onelogin

EBOOK

Prevent Laptop Security Breaches —No Active Directory Required

Introduction

The Battle to Secure All Endpoints

Corporate data spreads across an ever-growing number of applications. Users (employees, contractors, partners, and customers) access those applications over a wide range of devices.

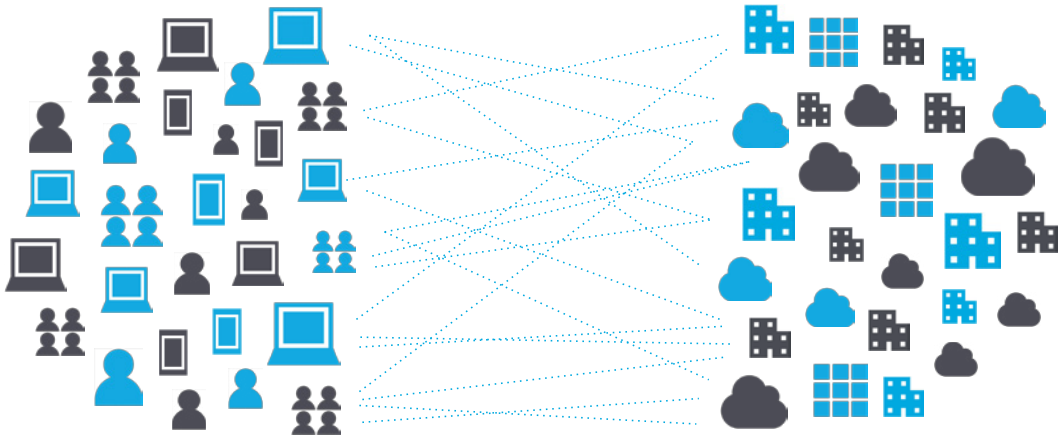
Those devices take different forms: desktops, laptops, tablets, smartphones, smartwatches. Each device may use a different operating system.

The locations from where people access your data can be on-premises or off, and in any number of places around the globe.

Data, users, apps, devices, locations—the sheer number of permutations and combinations is mind-boggling. This complex nature of today's IT environment opens security gaps and exposes your business to undue risk.

To illustrate, try to envision all the permutations and possible entry points for risk in your organization. Imagine that you have 400 users, each using 25 apps. When you multiply those together, that's 10,000 potential access permissions to manage.

INCREASING IT COMPLEXITY



Thousands of employees, partners, customers, and multiple devices ...

Working with many, many apps, both in the cloud and on-premise.

Access permissions change as users come and go, roles change, new apps are added, and older apps are decommissioned. Your business battles continuously to align its productivity needs and security needs with the organization. But with explosive growth and expanding access permissions, it's easy to see how security gaps occur.

The effects can be significant. As you fight this battle, your business wastes time and resources in so many ways:

- Manually onboarding and offboarding users
- Chasing down zombie accounts of former employees
- Allocating budget to unused application licenses
- Losing visibility and control over who accesses which applications, and from where
- Helping employees manage the passwords needed to access their applications
- Clashing with users who choose weak or static passwords
- Wasting help desk resources on login trouble and password resets

Whether you're a fast-growing tech company or a well-established multinational, managing this complexity is a costly burden that slows you down, and ignoring this complexity opens your business to harmful security risks.

Today's Laptop Security Gaps: Two Groups Traditional IAM Vendors Have Failed

Traditional IT solutions have included a company directory and traditional identity solutions have helped secure it. However, these break under the new business and productivity trends, such as masses of remote workers and the SaaS Tsunami.

IT has the challenge of balancing security and productivity by securing all endpoints in an efficient manner. This challenge is most notable in two significant groups: cloud natives and Active Directory exiles. Let's define these groups before explaining their unique security challenges.

Cloud natives are companies born in the cloud, and business units inside companies that use a cloud-first strategy. All their software is as-a-service with nothing on-premises. These companies strip away all activities that distract from their corporate strategy. They focus on their business purpose first and refuse to be drawn in by the aggravation of installing and maintaining on-premises software.

Conversely, **Active Directory exiles** are users in established companies who cannot access corporate on-premises Active Directory instances. Their identities go unmanaged and their machines go unsecured, all because they cannot access Active Directory.

Without a directory, IT lacks the features that provide strong authentication. Weak authentication results in the following:

- Flimsy passwords that are easily guessed
- Static passwords that users never change—which can be often purchased by hackers since people tend to use the same passwords across apps
- Sessions that cannot be revoked, giving unauthorized users access to data via lost or stolen devices
- No multi-factor authentication (MFA) that would prevent access from stolen or lost machines
- Manual password resets taking up the precious resources of your help desk
- No quick remedy for compromised accounts, like forcing immediate password resets

WEAK AUTHENTICATION = SECURITY RISK

Specific Challenges of Cloud Natives

As cloud natives grow, their need to access an increasing number of applications also grows. It starts with the common apps like email, document editing, file sharing, and messaging that everyone uses, and then grows to apps that power specific departments, like Sales, HR, Financing, and Operations, and have very particular functionality.

As they grow, cloud natives see the need to manage identities that access those apps. They must ask, “Who can access which app with which permissions?” And do that reliably, whether onboarding, crossboarding, or offboarding, in the face of rapid company growth and often in the turbulent company organization structure that characterizes new businesses.

The challenge extends from the apps to the device, which companies strive to protect because those apps are at risk of being compromised or stolen. Not all, but many cloud-native businesses use Macs rather than PCs. As identity management becomes an issue, they may consider Active Directory as a possible solution, but soon realize that connecting Macs to Active Directory—whether on-premises or on Azure—is difficult, if not impossible.

Specific Challenges of Active Directory Exiles

Established companies face the same problem. However, they have a different starting point and different constraints than cloud natives. For example, they may have an on-premises Active Directory instance that works for in-office PC users. However, not everyone uses a PC, not everyone works exclusively from the office, and not everyone who accesses apps is a full-time employee.

These companies might have the following:

- Remote sales teams for whom VPN is, at best, annoying, and, at worst, blocks access to the apps they need to do their jobs
- Developers writing software on Macs: since connecting their machines to Active Directory is not an option, they remain unauthenticated and their user identities unmanaged
- Contractors, agencies, or external recruiters that need to access corporate data, but it's difficult to connect short-term and remote resources using Active Directory

These Active Directory exiles see no workable solution to store or manage their identities.

ECONOMIC IMPACT OF SECURITY GAPS

Even one compromised identity is one too many. Stolen credentials can lead directly to a security breach.

In the first six months of 2016, *64% of all data breaches were due to identity theft.* This should raise concern whether you're a cloud-native organization or have unsecured Active Directory exiles.

- In the first half of 2016 alone, *554 million data records were lost or stolen.*
- A recent study found *the average cost paid for each lost or stolen record containing sensitive and confidential information was $158.*
- Multiply stolen records by cost per record and data breach costs exceeded $87 billion in just the first six months. That comes to $174 billion a year.

Yes, $174 billion is a lot of money, but how does that figure relate directly to your company? The 2016 Cost of Data Breach study found that $4 million is the average cost of a data breach per company. As you can see, unsecured laptops and devices are a costly problem.

Extending a Flexible Corporate Directory to the Desktop Increases Security

Directories are the foundation of an efficient IT team in a productive company—for tasks such as building and scaling app deployments, accomplishing HR processes, and enforcing basic security policies (e.g. password complexity to battle weak authentication).

The challenges of efficiency are compounded by desktops and laptops. If we want employees to access apps from any device, do we just assume that all devices are immediately trusted? Do we ignore the risk of local laptop access?

Desktop security is vital for protecting data that is automatically accessible, such as synced Dropbox files, and preventing malware attacks. For example, a Mac with a weak password could be easily compromised, and the hacker could install a key logger to capture all the passwords.

Thus companies need to understand the need to have a strong identity solution that extends to the desktop or laptop. Explore how you can close laptop security gaps in the next section.

How OneLogin Desktop Helps Solve Your Security Challenges

At the core, OneLogin provides a cloud directory that secures a wide range of concerns across your organization: your users, apps, devices, existing infrastructure—and endpoints. Through OneLogin Desktop, you can control your endpoints and secure all laptop user profiles.

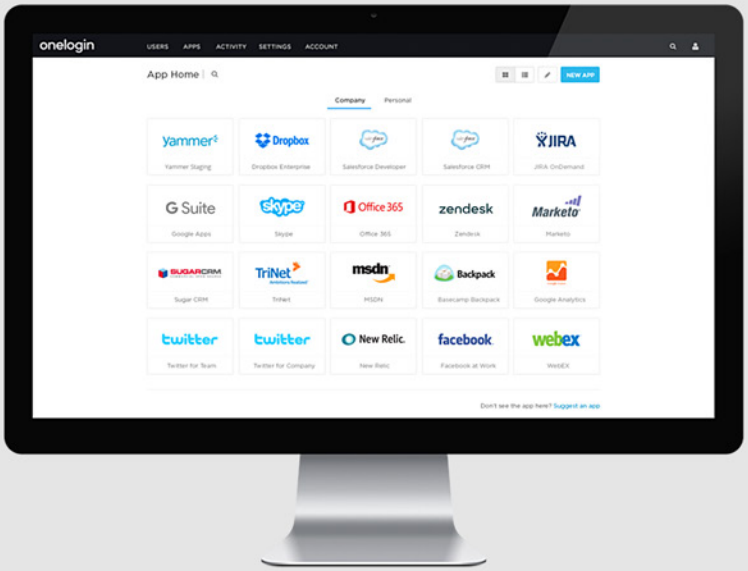
How OneLogin Desktop Works

OneLogin Desktop enrolls your laptops and desktops with OneLogin Cloud Directory. This enrollment creates a secure profile on your machine that can only be accessed with your OneLogin credentials. Once you log in to your new, secure profile, you can access web and desktop apps without entering your credentials again. This is a form of single sign-on (SSO) that OneLogin calls “machine SSO”.

ONELOGIN “MACHINE SSO” COMPARED TO MDM

The term “machine SSO” may make you wonder how OneLogin compares to mobile device management (MDM) software.

OneLogin is different from, yet complementary to MDM. Whereas MDM tools manage the machine itself—helping administer imaging, patching, and consistent settings, OneLogin Desktop manages the profile on that machine, securing it against unauthorized use. Once a user profile is trusted, it can be used in OneLogin policies, which will map the user’s identity to the right level of access to the right apps. This approach has a smaller footprint and is easier to distribute than MDM, which requires a wider, labor-intensive rollout.



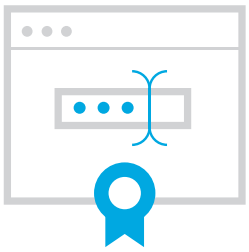
Painless Multi-Factor Authentication

OneLogin Desktop installs a certificate specific to a user and a device which provides a first authentication factor. When users log in using their Windows or OS X password, they provide a second authentication factor. These two factors authenticate users into their OneLogin portal, enabling them to access their SaaS applications with a single click.

HOW ONELOGIN DESKTOP WORKS

1st Authentication Factor

OneLogin Desktop installs a certificate specific to a user and laptop, providing a **first** authentication factor.



2nd Authentication Factor

When users log in using their Windows or OS X **password**, they provide a **second** authentication factor.

User Authenticated into Portal

These two factors authenticate users into their OneLogin Portal, enabling them to access SaaS applications with a single click *—no additional login required.*

In other words, once you log in to your operating system, you do not need to log in again to access your OneLogin application portal or SAML-enabled web and desktop apps. Unlike other identity products, you only log in once. This is true SSO.

Supported Systems

OneLogin Desktop supports current versions of Mac and Windows operating systems, as well as Chrome, Safari, and Edge browsers.

Windows 7 is not supported because mainstream support by Microsoft ended in 2015. Windows 8 is not supported because it has little market share. The Firefox browser is not supported because they have a proprietary keychain that makes it difficult to integrate with security software such as OneLogin.

SUPPORTED ENVIRONMENTS

		Mac	Windows
Operating System	Supported	OS X 10.10 Yosemite OS X 10.11 El Capitan macOS 10.12 Sierra	Windows 10
	Unsupported	OS X 10.9 Mavericks & earlier	Windows 7 Windows 8
Browser	Supported	Chrome Safari	Chrome Edge
	Unsupported	Firefox	Firefox

Windows 7
End of Life: 2015

6% Marketshare

Proprietary
Keychain

What You Gain With OneLogin Desktop

With OneLogin Desktop, IT gains the following benefits:

- Stronger authentication and lower risk
- Ability to discover lost or compromised devices
- Time savings with true SSO
- Improved IT effectiveness

OneLogin also integrates with existing directories and complements MDM tools.

Stronger Authentication and Lower Risk

Because OneLogin Desktop binds laptops to the cloud, all users simply use their corporate credentials, which are typically under a strong corporate security policy. These policies can include the following:

- Password complexity—ensure passwords are not easily guessed
- Password rotation—i.e. if a password is guessed, it will be replaced with a different one
- Password uniqueness—preventing password reuse for a set time

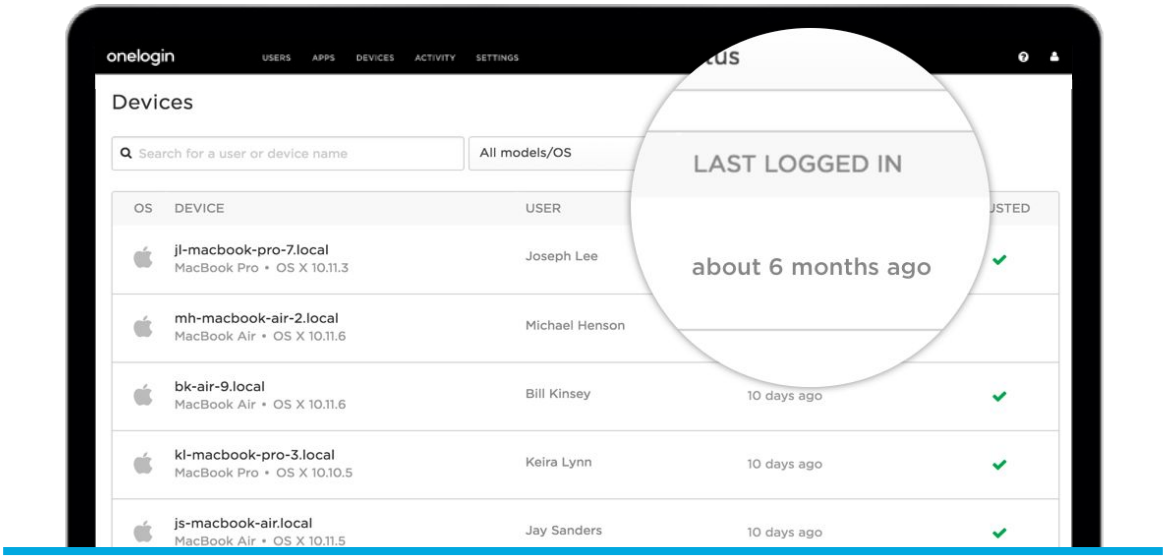
You'll face less risk that an attacker using an unattended laptop can access an app they shouldn't. You'll also benefit from MFA thanks to the certificate that OneLogin Desktop installs on the machine. For cloud natives, you stay secure as you grow. For established companies, your Active Directory exiles are finally brought into compliance with company password standards.

Ability to Discover Lost or Compromised Devices

OneLogin Desktop reports when someone last logged in from a device. If it's been a while, it's possible the device has been lost or stolen. You can also see which devices have a certificate installed by OneLogin Desktop. Again, the certificate provides an additional factor when logging into the OneLogin app portal.

Additionally, OneLogin shows which laptops have MFA and which don't. This ability lets you see how MFA is employed across all your laptops. You can then plug security gaps in laptops without a certificate. If a laptop is compromised, lost, or stolen, it's easy to block its access to the cloud directory, and therefore from your SaaS applications.

DISCOVER LOST LAPTOPS



Time Savings with True SSO

Because OneLogin Desktop makes it so easy to access apps, users save time. It's so simple: log in to your device, open your browser to the app portal, and click the app you want to access. The time savings of true SSO add up.

If you're offline, OneLogin uses your last good hash to authenticate your password. When you go back online, OneLogin validates that hash against your current password and picks up any new password that you've switched to. Additionally, when an employee leaves your company and is deprovisioned from the OneLogin directory, that person's login will be blocked. This is another way OneLogin secures your data at rest.

Improved IT Effectiveness

With OneLogin Desktop, an IT team can focus on important projects instead of software installs, password resets, or server maintenance.

Self-Service Setup

With the flip of one switch, IT teams can enable users to simply download and install OneLogin Desktop. Self-service installation makes less work for IT, which proves extremely helpful during periods of growth. For example, some OneLogin customers tell their new employees to buy a Mac, expense it, install OneLogin Desktop and authenticate their machine against the OneLogin Cloud Directory.

> "OneLogin Desktop is the missing piece of the puzzle that we've been waiting for. We can finally get rid of our internal directory and have users not only authenticate to the cloud but bind our entire fleet of Macs directly to the cloud. We knew this day would eventually come, and we're really excited to be partnering with an innovative company like OneLogin to make it happen."
>
> –TIM SCHWARTZ, Director of Innovation, Whitby School

Fewer Service Desk Loads

After installation is complete, the simplicity of using OneLogin means less confusion for users and that means fewer questions coming to your service desk. In a recent review of 730,000 help desk requests, one company found that a help desk employee spends 104 hours per year managing password resets. Multiply the salaries of your help desk team by those hours and you easily see how the costs of those requests add up. Add to that the time wasted by employees who are locked out of their applications. True SSO limits the number of passwords an employee needs to remember. If they forget, IT can use OneLogin to empower users to do self-service password resets. OneLogin can also automatically prompt end users to change their Active Directory password.

No On-Prem Maintenance

OneLogin Desktop does not require IT teams to install, maintain, patch, or secure their own AD instance. For cloud natives who don't need AD, they can have the necessary security without adding on-premise complexity.

Integration With Existing Directories

Sometimes companies must contend with legacy directories such as Active Directory, LDAP, or even Google Cloud Directory after a move to Google Apps. The OneLogin Cloud Directory syncs with all these directories in real-time. If you want to secure all your laptops and devices, but you cannot unplug your Active Directory or your LDAP directories, OneLogin enables you to migrate to the cloud while maintaining your legacy systems.

Integration for HR-Driven Identity

OneLogin makes a closed, fully automated loop when connected to your human capital management (HCM) apps. These include apps like Workday, UltiPro, and Namely. When a new employee joins your firm and HR adds him or her to your HCM app, that identity is automatically synced into OneLogin Directory, where it can be used by OneLogin Desktop.

OneLogin can also provision the new identity into legacy Active Directory and LDAP directories. If you use the System for Cross-domain Identity Management (SCIM) standard, OneLogin can provision the new identity into on-premises applications. The new user gets SSO to all appropriate SaaS and on-premise apps. For cloud-native companies experiencing rapid growth, HR-driven identity (HDI) ensures that employees are properly onboarded. As an established company with complex directories and identities to keep in sync, HDI properly manages app access for all your users.

What happens when an employee leaves the company? OneLogin's integration with HR-driven identity means that as soon as HR makes that change in the HCM app, OneLogin will automatically deactivate the user account. Additionally, OneLogin provides offboarding checklists, which work for two kinds of tasks:

1. Automated tasks, where OneLogin automatically deprovisions the user from an app using that app's user management API
2. Manual tasks, performed when an app doesn't have a user management API

These checklists ensure that nothing falls through the cracks and you have no zombie accounts as easy points of entry for a hacker.

Summary

OneLogin Desktop was designed to be simple. Why? IT is complex enough.

As the volume of data, users, devices, apps, and locations grows, your security gaps and risks grow too. If those risks become real and threaten your company, the costs can reach into the millions.

Cloud-native companies and established companies with Active Directory exiles face significant risks from these security gaps. OneLogin Desktop was built to address those two groups in particular.

By focusing on endpoint management and user identity, OneLogin allows the right access to the right person accessing the right apps. With MFA and true SSO, OneLogin Desktop makes identity and access management even easier for your users.

OneLogin Desktop also removes the burden from your IT team. Rather than focusing on password resets, software installation, and server upkeep, IT can spend time focused on your core business.

Lowered risk. Greater productivity. Core business focus.

OneLogin is the comprehensive identity and access management solution you've been looking for.