DASHLANE

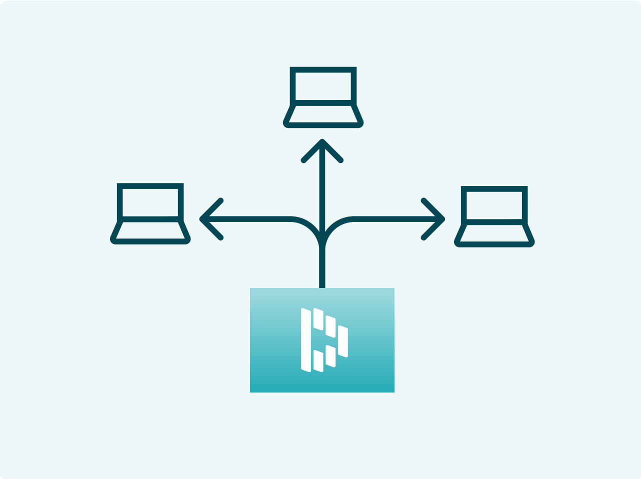
# Get unmatched visibility for maximum breach protection

## How Credential Risk Detection works

## Automate monitoring for real-time visibility and enhanced security

Credential Risk Detection proactively monitors for employees who may be at risk because they're using weak or compromised passwords on company-managed devices. This tool leverages Dashlane's browser extension to continually detect when employees who aren't logged in to Dashlane use risky passwords. That way, IT admins can identify the most vulnerable employees and invite them to secure their credentials with Dashlane.

Dashlane uses a proprietary algorithm to detect weak and compromised credentials. Neither Dashlane nor the company admin has access to employee passwords monitored by Credential Risk Detection.



### Deploy silently

The browser extension is configured and deployed silently so Credential Risk Detection can monitor for risk without alerting employees, giving admins an accurate view of every employees' credential threats.

### Monitor while maintaining privacy

Detected threats are collected in a dashboard and granular activity logs. Logs are end-to-end encrypted and include the associated employee and website but don't show the password itself, maintaining privacy.

### Detect hidden credential risks

Admins are empowered with actionable insights and a clear view of their entire org's security posture. They can then invite vulnerable employees to their Dashlane plan to resolve risk and enhance breach protection.