PROTECTING THE NEW PERIMETER:

1Password

Addressing the identity crisis in hybrid work

The hybrid work era is here. Work can happen anywhere: in the office and at home, at coffee shops and coworking spaces, on laptops and phones and tablets. And to get that work done, employees want the flexibility to pick the best app for the task. Today the average organization uses more than 125 different apps.

In the past, companies could rely on technologies like single sign-on (SSO) and network firewalls to protect company data on company-managed devices and apps.

In a hybrid world, that approach is no longer enough.

Four considerations to securing your hybrid workforce:

1. ✓ **Identity:** How do you validate the person signing in is actually that person?
2. **Shadow IT and BYOD:** How can you ensure security when access can be from any device or to any application–even those not managed by IT?
3. **Security adoption:** How do you drive adoption of critical security tools while ensuring that productivity is not compromised?
4. **Security costs**: How can you make sure that your investments in security tools are actually worth the cost?

Identity by the numbers

- 70% of breaches in 2023 still involved an identity element.[1]
- Forrester predicts that number will climb to 90% in 2024, in large part due to AI.[2]
- 49% of breaches in 2023 involved credentials.[1]
- 193 billion credential-stuffing attacks occurred globally in 2020 – a 360% increase from 2019.[3]

49%

of breaches in 2023 involved credentials.

1 2023 Data Breach Investigations Report (Verizon)
2 Predictions 2024: Cybersecurity, Risk, And Privacy (Forrester)
3 2021 State of the Internet / Security: Phishing for Finance (Akamai)

The days of badging into a building and signing onto a network are long gone. Welcome to the new era of needing to validate a user's identity and secure access regardless of location, device, or application being used.

This change has broken the traditional approach of using an identity provider (IdP) and single sign-on (SSO) provider to validate identities. SSO can help prevent credential leaks for managed apps, but today one in three apps used at work are still unmanaged – and unknown to the company.

When company-provided devices, secure networks, and VPNs are no longer part of the picture, how can you be sure that your company's data is protected? How do you ensure that protection spans every device and every app when there's no longer an office to badge into?

70%

# of breaches in 2023 still involved an identity element.

The 3 keys to verifying identity in a hybrid workforce

1 Provide a universal and secure login experience

Secure access to every application, on every device, for every person. The best enterprise password managers work wherever users are, and provide a universal sign-in experience across managed and unmanaged apps. Critically, they help generate strong, unique logins for your entire application estate, especially for apps outside your direct control. This can help reduce the risk of weak or reused credentials being used in credential stuffing or brute force attacks.

2 Identify threats and understand company risk

The best enterprise password managers can identify and alert users and administrators when a password is compromised in a third-party breach, or if it's weak or reused elsewhere. By constantly monitoring your organization's security posture, you can stay one step ahead of the attackers.

3 Follow the principle of least privilege

The principle of least privilege is a security philosophy that is focused on ensuring that the least amount of access possible is provided to each employee. By only providing the least amount of access needed for each person to do their job, your overall risk and breach surface is reduced in the case of a breach. This approach also helps to reduce the risk associated with privilege escalation to gain additional unauthorized access.

Your business needs 1Password

1Password was built to secure hybrid workforces, making it easy to:

- Protect company data in both managed and unmanaged apps. Ensure your employees can secure any app with strong, unique credentials while giving them the flexibility to choose their own apps for work.
- Prevent breaches with active threat detection. Spot security issues quickly with a single view that brings together data breaches, password vulnerabilities, and employee usage insights.
- Manage access to company data. Control which groups can access specific vaults, and limit who can create a vault or invite new users. You can also set custom policies – minimum password requirements or mandating two-factor authentication, for example – to align with company security policies.

For more information on how 1Password can help you secure your hybrid workforce, contact us.

1Password