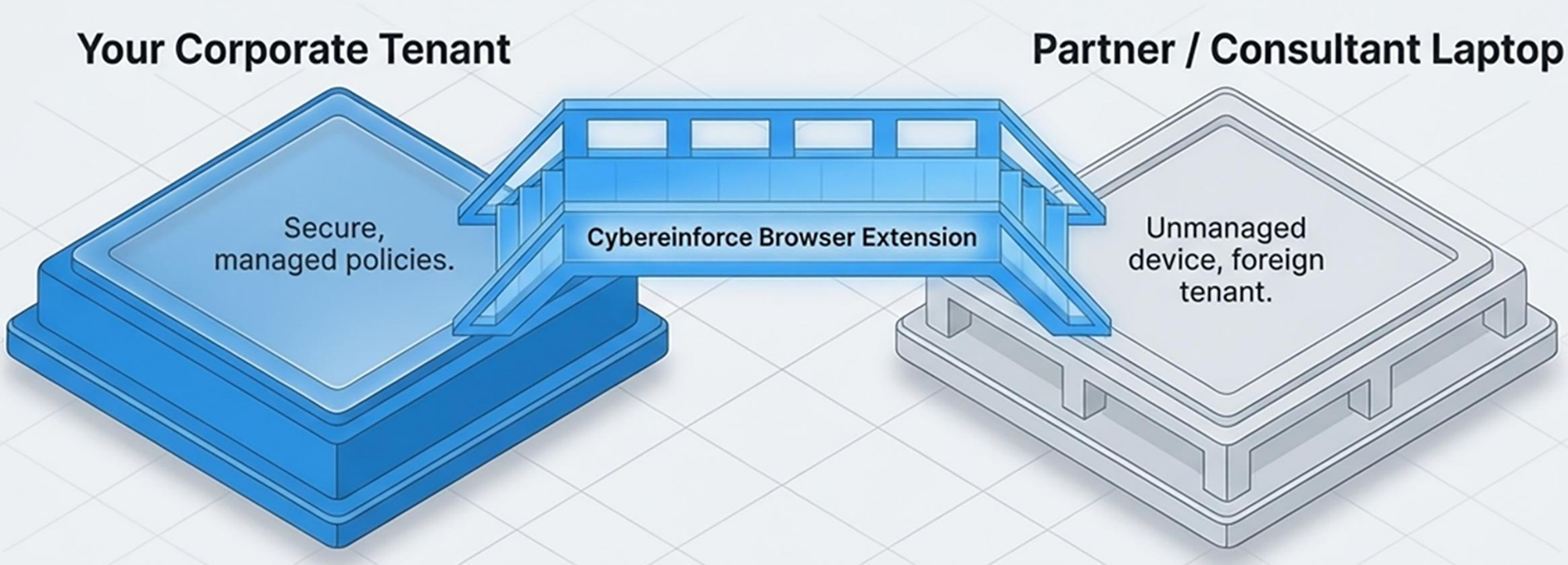


- Offload URL IOCs to tenant-level Cybereinforce hosting.

- Preserve native Defender capacity for file and IP indicators.

- Maintain 100% enforcement coverage without hitting Microsoft's ceiling.

Securing the External Workforce



The Blind Spot:

Consultants, MSP partners, and external users operate on foreign Defender tenants or unmanaged devices. You cannot protect them natively.

The Bridge:

- Enforce your corporate IOC policy directly inside their browser.
- Zero complex tenant migration required.
- Total protection against supply-chain credential theft while respecting their endpoint boundaries.

Closing the Mobile Phishing Gap

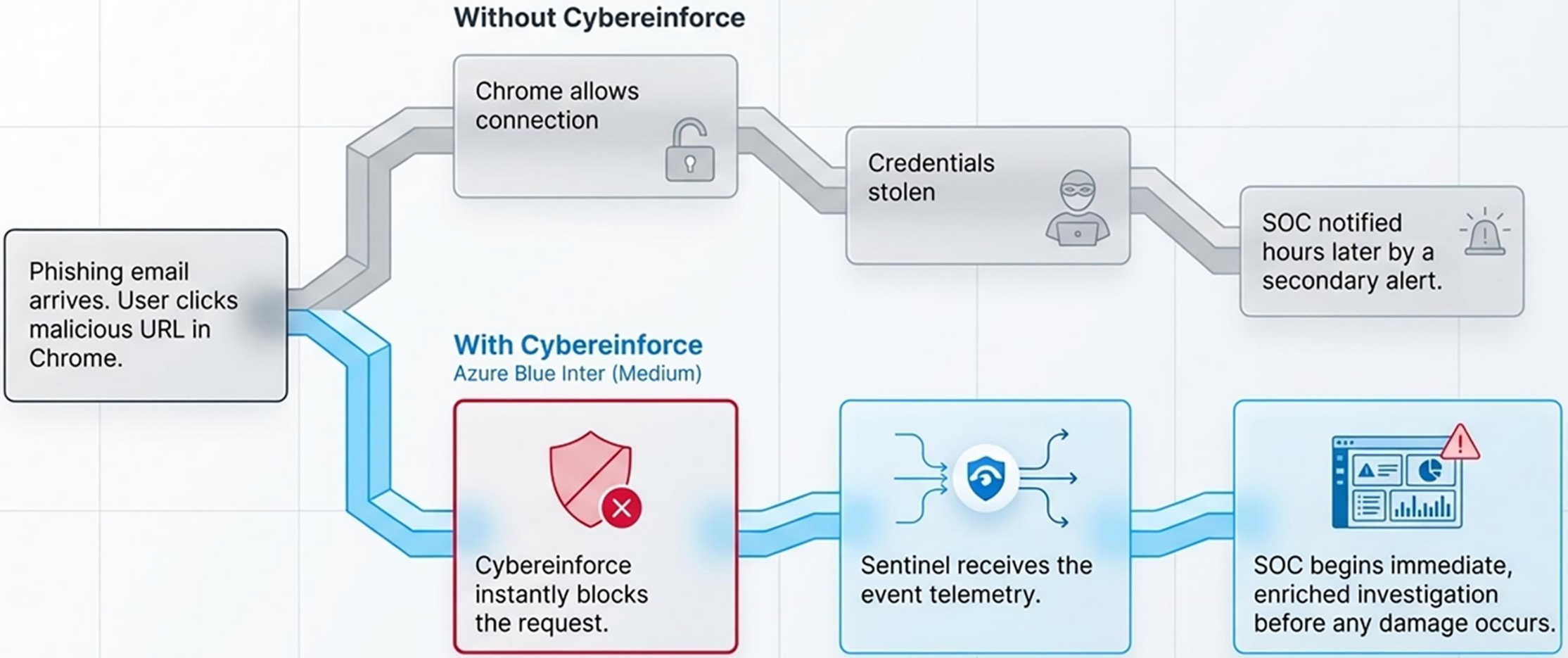
The Threat

Mobile is the #1 entry point for phishing in 2026. Yet, unmanaged mobile browsers lack any native Defender URL enforcement.

The Coverage

- Seamless protection for iOS Safari and iPadOS Safari.
- Full coverage for Android Firefox.
- Every mobile block still generates rich SOC telemetry back to Sentinel.

Anatomy of an Attack



Proactive Threat Intelligence Layer

Beyond Custom IOCs

For Corporate+ environments, Cybereinforce brings its own dynamic arsenal.

The Arsenal

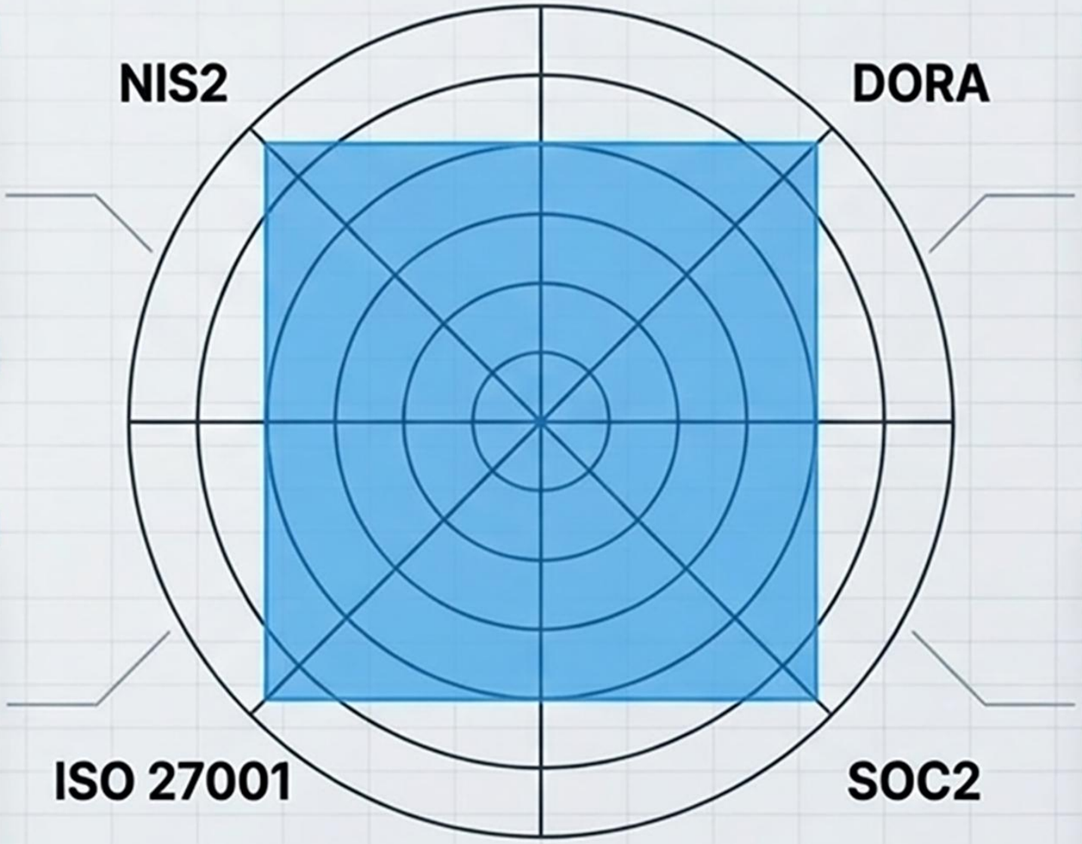
Active protection against 500,000+ known malicious domains and 100,000+ targeted URLs.

The Result

- Immediate protection against unknown threats.
- Rich data enrichment via block visibility.
- Automated, proactive blocking without manual SOC input.

The Compliance Mandate

Delivers mandatory incident detection capability and supply-chain access risk mitigation.



Achieves ICT risk reduction and audit-evidence telemetry generation for financial institutions.

Inter

Directly satisfies controls A.8.7 (Protection against malware) and A.8.20 (Web filtering).

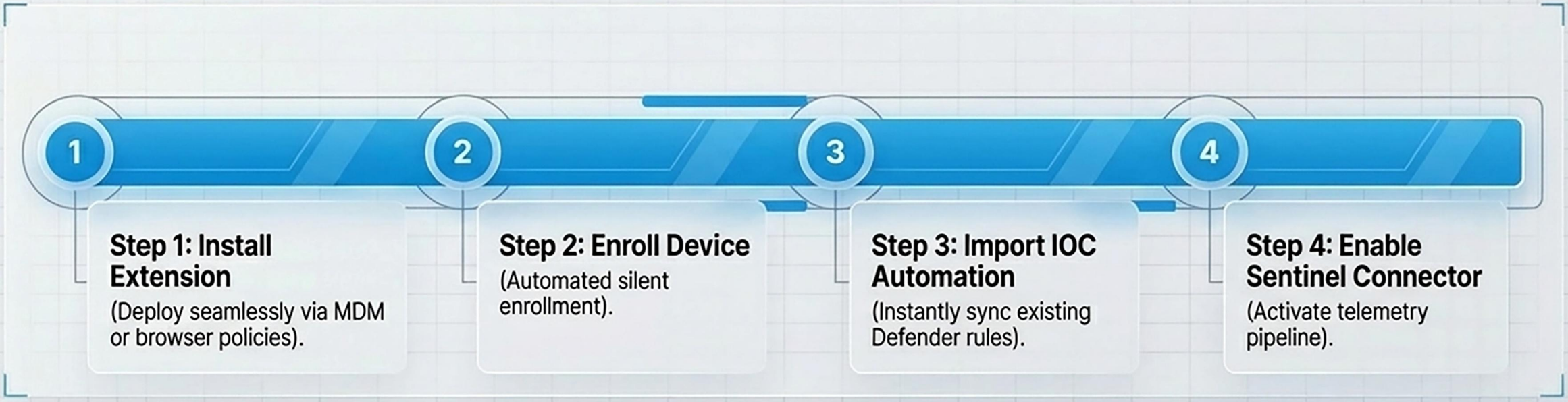
Inter

Fulfills CC6.1 (Logical access controls) and CC7.3 (Detection capability).

The Defender Plan Fit Matrix

Microsoft Investment	Cybereinforce Value Multiplier
Defender P1	Adds the missing **browser-level enforcement layer**.
Defender P2	Extends **IOC enforcement scope** beyond edge cases.
Defender for Endpoint	**Guarantees browser consistency** across all operating systems.
Defender XDR	Dramatically **improves cross-platform incident visibility**.
Microsoft Sentinel	Adds critical, **early-stage investigation** telemetry previously lost to DNS blind spots.

Deployment in Under 10 Minutes



Zero network downtime. Zero complex complex routing. Immediate protection.

Transparent Licensing Tiers

Standard
(Enforcement)

ENFORCEMENT

RETENTION
0 days

EVENT LOGS
None

RULE LIMIT
500

Best for deterministic blocking.

SME
SOC-Ready

SOC-READY

RETENTION
30 days

EVENT LOGS
Up to 500

RULE LIMIT
1,000

Exportable event history.

Corporate
XDR-Ready

XDR-READY

RETENTION
90 days

EVENT LOGS
Up to 1,000

RULE LIMIT
2,000

Curated threat intelligence included.

Enterprise+
Premium

PREMIUM

RETENTION
365 days

EVENT LOGS
Up to 2,000

RULE LIMIT
5,000

Compliance-grade with analyst-backed investigations.

CYBEREINFORCE

Secure Your Endpoints Today.

2 Weeks Completely Free Trial

- Automations unlocked.
- Up to 100 rules and 50 devices supported immediately.
- No credit card required.

Start Trial Now at cybereinforce.com