LastPass | Partner Program

The Missing Layer in Your Security Strategy: Credential Management

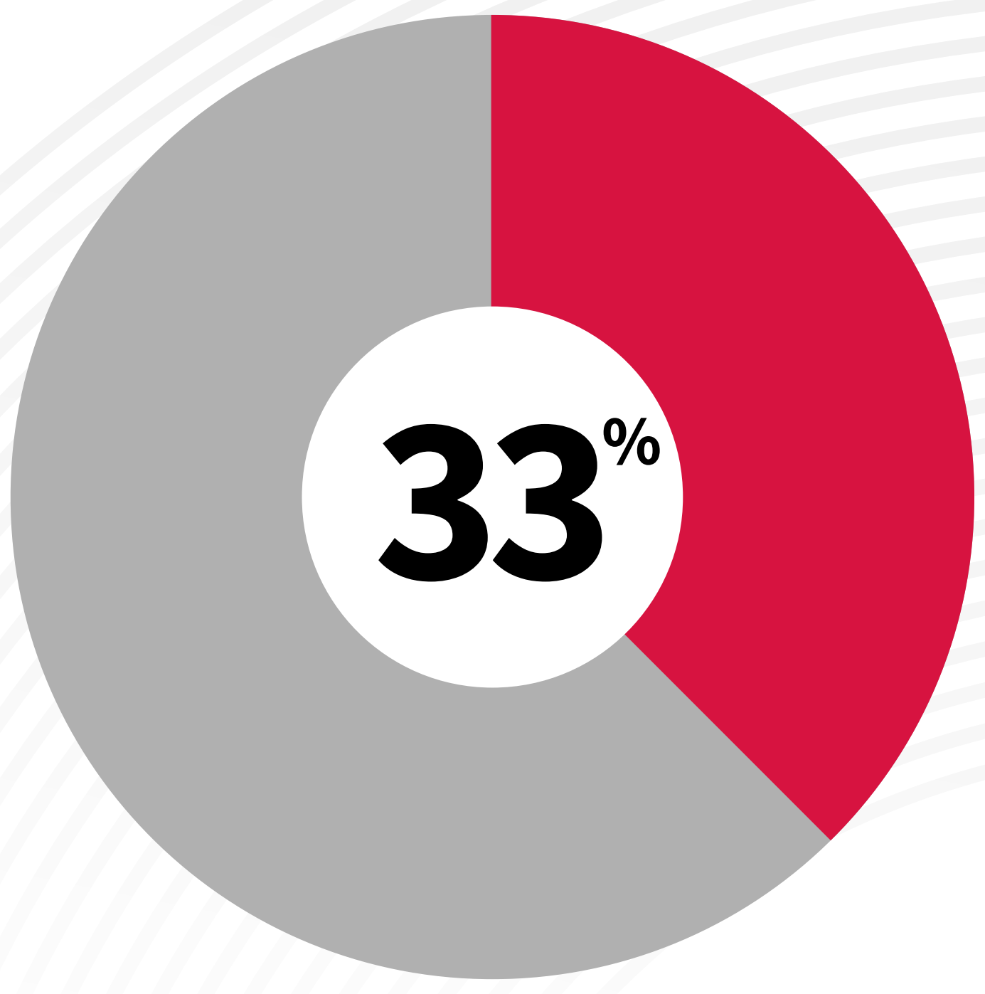
Regardless of your company's size think about the security tools that **you rely on right now.**

One in five mid-sized businesses have experienced a breach in the past year.

Think about the security tools that you rely on right now. You've likely invested time, money, and resources into some combination of these security tools:

- Firewalls/Intrusion Detection
- Anti-Phishing/Email Security
- Identity Providers (IdP), like Okta or Microsoft Entra
- Security Information Event Management (SIEM)/ Extended Detection Response (XDR)
- Managed Detection and Response (MDR)/ Endpoint Detection and Response (EDR)
- Business Disaster Recovery (BDR)

And you've proactively put up these defenses for good reason.



One-third of all security incidents are linked to stolen credentials.

But despite all the investments you have made to secure people, processes, and technology, you may be leaving one of the most common attack vectors wide open: weak and reused passwords.

The truth is, most breaches don't start with sophisticated hacking, they start with poor password hygiene—like someone using an easily guessable password like "Welcome123" or reusing the same password across multiple work and personal SaaS tools, systems, and devices.

⚠ **Nearly half of small businesses are targeted by cyberattacks.**

That's why credential management shouldn't just be a nice-to-have, it must be foundational to your security program. Without it, even the best security tools cannot fully protect your customer's business.

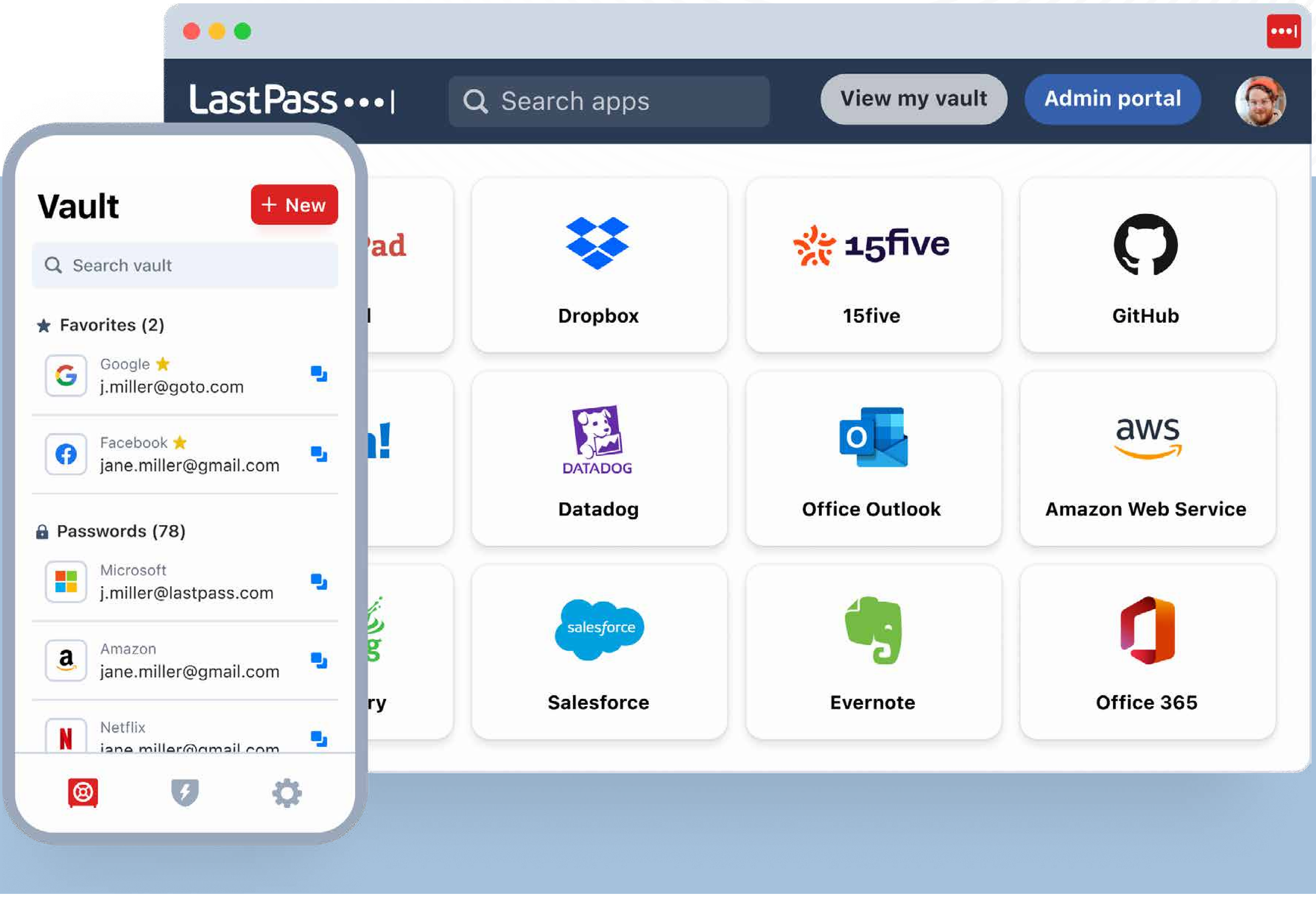
Partnering with a strong password manager can help you get more out of every layer of your security stack by reducing human risk and locking down the numerous access points attackers thrive off exploiting.

> "The good news is that creating and storing strong passwords with the help of a 'password manager' is one of the easiest ways to protect ourselves."
>
> - Cybersecurity and Infrastructure Security Agency (CISA)

Unlock More Value from Your Security Tools with a Password Manager

Adding a password manager to your security setup helps protect your customers by fixing one of the biggest weak spots—passwords. It makes sure everyone uses strong, unique passwords and gives you more control over who can access what. That means your other security tools work better, and your customers stay safer.

But it doesn't stop there. A password manager also boosts the performance of your other security tools. By reducing weak passwords, shared credentials, and risky behaviors, it helps tools like firewalls, endpoint protection, and identity providers do their jobs more effectively, making your entire security setup stronger.



PASSWORD MANAGER + FIREWALL

Locking the Front Door, Not Just Guarding the Perimeter

Firewalls are essential for monitoring and controlling network traffic, blocking suspicious or malicious activity before it spreads. But they cannot stop an attacker who walks right through the front door using stolen or weak credentials.

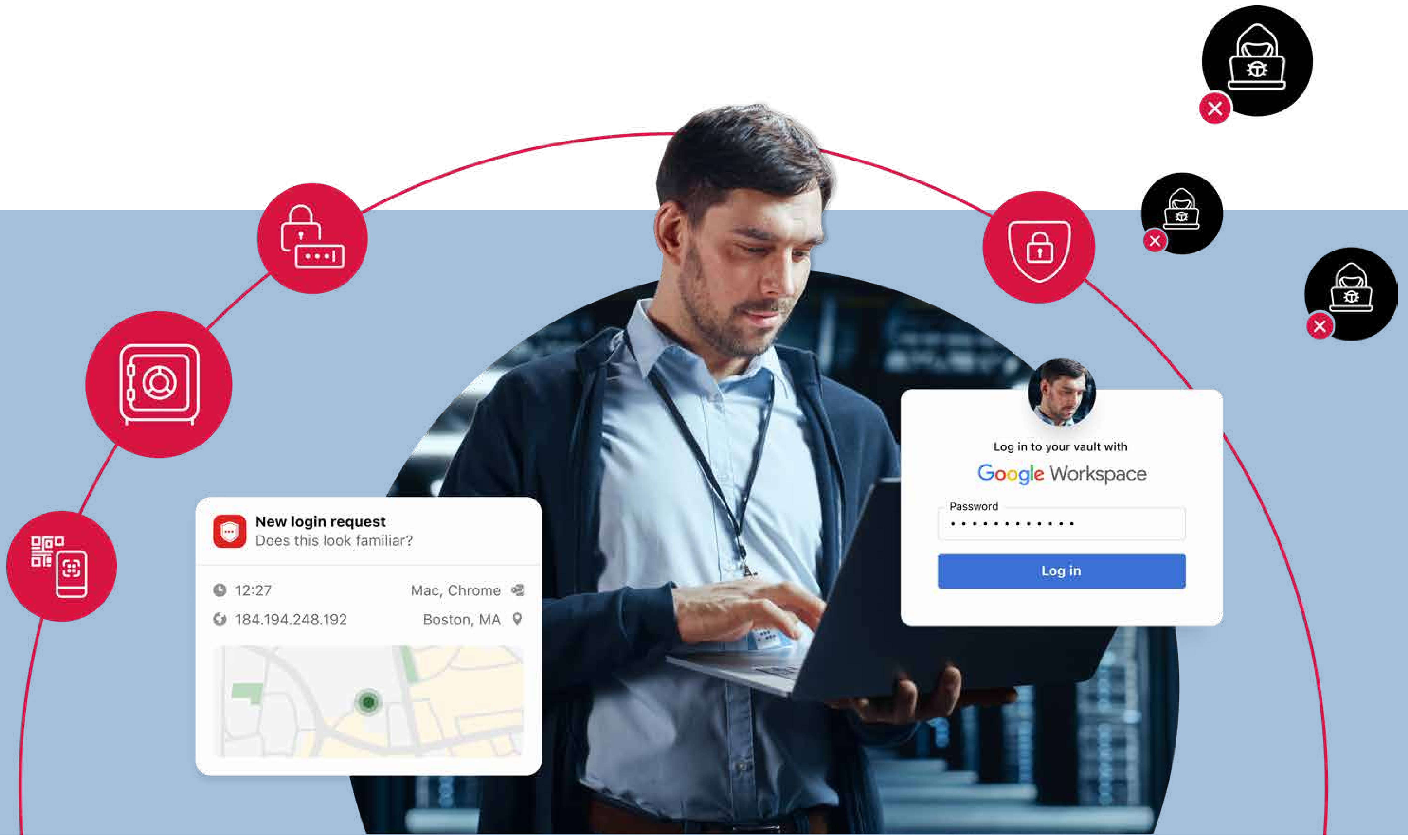
While traditional firewalls protect your system from bad network traffic, they do not do anything to protect the legitimate ways in which someone can access their network. This is where a password manager comes in to help.

What a password manager adds to a firewall:

- Enforces strong, unique passwords and role-based access controls to reduce credential reuse and prevent unauthorized access.
- Aligns with network security frameworks by supporting password complexity requirements, access policies, and audit readiness.
- Accelerates response: in the event of a breach, IT teams can quickly retrieve critical credentials to isolate systems and contain threats.

Firewalls form the walls and doors to your network, but a password manager protects the keys.

Together, they provide stronger, more comprehensive network security.



PASSWORD MANAGER + PHISHING & EMAIL SECURITY

Stronger Defense, Better Recovery

Phishing and email security tools are essential for identifying and blocking malicious messages before they reach employees. But no filter is flawless, and when phishing emails slip through, your next line of defense is credential protection.

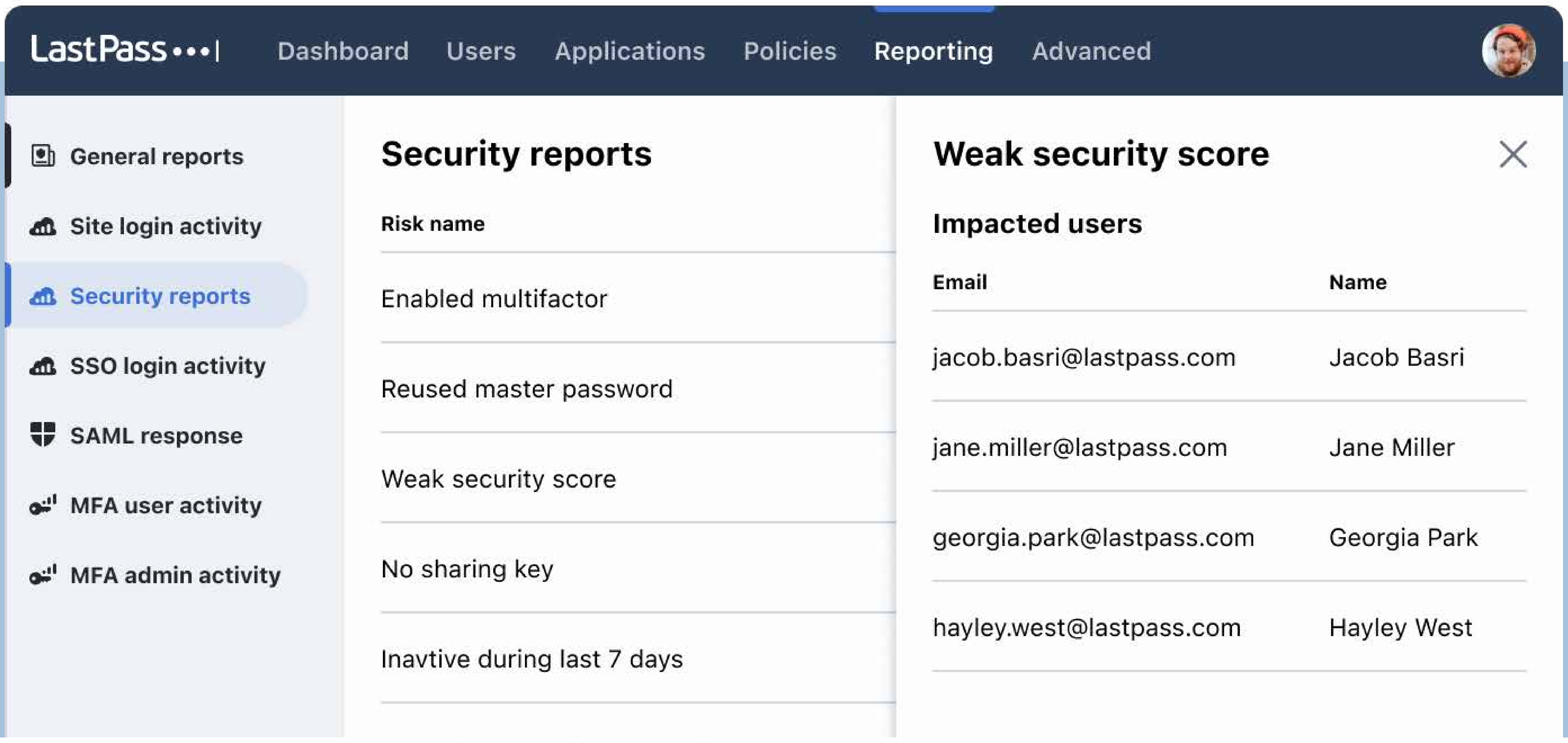
The bad guys know that many people reuse their passwords across many sites, and without a password manager, a single successful phishing attempt can expose reused or weak credentials, leading to widespread compromise in moments.

What a password manager adds to phishing and email security:

- Acts as a safety net by securing credentials even when phishing filters fail—limiting the blast radius of any breach.
- Enables you to quickly access, reset, or revoke compromised credentials, reducing response time and business impact.
- Protects admin credentials and MFA recovery codes for your email security tools, ensuring secure access and uninterrupted operation.

When phishing gets personal, password management keeps you protected—by locking down the keys before attackers can use them.

Password managers also securely store multi-factor authentication (MFA) recovery codes that spam filters require, making authentication more efficient and secure.



Security reports

Risk name
Enabled multifactor
Reused master password
Weak security score
No sharing key
Inavtive during last 7 days

Weak security score

Impacted users

Email	Name
jacob.basri@lastpass.com	Jacob Basri
jane.miller@lastpass.com	Jane Miller
georgia.park@lastpass.com	Georgia Park
hayley.west@lastpass.com	Hayley West

PASSWORD MANAGER + IdP

Extend Protection Beyond What's Federated

Most organizations rely on identity providers (IdPs) like Entra, Okta, or Ping to secure access to key applications through single sign-on (SSO). These tools are highly effective at centralizing identity and enforcing policies for the apps they cover.

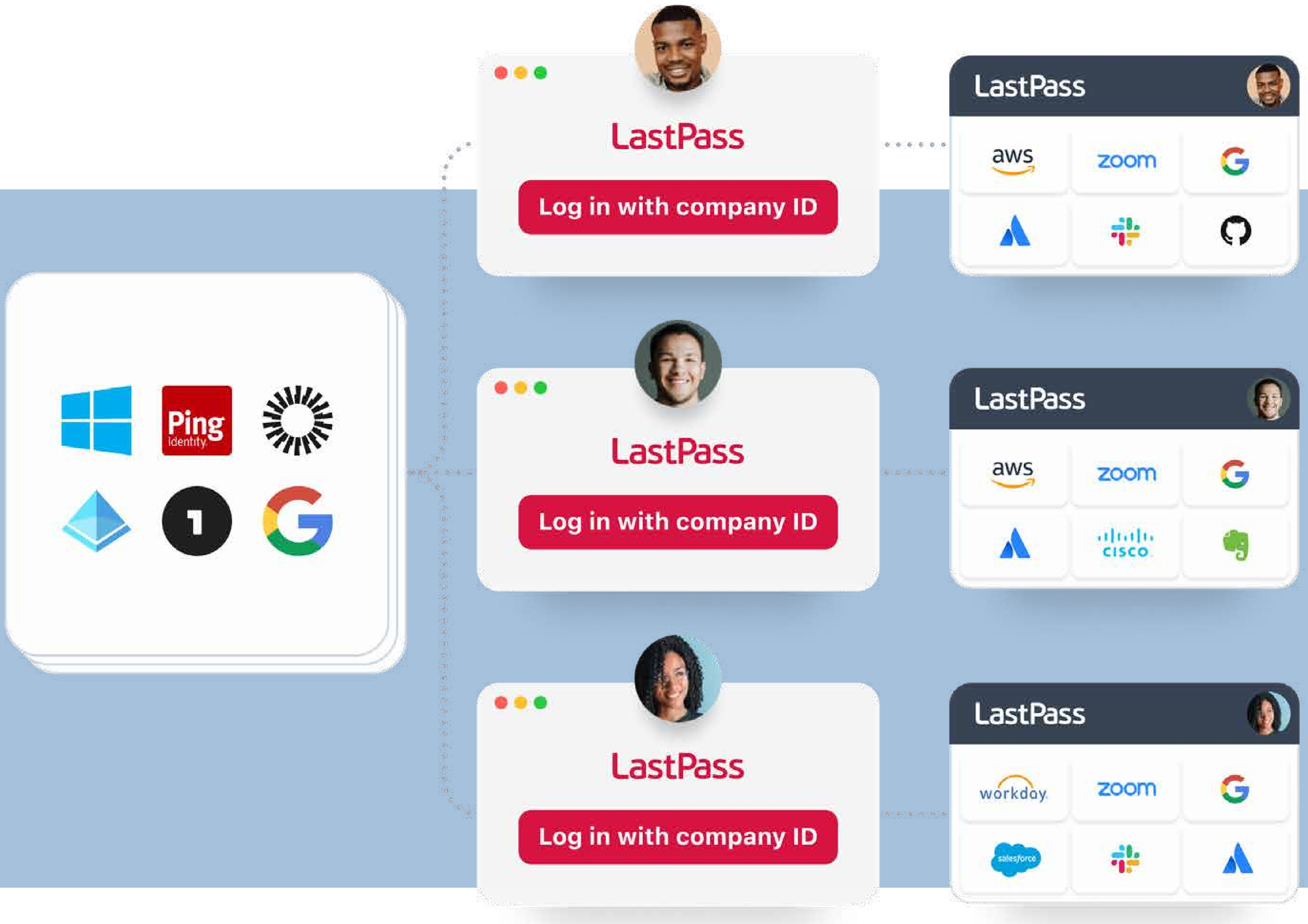
But the reality is, many of the tools employees use daily for collaboration, scheduling, file sharing, and marketing—like Canva or Monday.com—often fall outside of SSO coverage. These non-federated apps may rely on locally stored passwords, shared credentials, or weak authentication methods. Worse, they may not even be visible to you.

That creates risk. Unmonitored, under-protected accounts become easy entry points for attackers and increase the potential for internal misuse.

What a password manager adds to an IdP:

- Pairing your IdP with a password manager closes the gaps that SSO leaves behind—extending secure access to every app, including those not yet integrated into your identity ecosystem.
- Password management scales credential security across your environment, helping employees adopt strong authentication practices while giving you better visibility and control.

Together, your IdP and password manager create a unified identity and access strategy that secures every login, not just the ones you already know about.



PASSWORD MANAGER + SIEM/XDR

Better Signals, Fewer False Alarms

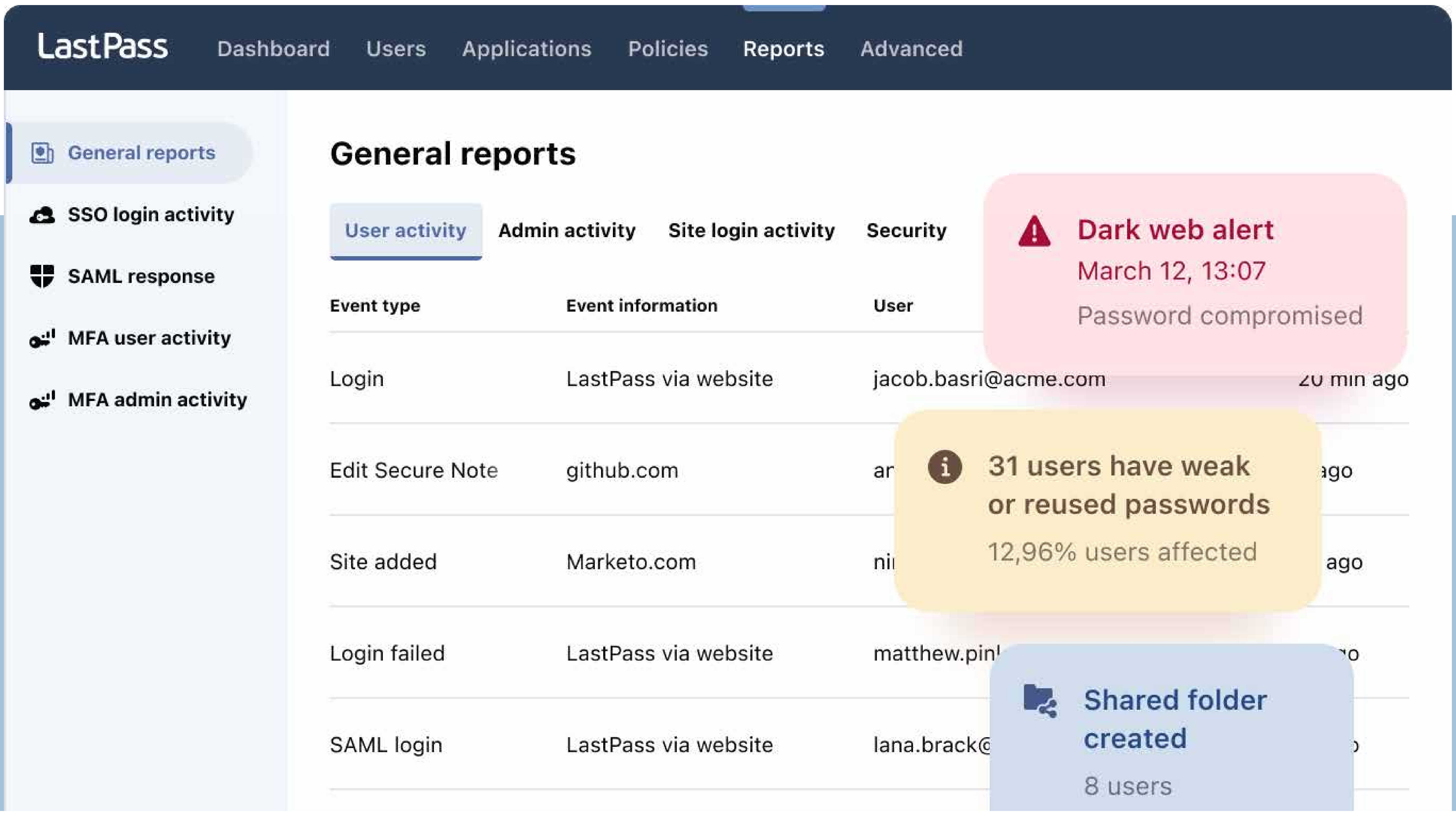
Businesses use Security Information Event Management (SIEM) to collect and analyze security data from endpoints, networks, and cloud environments. Extended Detection and Response (XDR) platforms take this further by correlating signals across these systems to provide a broader and more unified view of threats and accelerate response.

However, without credential management, common issues like reused passwords, shared accounts and weak authentication practices can create unnecessary noise, leading to false positives and obscuring real threats.

How credential management enhances SIEM and XDR:

- Reduces signal noise by enforcing strong and consistent password hygiene, allowing security tools to focus on true risks and not basic human behavioral mistakes.
- Improves incident context by providing visibility into who has access to what and when, helping teams identify compromised accounts quickly and with high confidence.

Integrating credential management with SIEM and XDR sharpens threat detection, reduces operational inefficiencies, and strengthens your overall security posture by addressing the weakest link—user credentials.



General reports

Event type	Event information	User	
Login	LastPass via website	jacob.basri@acme.com	20 min ago
Edit Secure Note	github.com	ar	ago
Site added	Marketo.com	ni	ago
Login failed	LastPass via website	matthew.pin	o
SAML login	LastPass via website	lana.brack@	

Dark web alert
March 12, 13:07
Password compromised

31 users have weak or reused passwords
12,96% users affected

Shared folder created
8 users

PASSWORD MANAGER + EDR/MDR

Protect the Endpoint and the Entry Point

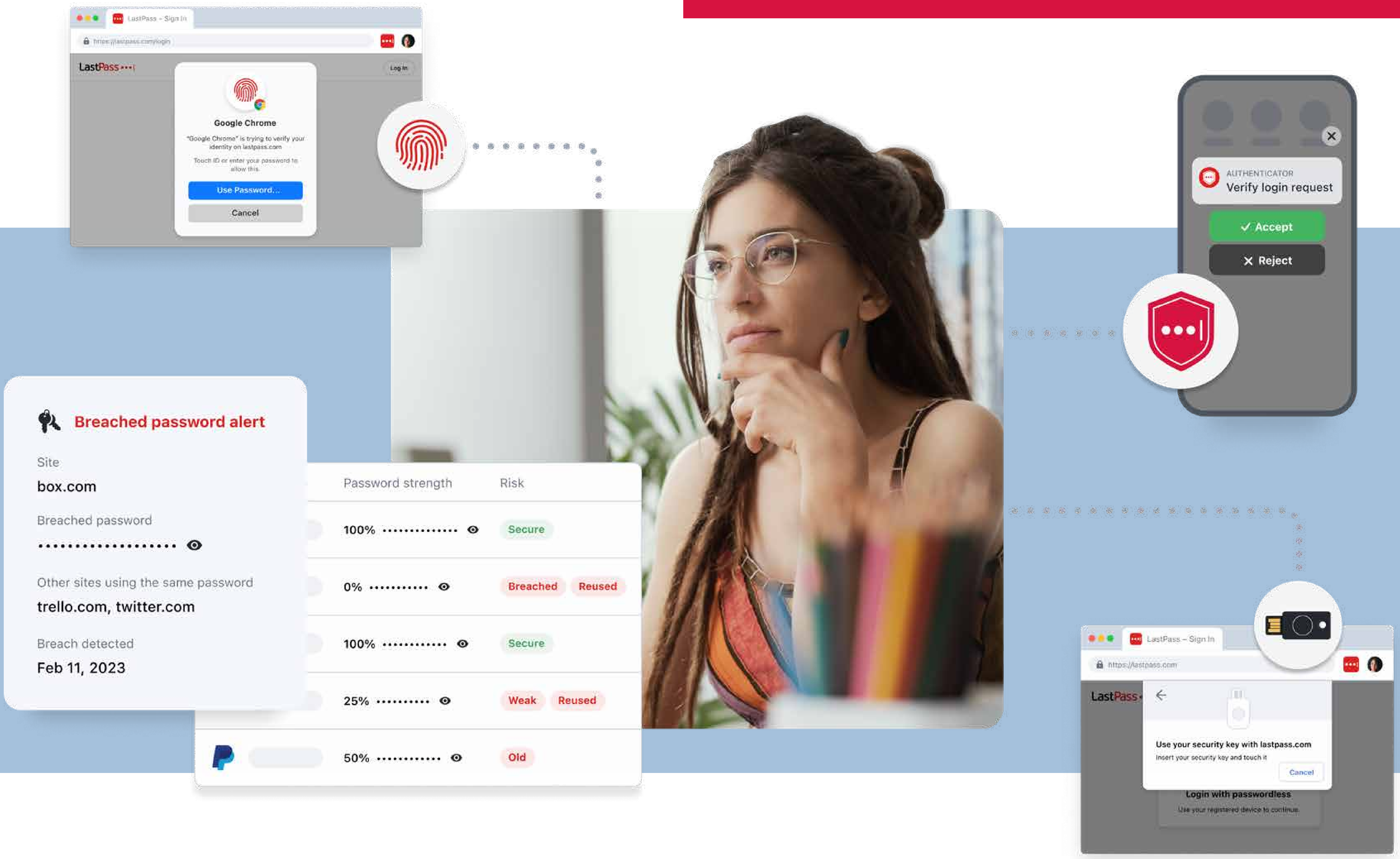
Endpoint Detection and Response (EDR) protects individual devices (laptops and desktops) while MDR (Managed Detection and Response) extends visibility and threat detection across your entire environment.

But even the most advanced EDR or MDR solutions are less effective without strong credential hygiene. Compromised passwords, shared accounts, and poor access practices can allow threats to bypass detection altogether.

What credential management adds to EDR/MDR:

- Establishes a preventive control that stops unauthorized access before it reaches the endpoint.
- Reduces the risk of credential-based attacks, insider threats, and account takeovers, improving overall detection accuracy.
- Enhances MDR's correlation of events by providing user-level context that links access behaviors with potential threats.

Together, password management and EDR/MDR strengthen both prevention and response, giving you a more complete and resilient security posture.



"Google Chrome" is trying to verify your identity on lastpass.com

Touch ID or enter your password to allow this.

Breached password alert

Site
box.com

Breached password
••••••••••••••••••••

Other sites using the same password
trello.com, twitter.com

Breach detected
Feb 11, 2023

Password strength	Risk
100% ••••••••••••••	Secure
0% •••••••••••	Breached Reused
100% ••••••••••••	Secure
25% ••••••••••	Weak Reused
50% ••••••••••••	Old

Use your security key with lastpass.com

Insert your security key and touch it

Use your registered device to continue.

LastPass

PASSWORD MANAGER + BDR

Backup Your Business and Protect the Keys to Recovery

Backup and Disaster Recovery (BDR) solutions help you minimize downtime, protect data, and bounce back from cyberattacks or system failures. But without secure credential management, recovery can be delayed or compromised altogether.

Weak or poorly managed credentials create gaps in access control, increasing the risk of credential theft, brute force attacks, and unauthorized access during high-stress recovery periods.

What credential management adds to EDR/MDR:

- Ensures critical credentials are securely stored and accessible only to authorized personnel during system restoration.
- Reduces recovery time by making the right credentials available immediately, minimizing disruption and helping teams act with confidence.
- Strengthens your overall resilience by preventing credential-related vulnerabilities from undermining your recovery plan.

In a crisis, every second counts, and a password manager ensures you are never locked out when it matters most.

LastPass

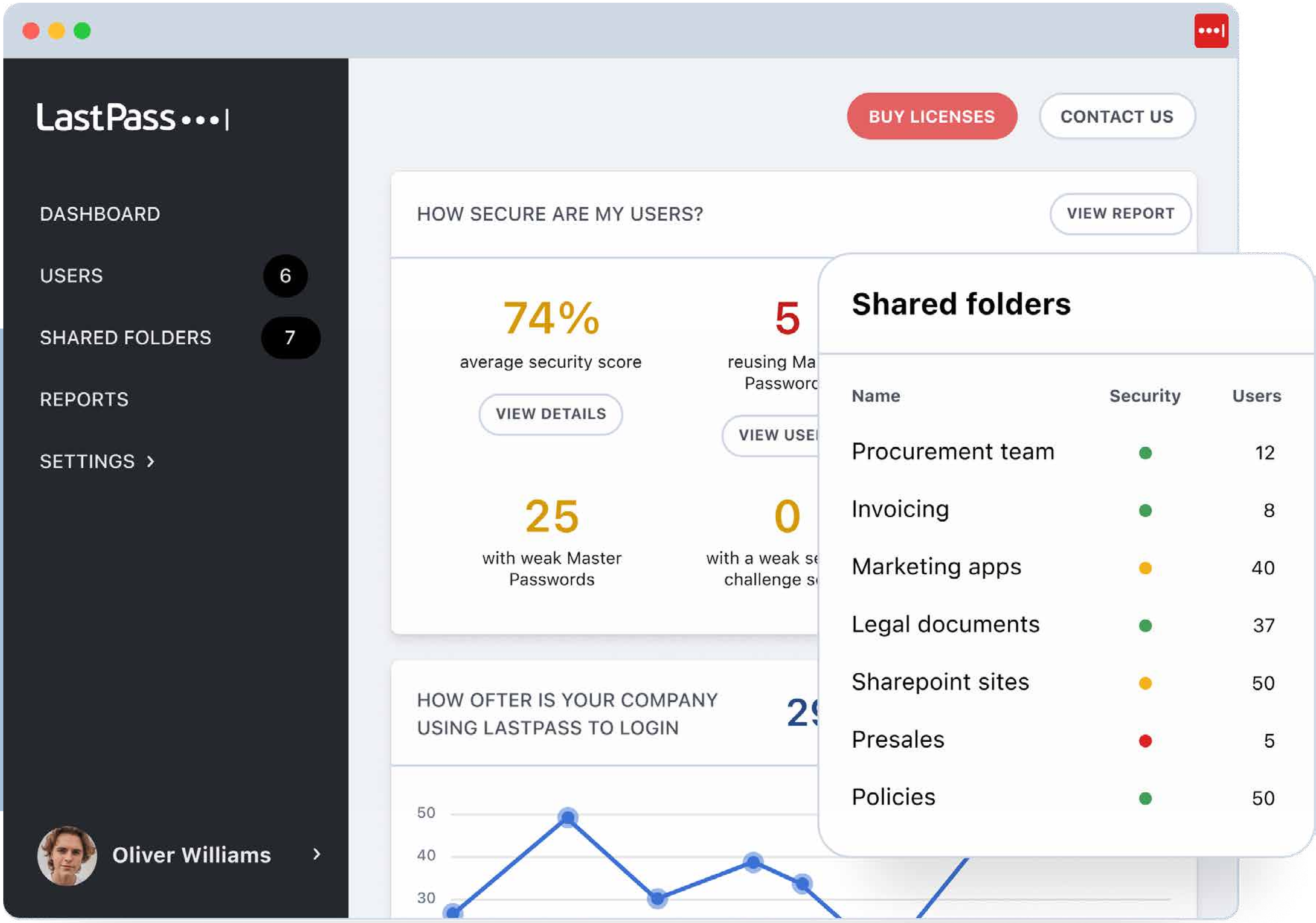
Strong Security Begins with Robust Credential Management

You've invested in powerful security tools. But without credential management, you're not getting the most out of your investment.

A password manager, like LastPass, makes each part of your security stack more effective, giving your customers the holistic protection they deserve:

- Your identity provider becomes more reliable
- Your endpoints and email mailboxes are harder to bypass
- Your threat data becomes more actionable

And in the event of an incident, your remediation and recovery are quicker.



HOW SECURE ARE MY USERS?

74% average security score

5 reusing Ma Passworc

25 with weak Master Passwords

0 with a weak se challenge s

HOW OFTER IS YOUR COMPANY USING LASTPASS TO LOGIN 2

Shared folders

Name	Security	Users
Procurement team	🟢	12
Invoicing	🟢	8
Marketing apps	🟡	40
Legal documents	🟢	37
Sharepoint sites	🟡	50
Presales	🔴	5
Policies	🟢	50

LastPass: Easy, Affordable Password Management

LastPass isn't just an award-winning password manager. It's your trusted Partner to boost customer security.

Partnering with LastPass allows you to:

✓ **Log in with ease:** Securely manage how your customers store and use passwords and passkeys.

✓ **Control who gets access:** Make sure the right people have access to the right apps, systems, and data — nothing more, nothing less.

✓ **See what's happening:** Know which apps your customers are using, when, and how. Stay informed, spot issues early, and feel confident that everything is running smoothly.

But the benefits of LastPass are matched only by its ease of use:

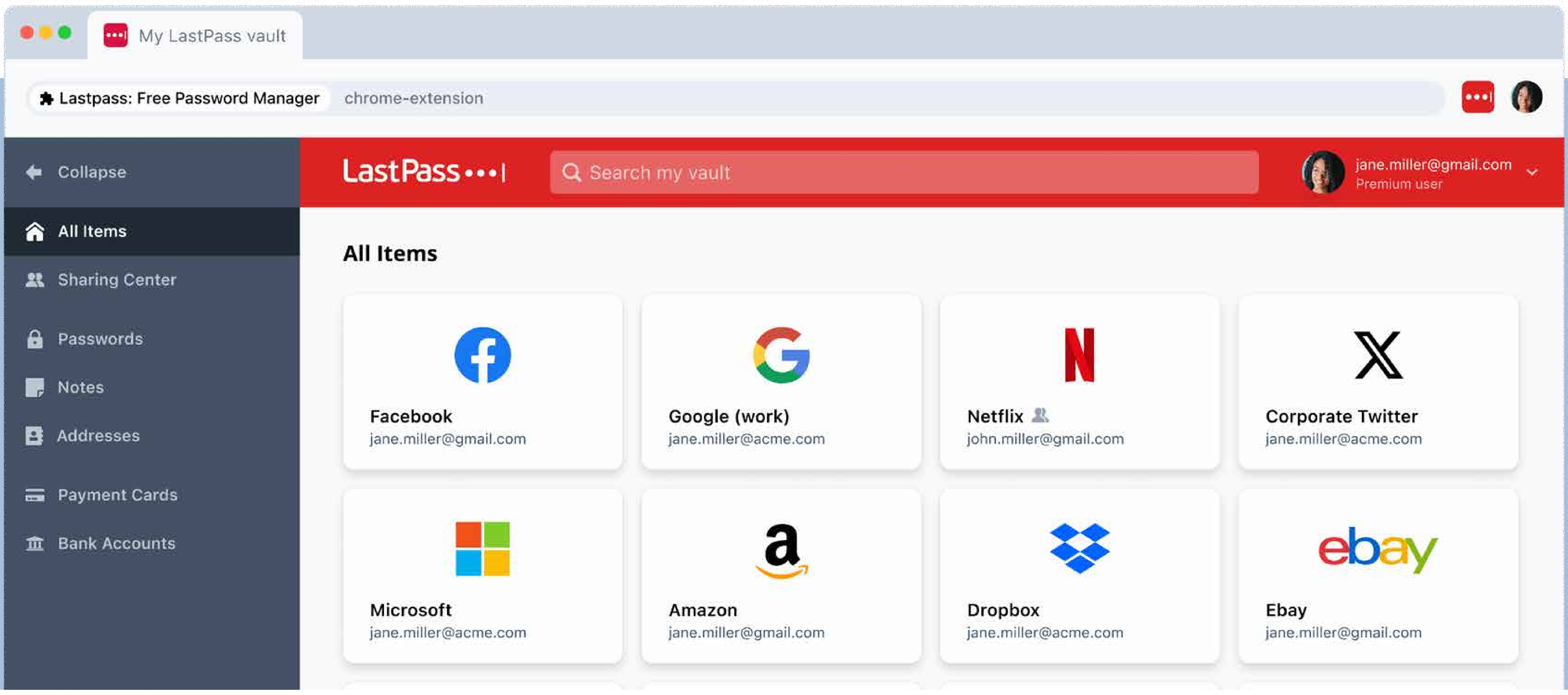
- Easy to set up—no complicated installs or tech headaches.
- Works for everyone, whether you are a tech pro or not, right from day one.
- Affordable and grows with your customers' businesses, whether big or small.

Credential management empowers your customers to make better security choices. It gives you better insight to prevent threats from manifesting into attacks. It makes you more resilient when recovering from incidents. And it makes all your other security tools more efficient.

It is an essential layer of security that you cannot afford to live without.

Reach out to the LastPass Partner team to learn more about incorporating LastPass into your security stack.

Contact Partner team


My LastPass vault
Lastpass: Free Password Manager
chrome-extension
LastPass•••|
Search my vault
jane.miller@gmail.com
Premium user
Collapse
All Items
Sharing Center
Passwords
Notes
Addresses
Payment Cards
Bank Accounts
All Items
Facebook
jane.miller@gmail.com
Google (work)
jane.miller@acme.com
Netflix
john.miller@gmail.com
Corporate Twitter
jane.miller@acme.com
Microsoft
jane.miller@acme.com
Amazon
jane.miller@gmail.com
Dropbox
jane.miller@acme.com
Ebay
jane.miller@gmail.com