DASHLANE

Secure by Design in Action: Re-Architecting Authentication to Eliminate Credential Risk

CISA TXG - Septembre 17, 2025

Dashlane is the leading credential security solution for businesses and consumers

Protects and manages passwords, passkeys, secrets, and other sensitive info for millions of users

Provides over 25k businesses with secure access and proactive protection from credential threats

Pairs enterprise-grade security with consumer-grade design in a top-rated platform

2

Some context

Founded in 2009

~300 employees in Paris, Lisbon and New York

Consumer product (B2C) + Enterprise offer (B2B)

10 “product & engineering” teams

~120 in Product & Engineering

CISA Secure by Design Goals

1. Multi-factor authentication (MFA)
2. Default passwords
3. Reducing entire classes of vulnerability
4. Security patches
5. Vulnerability disclosure policy
6. CVEs
7. Evidence of intrusions

CISA Secure by Design Goals → Aim for Secure & Private by Design

1. Multi-factor authentication (MFA)
2. Default passwords

→ **Move to passwordless**

3. Reducing entire classes of vulnerability

→ **Reduce exposure**

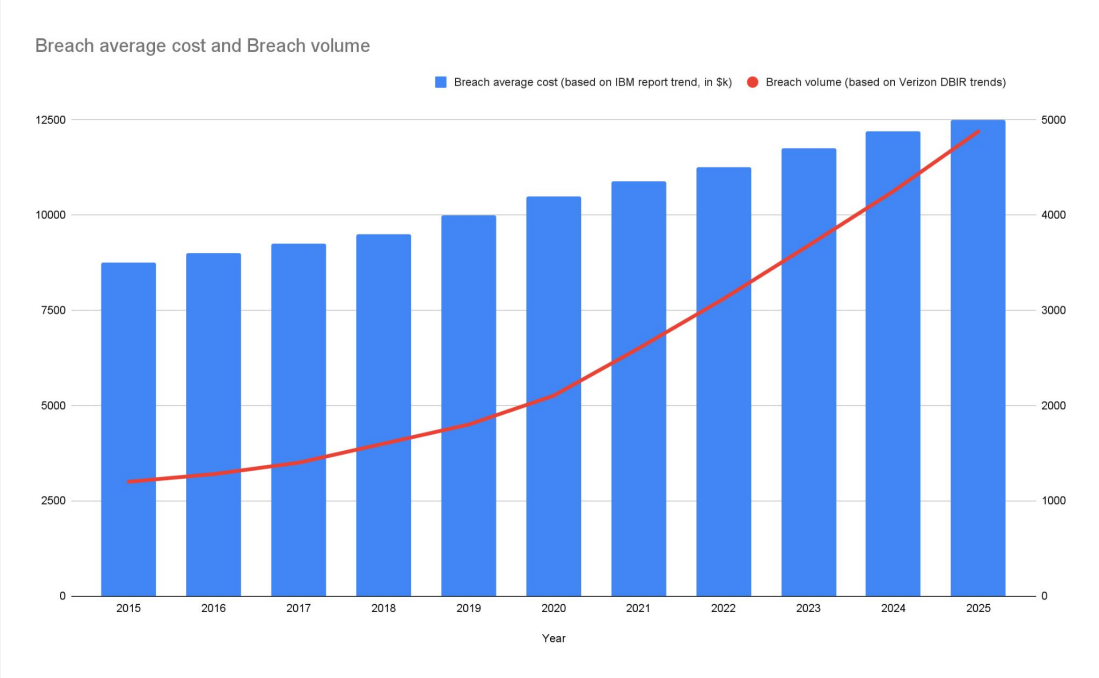
4. Security patches
5. Vulnerability disclosure policy
6. CVEs
7. Evidence of intrusions

→ **Proactive Security**

The Move to Passwordless

The phishing threat

- Average user has more than **100 passwords**, with **40-50% reused passwords**
- 54% of AI-powered phishing campaigns are successful (vs 12% for traditional attacks)
- **4,151% surge in phishing volume** experienced by organizations since the launch of ChatGPT.
- 67.4% of attacks now utilize some form of AI to generate perfect grammar and analyze corporate communication patterns.



Achieving Phishing-resistance

- We aim to fix authentication at the root and get rid of passwords.

- **Our goal as a credential manager: go Passwordless**
  - **Migrate customers to Passkeys**
  - **Use phishing-resistant solutions in particular for critical systems**

Some numbers*

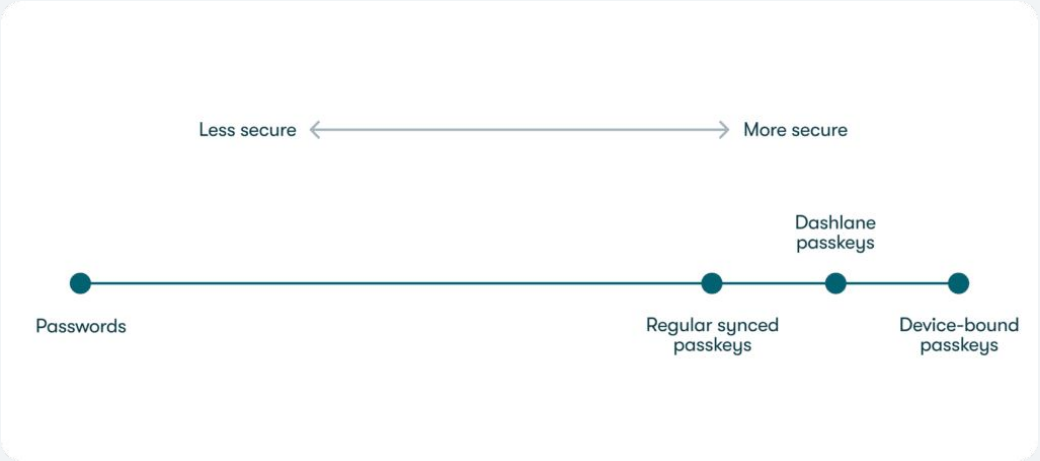
- **76% of IT leaders** say their C-Suite is pushing for passkey adoption

* From Dashlane State of Credential Security Report 2025

Dashlane's journey to passwordless and to phishing resistance

Deep dive on Passkeys

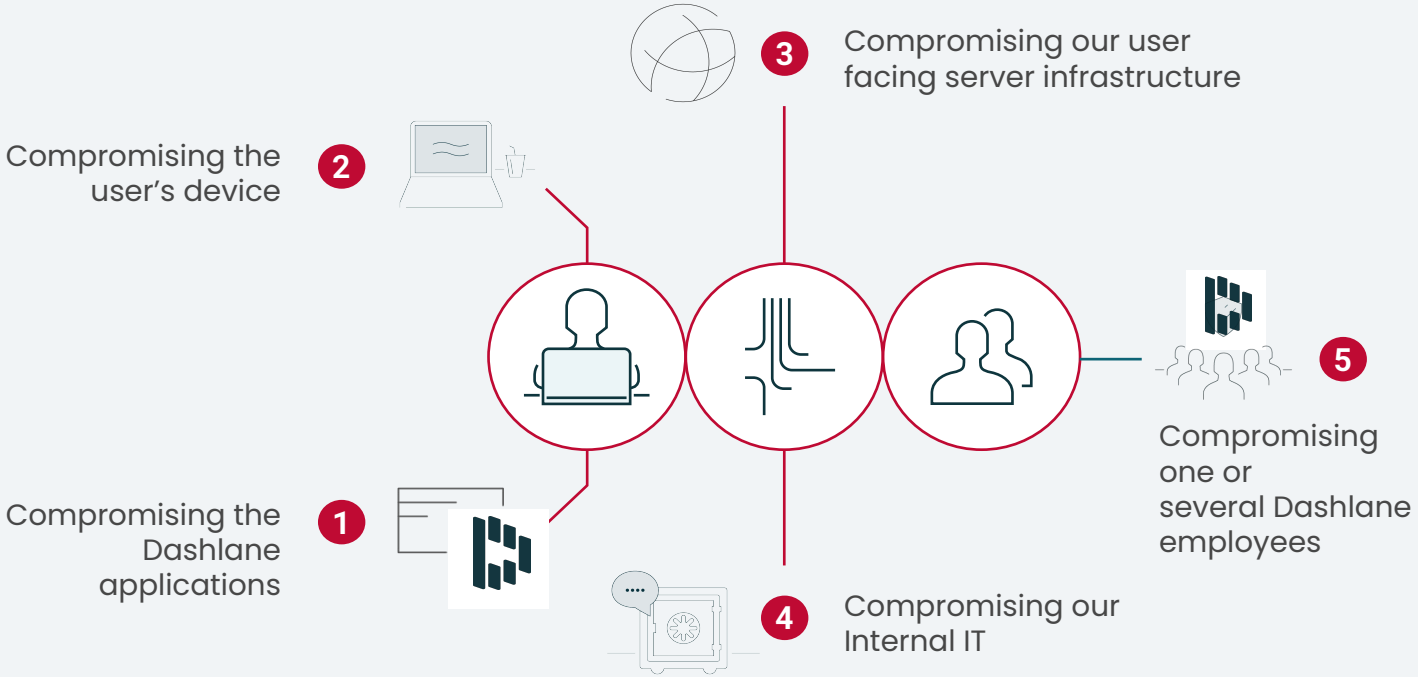
- For Service providers
  → Improved security and convenience for customers
  → Reduced liability and customer support cost
- Get started: [Developer Resources | FIDO Alliance]



- 6x passkey authentication with Dashlane in the last year
- 500k passkey use / month
- 20+% of active Dashlane users now have at least 1 passkey
- Signins are 70% more successful compared to passwords.

Reducing exposure

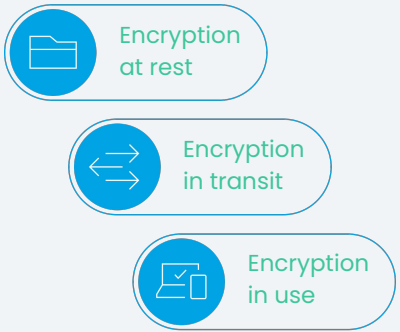
Dashlane Threat Model



Minimize exposure at the architectural level

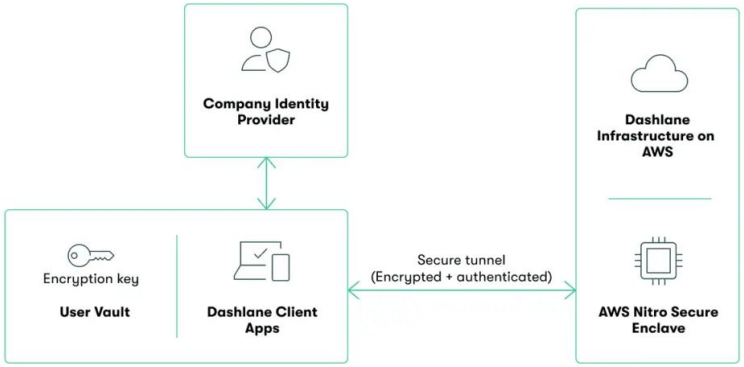
- We aim to build a Dashlane product that is structurally **secure + private**.
- **Zero-Knowledge Architecture**: applied throughout the product
  - Encryption/decryption on device
- Risks inherited from the ecosystems we live in

End-to-End encryption powered by Confidential Computing



- Achieving end-to-end encryption: in transit, at rest and in use
- Extending zero-knowledge to cloud through cloud secure enclaves and confidential computing

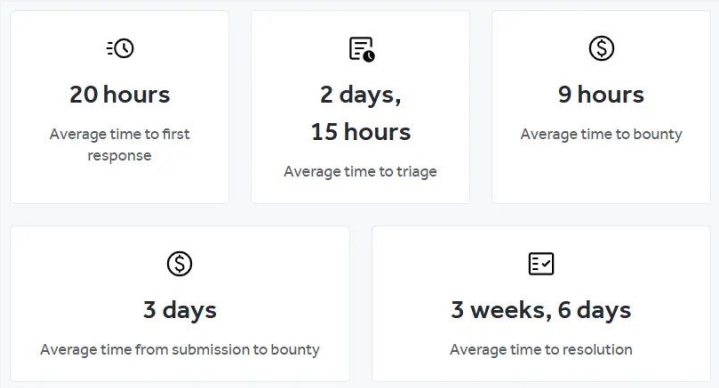
→ Zero-knowledge should apply to all products and services that process sensitive customer data!



Embedding Secure by Design into organizational culture

Our practices to foster a mindset of Secure by Design:

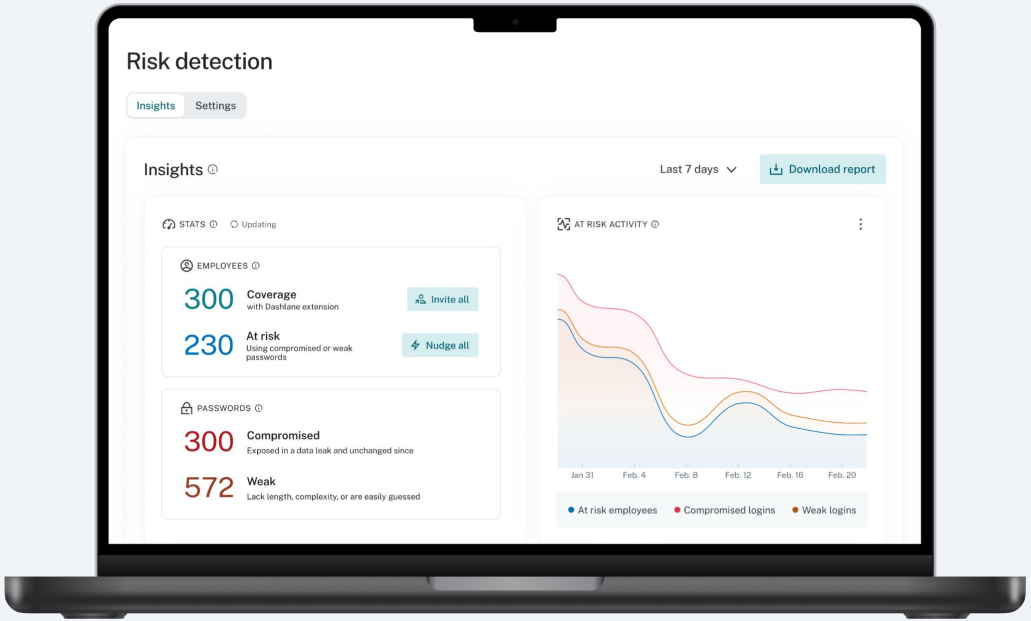
- Making our source code publicly available
- Public bug bounty program
- Risk Committee
- Dogfooding our own product
- Cross-functional security education
- Active participation in FIDO Alliance
- Blog articles, security white-paper, share about our tech and product



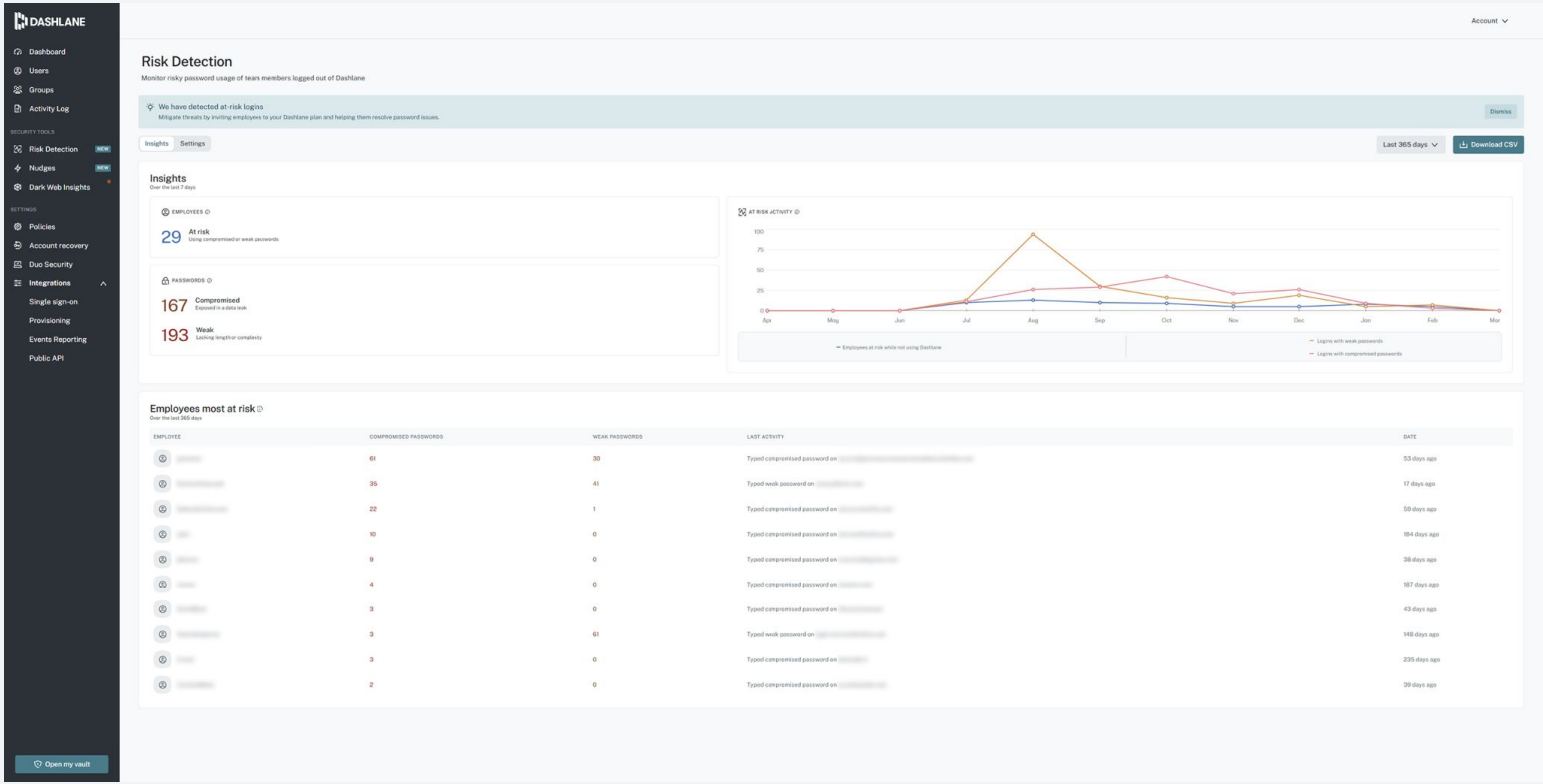
Proactive Security

Providing Full visibility

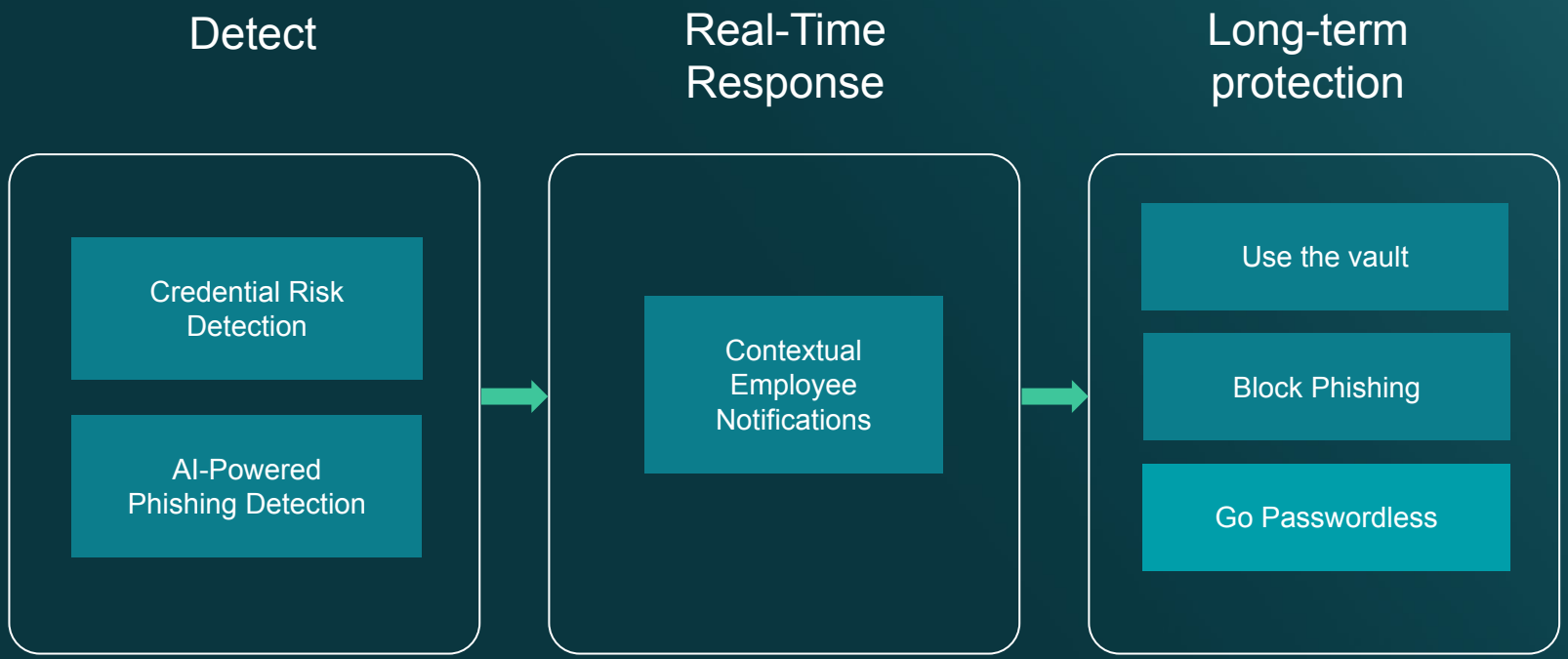
- What is happening in organizations?
- Need visibility to act
- Monitor credential behaviors proactively
- Act at the employee level. Influence behaviors in context



Our own case study



The virtuous cycle: detect, respond, protect



Key Takeaways

- Credential security remains at the heart of the Authentication problem.

- Our goal - Fix the root causes:
  - Eliminate passwords. Move to passwordless and phishing-resistance
  - Invest in privacy and security by design, to reduce exposure
  - You can only secure what you know: provide visibility so you can take action


DASHLANE