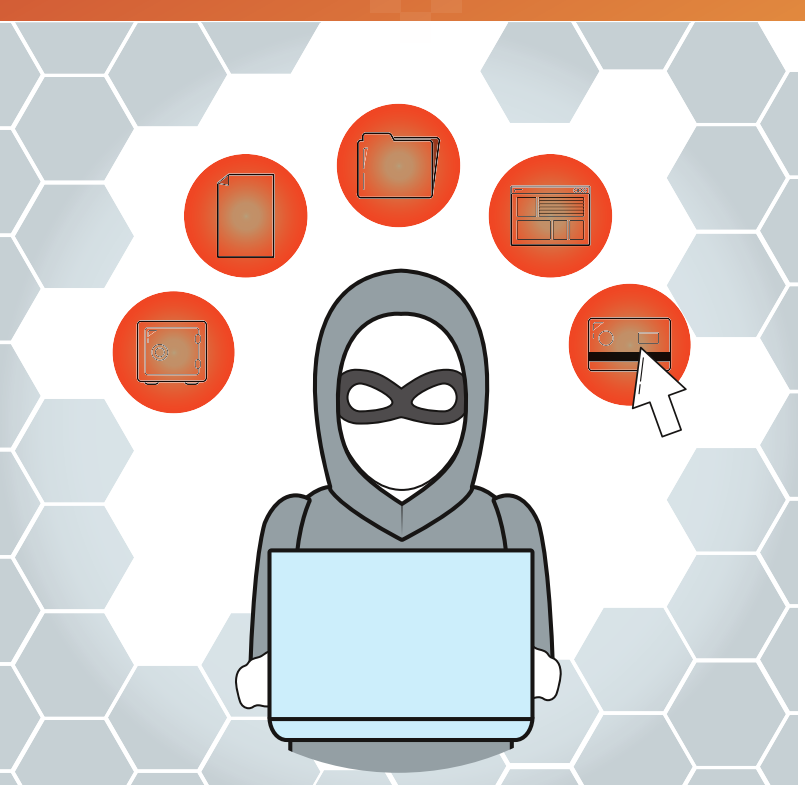
ONE PASSWORD FROM DISRUPTION

The remote workforce is rapidly expanding, and so are security risks. Single Sign-On (SSO) boosts security and user experience with one set of credentials across applications. Demand for SSO is reaching new levels—these stats explain why.



- **80% of data breaches in 2018 started with a weak password**
- **29% of all breeches are powered by stolen credentials**
- **Spear phishing messages connected to ransomware have an engagement rate 6x higher than actual emails**
- **Ransomware attacks increased by 12% last year costing organizations more than $8B**
- **Downtime from ransomware alone costs organizations $64,000 on average**

HOW DOES SINGLE SIGN-ON WORK?

When you try to log onto an app or a website...

Step #1

The website first checks to see whether you've already been authenticated by the SSO solution, in which case it gives you access to the site.

Step #2

If you haven't, it sends you to the SSO solution to log in. You enter the single username/password that you use for corporate access.

Step #3

The SSO solution requests authentication from the identity provider or authentication system that your company uses. It verifies your identity and notifies the SSO solution.

Step #4

The SSO solution passes authentication data to the website and returns you to that site.

Step #5

After login, the site passes authentication verification data with you as you move through the site to verify that you are authenticated each time you go to a new page.

PASSWORD FATIGUE IS REAL

35%
Organizations who actively cross check credentials with common password lists

500+
Average number of hours a company sends on password resets each year

73%
User accounts online who use duplicate passwords

37%
Organizations who require unique passwords for more than 25 applications

6
Number of unique passwords used to arm 4x as many accounts on average

2:5
Had a password stolen, an account hacked, or a compromised account

3 IN 10 PEOPLE TRUST IN PASSWORDS

Q

Why a 16-character password?

A

187 nonillion combinations

IDEAL PASSWORD

R?d#5PuF3dcW8D/@

Fortify your password with a **16-character password** that includes lower case, upper case, numbers and all special characters on a standard keyboard.

Mitigate risks while increasing productivity with LastPass by LogMeIn. Users can have their passwords remembered on every app and every device with multi-factor authentication available for an extra layer of security.

Email solutions@microage.com to get started.

LogMeIn®

MicroAge®
The Digital Transformation Experts