DATA SHEET

Tanium Security Browser Connector for Microsoft Edge for Business

Unlock real-time browser visibility inside Tanium's unified, AI-driven platform.

Tanium Security Browser Connector for Microsoft Edge for Business ingests real-time intelligence from Microsoft Edge for Business, giving your security teams a more holistic view of endpoint security posture by including browser tabs, extensions, downloads, navigation, and risky behaviors—along with Tanium information about the endpoint, in real time.

Gaps in browser visibility are putting your enterprise at risk

Enterprise work happens in the browser, but most security tools stop at maintaining browser software versions and patching. Browser activity—sites visited, extensions installed, AI tool usage, downloads, and navigation patterns—remains invisible or delayed. This creates blind spots exploited by phishing, malicious extensions, shadow IT, and malicious activity. Without real-time, endpoint-level telemetry from the browser itself, investigations stall, responses slow, and risk increases.

Challenges

- Browsers have become the de facto workspace for SaaS, AI, and core business applications.
- Traditional logging is delayed, incomplete, or entirely missing across many organizations.
- Attackers increasingly target users through embedded browser workflows.

Outcomes

- Improve endpoint security by unifying insights from Edge browser activity into Tanium's Autonomous IT Platform for investigation and correlation.
- Enhance exposure management with browser-based insights such as unsafe downloads and risky extensions.
- Enrich security operations by integrating browser signals into threat investigations.
- Improve compliance validation by pairing browser telemetry with device configuration data.

By combining Edge browser events with Tanium's real-time endpoint intelligence, organizations can investigate faster, eliminate blind spots, and build a complete picture of device and user activity from a single platform.

Real-time intelligence from the Microsoft Edge browser feeds directly into the Tanium Autonomous IT Platform. This gives IT and security teams real-time insight into what users are doing in the browser—tabs, downloads, extensions, navigation—alongside the endpoint data they already rely on to uplevel their security workflows, including:

- Detection of anomalies such as unsafe browsing, malicious extensions, or risky behavior.
- Correlating browser activity with endpoint intelligence for deeper investigations.
- Strengthening compliance on the endpoint.

The following security events can be enabled in a Tanium reporting connector:

- **Browser crash:** Browser or tab crashed (only reported when device-level reporting is available).
- **Browser extension installation:** Extensions are installed, updated, or removed.
- **Malware transfer (download):** Download blocked by Microsoft Defender SmartScreen, or download block bypassed/opened by user.
- **Unsafe site visit:** SmartScreen blocking page is shown or bypassed.
- **URL filtering interstitial:** Web Content Filtering interstitial is shown (can be from SmartScreen's E5/ MCAS or Edge management).
- **Content transfer:** This event will be enabled after V1 of the Microsoft reporting connector launch.
- **Content unscanned:** Content failed to scan for DLP (requires Analysis connector to be configured).
- **Sensitive data transfer:** Content marked as sensitive by DLP scan (requires Analysis connector to be configured).
- **Password changed:** A password is changed in response to a password reuse warning.
- **Password reuse:** A password is detected as reused between an enterprise account and an account on an external site.
- **Login:** A sign-in to a domain in the specified list is successful.
- **Password breach:** A password is detected as compromised as part of a known data breach.

Only Tanium gives security and IT teams real-time browser intelligence as part of a comprehensive, Autonomous IT solution—closing a large blind spot in enterprise security

Seamless browser integration

No browser add-ons, plug-ins, or clients required.

Real-time intelligence

Real-time ingestion of browser telemetry enables confident triage, clearer investigations, and context for faster decisions.

Unified endpoint + browser context

Edge browser intelligence becomes part of Tanium's unified data model—enriching every IT and security workflow.

Learn more at tanium.com or contact your Tanium account team.