DASHLANE

Close Your SIEM's Credential Risk Blind Spot

Browser-native credential risk telemetry is now a native signal across the SIEM your security team already runs

The challenge: A blind spot no SIEM can see

Employees spend much of their work days in the browser. As a result, that's where the majority of credential risk occurs.

However, identity providers (IdPs) and endpoint detection and response (EDR) tools can't see how credentials are entered, reused, or exposed in the browser, which means that signal never reaches the Security Operations Center (SOC).

Shadow IT and unmanaged SaaS logins compound the problem. With no credential telemetry source outside the sanctioned stack, those logins never surface in the SIEM.

Traditional identity and endpoint tools don't:

- Capture browser-native credential risk telemetry, regardless of SSO or vault use
- Surface shadow IT and unmanaged SaaS logins inside the SIEM
- Unify credential investigations without pulling context from a separate console

The result: Siloed data, manual investigations

Credential data stays siloed no matter which tool a team uses. Investigating a credential-based threat means manually correlating events and rebuilding timelines, adding workload for already-stretched security teams.

The solution: Omnix SIEM integrations

Dashlane Omnix® sends browser-native credential risk telemetry directly into the SIEM security teams already use.

Every weak or compromised credential, suspected phishing domain, and admin response action becomes a structured event, correlated against identity, endpoint, network, cloud, and observability data already in that SIEM.

SIEM integrations

CROWDSTRIKE
panther
DATADOG
splunk> a CISCO company
Microsoft Sentinel®
DASHLANE

DASHLANE

Why it's different

- Browser-native telemetry, portable across your stack. Omnix captures credential events at the moment of use, regardless of SSO or vault use, and that signal integrates with your SIEM of choice.
- Last-mile phishing protection, wherever you triage. Omnix's proprietary AI phishing model evaluates suspicious sites before credentials are entered, and those enriched events show up natively in the tool analysts already use.
- Correlation-ready events, not raw logs. Omnix structures and enriches each credential risk event before it streams into the SIEM, so security teams get context-rich signals ready to correlate, not raw data they have to normalize themselves.
- Zero net-new tools required. Instead of having a new console to learn, credential risk becomes a native signal inside the existing stack.

> "You can't solve credential risks if you don't know where they are. With Omnix, now we have that visibility."
>
> — Chris Scalise, CISO, Ambient Enterprises

How it works

1. Omnix captures credential events directly in the browser—how credentials are entered, reused, or exposed—the moment they happen.
2. Those signals are normalized into structured events enriched with context, which means no raw logs or manual tagging.
3. That event streams directly into the customer's SIEM of choice, so there's no new console or manual export.
4. Security teams correlate credential risk against identity, endpoint, network, and observability data already in the SIEM and trigger automated remediation at scale.

Close the blind spot, no matter your stack

These SIEM integrations are available through Omnix, the only credential security platform that goes beyond the boundaries of a traditional password manager, with browser-native telemetry for every login, correlated wherever a security team already works.

Make credential risk a standard signal across your SOC, the same way EDR and identity logs already are.

Close your SIEM's credential risk blind spot

Learn how