ivanti

Secure Cloud Access Without Passwords

Ivanti UEM holds the key

Securing cloud services

As your business moves to the cloud and adapts to the Everywhere Workplace, providing secure access that doesn't impede productivity is critical – and extremely challenging. Because password-only security is no longer up to the task, relying on it presents a tremendous risk.

The good news is that you already hold the key to protecting your mobile and cloud resources. By leveraging your existing Ivanti UEM, you can achieve zero trust security. Adding Ivanti Access allows you to eliminate passwords and strengthen your company's entire security posture – anywhere.

This eBook explores how you can better secure access to your enterprise cloud services by taking your security requirements anywhere your digital infrastructure takes you. Learn how Ivanti's zero trust security enables your organization to confidently adopt mobile-cloud technologies to drive greater business efficiency in the Everywhere Workplace while reducing the risk of data breaches.

Cloud-bound and security-challenged

Cloud-based technologies are becoming the default choice for more and more companies – a trend that has experienced a steep rise in the Everywhere Workplace. From Microsoft 365 to Salesforce and Dropbox, most organizations are either aggressively adopting cloud services or are being forced to as users bring them in. They introduce significant business efficiencies – and a large security gap.

The adoption of mobile and cloud technologies is the new business landscape, but for many organizations, their security hasn't kept up. Protecting mobile and cloud resources from unauthorized or malicious access is one of the toughest challenges facing organizations today.

Securing them takes a different approach – a zero trust security approach that eliminates passwords and strengthens your entire security posture.

>45%

of all enterprise IT spending will be on public cloud services by 2026 – up from less than 17% in 2021.[1]

Why passwords fail

They aren't secure.

Users have their own way of managing passwords, often with cringeworthy work-arounds like password sticky notes and files named "Password". Many use the same password across multiple accounts. Add this to the relative ease with which hackers can steal passwords, and it's little wonder passwords are among the top causes of breaches – and are compromised faster than any other kind of data.[2]

They aren't smart enough.

Passwords only give you one piece of an intricate security puzzle: verifying user identity before granting access to cloud services. But you're no longer on tethered computers in a tidy, defined enterprise network. Access is now from anywhere, often on questionable Wi-Fi, via a variety of mobile devices, across a variety of apps. Passwords don't give any security context, such as the state of the device requesting access, the application, the network and possible threats on the device. Insight into each of these factors helps make the right access decisions.

Users can't stand them.

Ask anyone their opinion of passwords and the eye roll is similar. The complex combination of caps, numbers, symbols and unrepeatability creates a frustrating cycle of forgetting, resetting and lockouts. And as the number of apps your company uses grows, so too does the password memory challenge and hassle.

They're expensive.

The major issue with passwords is forgetting them. The cost of supporting password systems, including staffing and infrastructure, can be significant. As more work is done in the cloud on more systems with multiple login details, chances grow for problems to arise and workflow to be interrupted. In the enterprise, every minute wasted affects productivity, which in turn, directly affects revenue. On top of that, when a user is locked out of their account due to a lost or forgotten password, it's often not just that user that is prevented from being productive, but the helpdesk employee they enlist to reset their password as well.

There's a better way.

The productivity benefits of your mobile and cloud resources need not be diminished by using frustrating and ineffective passwords to secure access. You can eliminate the pain of passwords and strengthen your security by building upon your existing Ivanti UEM to create a zero trust security approach that supports your mobile-cloud technologies. Let's take a look at how that's achieved by adding **Access and Mobile Threat Defense** solutions from Ivanti.

The power of zero trust security for the Everywhere Workplace

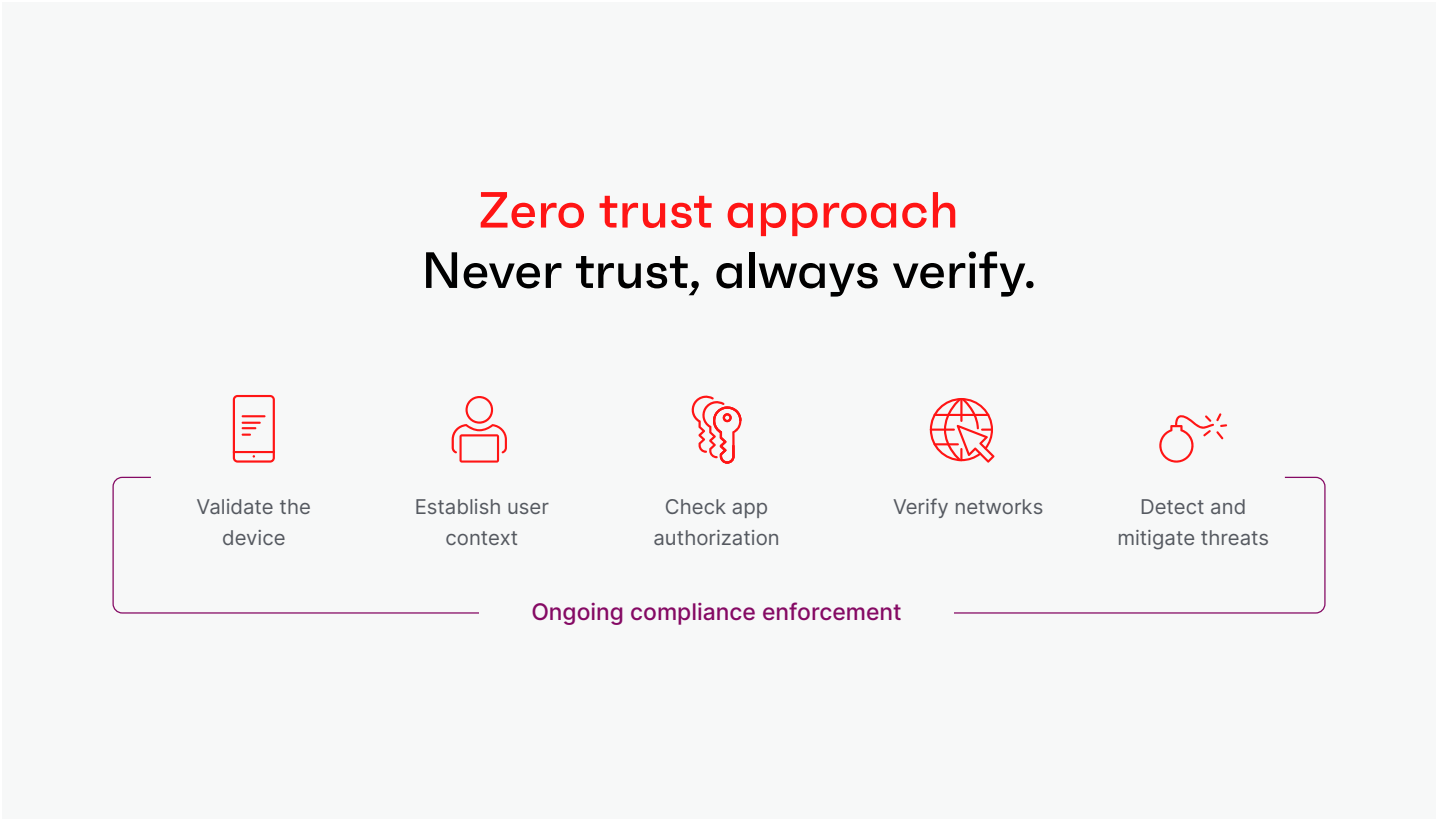
For companies that rely on cloud platforms and apps to move their business forward, our zero trust approach security is ideal.

It allows you to grant access to your cloud services only after receiving far greater security context than passwords can provide.

Access: stronger security without passwords

Your existing Ivanti UEM gives you the foundation to redefine your security strategy and achieve end-to-end, zero trust security by turning your device into your secure identity to the enterprise.

By adding Ivanti Access, you'll have a more complete security snapshot before granting access to any cloud service or app. Ivanti Zero Sign-On (ZSO), residing of the Ivanti Access platform, verifies critical signals for greater security context before granting access – without a single password.



Smarter, secure access to the cloud

More context, security and freedom

With Access, ensure that business information is only available to verified users on authorized endpoints, apps, and cloud services – all without a single password. Consider the advantages:

Passwordless experience

With ZSO, Ivanti has eliminated the password once and for all.

We turned a mobile device into your ID and secure access, for a seamless authentication experience from anywhere. Users can securely access any business app, device or resource with a glance or a tap of their finger. No passwords required. Just simple, passwordless access from anywhere.

Secure access from any device, whether you manage it or not

Whether Android, iOS, macOS, or Windows 10 or 11 devices, our standards-based platform is device agnostic to provide passwordless access from any device – even those not managed by your organization. That means not a single unauthorized device, app or network can connect to your business systems.

Cloud service freedom with standards-based security

Our zero trust security is built on a standards-based platform that allows you to deploy a common security framework across all of your cloud services. Whether it's Microsoft 365, Salesforce or an internally developed app, Access can protect any enterprise app and is designed to meet evolving business needs.

Data protection, wherever it lives

Mobile Threat Defense

The third leg of our zero trust security approach is Ivanti Mobile Threat Defense (MTD).

Immediate, on-device threat protection

Protect against device, app, network and phishing attacks even when the device is offline. Receive unmatched detection of known and zero-day mobile threats with machine-learning algorithms on-device, and local remediation actions with local user notification, across iOS and Android devices.

100% user adoption

A single app makes it easy to deploy and manage for every user, because threat protection is built into the Ivanti UEM client. That means IT can activate threat detection and remediation capabilities without requiring any user action.

Detailed threat forensics

Gain immediate and ongoing visibility into malicious threats across all mobile devices and receive detailed analyses of risky apps.

Head to the cloud
Securely with Ivanti

As your company embraces more cloud resources and the Everywhere Workplace, make sure you have the right security to protect those resources from unauthorized or malicious access. Passwords are no longer up to the task, from the breach risk they represent to their widespread unpopularity with IT and end users alike.

Your existing Ivanti UEM is the key to achieving zero trust security. By adding standards-based security with Access, you can ensure that access is only granted after users, endpoints, apps and cloud services are verified – without a single password. On top of that, MTD blocks any type of threat, around the clock.

Maximum security. Minimal hoops.

The cloud is where your business is headed. Ivanti can take your security where it needs to be, too.

- End users can access their cloud business tools on any device they choose with a seamless access experience.
- IT can interact with one scalable platform and one screen into your mobile and cloud security.

With the UEM you already have, you're already on your way to achieving zero trust security. Head to the cloud with elevated security and productivity by adding Access and MTD today.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Gartner Says Four Trends Are Shaping the Future of Public Cloud", 2 August 2021. https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

2. Verizon, "2021 Data Breach Investigations Report", 13 May 2021. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/