Dashlane

The Credential Risk Visibility Gap

April 7, 2025

How CISOs can reduce their blind spots and determine their organization's credential risk

innovate
CYBERSECURITY SUMMIT

DASHLANE

Stolen credentials are the #1 cause of breaches

Verizon, "2024 Data Breach Investigations Report," 2024

AI is accelerating cyber threats

84%
of IT leaders report an increase in phishing volume, sophistication, or both

80%
of IT leaders say phishing attempts targeting their organization are on the rise

74%
of IT leaders say AI poses an increased threat to password security

According to a Dashlane survey of 500 IT leaders and 1,000 employees in the U.S.

Credential risk visibility is an ongoing challenge for most organizations

39%

of employees use apps not managed by their company on work devices

- Blind spots in your credential security lead to an increased attack surface

- SSO isn't the solution. IT leaders estimate that, on average, **37% of their corporate apps are not behind SSO**

- Without visibility into credential events related to devices and apps that access corporate resources, IT teams can't secure data and prevent unauthorized usage

According to a Dashlane survey of 500 IT leaders and 1,000 employees in the U.S.

Security teams need a proactive, enterprise-wide solution

Security teams are already overburdened, with 58% reporting being overwhelmed by their daily tasks.

Supporting them and preventing attacks before they happen requires:

- **Real-time monitoring:** Continuous, event monitoring of credential data for all employees, including employees not logged into a credential manager and those using shadow IT

- **Risk detection:** Identify at-risk credentials, highlighting the number of weak or compromised passwords that pose a security threat

- **Actionable Data & Automation:** Reporting and activity logs that give admins a clear picture of their organization's credential risk posture and automated notifications to employees

Detect and manage credential risks across all employees
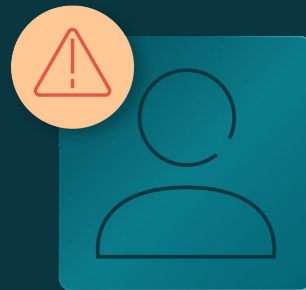
Protect your organization, even when employees:

Log into corporate apps
not under SSO

Log into shadow
IT apps

Log into
personal apps

Detect and manage credential risks across all employees

Employees get real-time, in-context notifications about:

Usage of risky credentials

Corrective actions

Warnings of phishing attempts

You can understand your credential risk posture within hours

Deploy Dashlane's Credential Risk Detection to all or a subset of employees

Get compromised credential usage event logs

See top at-risk users

Learn about risky credential usage across corporate and shadow IT apps

We invite you to test it and provide feedback

Credential Security Essentials for Global Enterprises
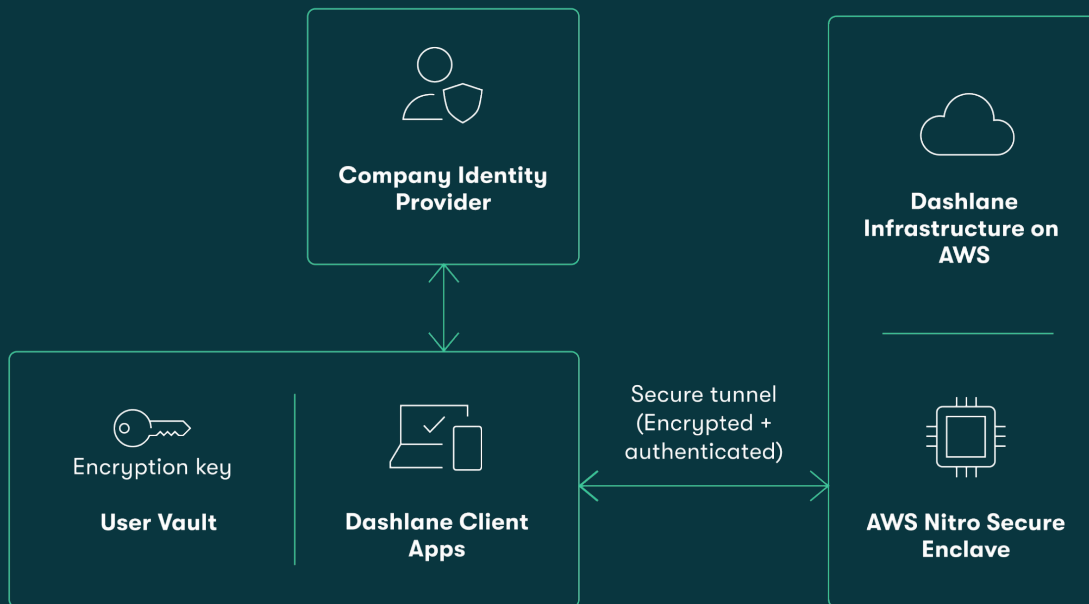
- Zero-Knowledge Architecture
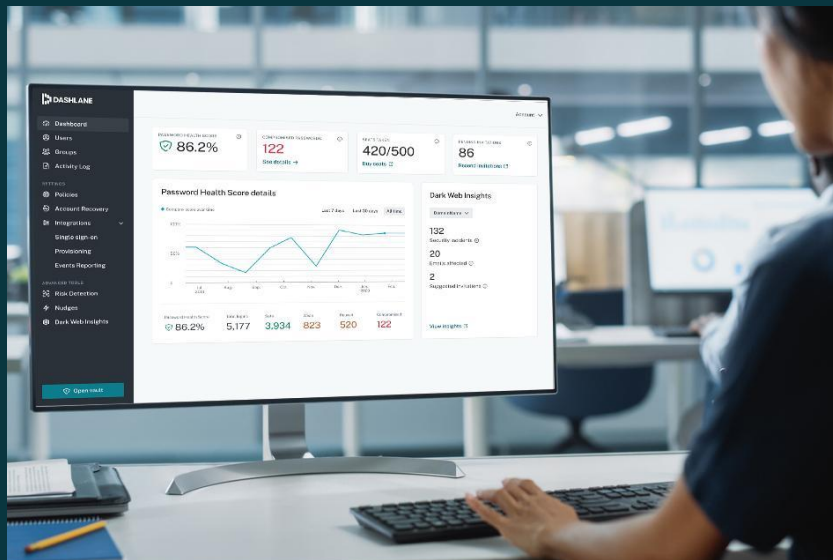- Confidential Computing
- Passwordless & Passkeys
- Browser-based Credential Technology

Company Identity Provider

Dashlane Infrastructure on AWS

Encryption key

User Vault

Dashlane Client Apps

Secure tunnel (Encrypted + authenticated)

AWS Nitro Secure Enclave

DASHLANE

On a mission to close the credential security gap

- Serving 24k+ SMB, mid-market & enterprise orgs

- Secure by design with zero-knowledge architecture

- 1-click integrations: SSO, user provisioning, SIEM

- Phishing protection & secure password sharing

- A passwordless leader & FIDO Alliance member

Learn more about proactive credential security - and passwordless

How does your company's credential security measure up?
Read our report

Dashlane State of Credential Security Report

DASHLANE