ivanti

The Perimeter's Gone. Can Your Security Handle It?

Protect the Everywhere Workplace with a zero trust framework

Security in a perimeterless world

It's safe to say that mobile dominates the enterprise – especially in the Everywhere Workplace. In addition to changing the way we work, mobile and cloud technologies have dissolved the enterprise security perimeter. This has introduced new threat vectors that traditional security frameworks are simply not designed to defend against.

Organizations need to shift their security strategy to secure the new ways work gets done. That takes a "never trust, always verify" approach that starts with devices and goes further than other zero trust security methods.

In this eBook, we'll explore the industry-leading zero trust framework, and how a strategy using this approach can help the modern enterprise stay agile and secure in the Everywhere Workplace.

The Challenge

With freedom comes risk

No one doubts the impact mobile devices have on our lives – or the enterprise. The latest statistics speak for themselves.

Productivity and business innovation have benefited immensely as data flows freely across a wide information fabric of devices, apps, networks and cloud services. This freedom of anytime, anywhere access has enabled the Everywhere Workplace – and effectively dissolved the traditional security perimeter. This is exciting, but it has also created a massive attack surface and a host of new risks and threats that traditional security approaches weren't designed to address.

Data's getting around

As desktops are replaced by mobile endpoints, and data centers move workloads to the cloud, data no longer stays inside a tidy enterprise perimeter. It's on devices and clouds you own and those you don't, crossing networks other than yours – many with less than robust security.

Hackers follow the opportunity

Attacks that we've seen on the desktop are quickly making their way toward mobile because of simple economics. Hackers follow the data. It's more efficient for hackers to try new doors instead of breaking through old ones with layers of PC protection. Today's landscape: so many devices, so little security.

Mobile vulnerabilities

Hackers can easily exploit mobile vulnerabilities and user behavior to gain significant control over your entire company. As mobile attacks become more sophisticated, organizations need a modern security approach to keep their data secure.

It's clear that traditional security models built for the PC and data-center world don't translate to the Everywhere Workplace. It's time to take a hard look at your security strategy.

80x

We check our phones 80x per day[I]

77%

of enterprises use cloud services[II]

52%

of all web traffic is from phones[III]

1,000

An average enterprise uses ~1,000 apps[IV]

The zero trust approach

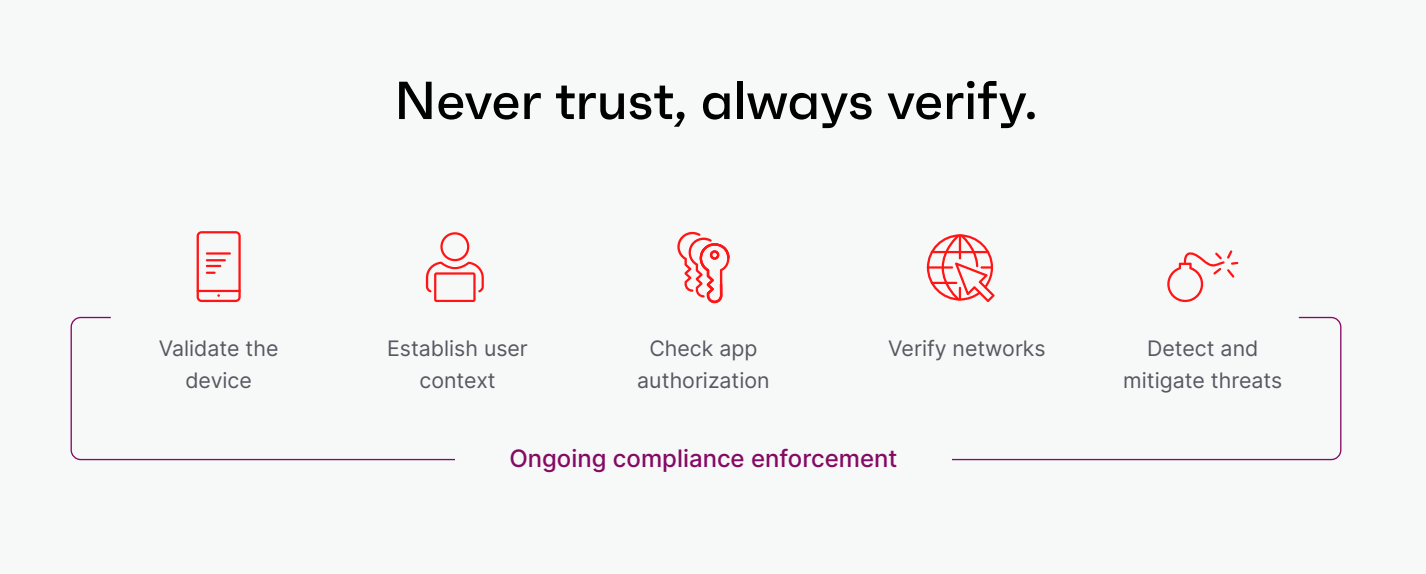
Never trust, always verify

Introduced by Forrester in 2014, the zero trust approach recommends that while building a security strategy, you should start from the assumption that your network is already compromised. Secure access should be determined by a “never trust, always verify” approach that requires you to verify the device, user, apps, networks and presence of threats before granting access – with constant enforcement.

There are multiple approaches to zero trust, and the main ones focus on identity, gateway and the device. Only an approach built for the Everywhere Workplace addresses the security challenges of the perimeterless modern enterprise while allowing the agility and anytime access.

Raising the security bar

A modern, zero trust framework goes beyond traditional identity management and gateway point solutions by raising the security bar. It demands more answers from a comprehensive set of attributes before granting access. It validates the device, establishes user context, checks app authorization, verifies the network and detects and remediates threats – all before granting secure access to any device or user. And this happens instantaneously.



The Ivanti solution

Zero trust security for the Everywhere Workplace

Ivanti has always believed that mobile is the center of the enterprise. That's why we created a security platform that starts from the device and goes beyond other zero trust approaches.

Your device is your ID

By making your mobile device your secure ID, we eliminate passwords and make access to business information more secure and much easier. This allows organizations to give mobile users the freedom and flexibility they need to be productive whenever and wherever they work. It also makes it simple to protect data wherever it lives.

How we do it

Ivanti is redefining enterprise security with the first zero trust platform built for mobile on our award-winning, unified endpoint management (UEM) foundation to secure access in the Everywhere Workplace.

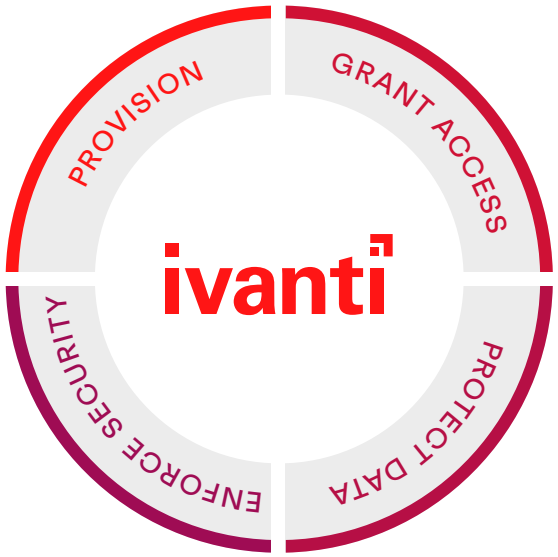
Our approach significantly reduces risk by taking more signals into account before granting access. It validates the device, establishes user context, checks app authorization, verifies the network and detects and mitigates threats – all before green-lighting access to a device or user. This gives you complete control over your business data as it flows across devices, apps, networks and cloud services.

The diagram below outlines the four-step process to implement a zero trust approach for mobile – one that's both embraced by users for its seamless experience, and by IT for its easy implementation and dramatic reduction in help ticket requests.

Zero trust. Everywhere.

1. Provision
any device for a user with the appropriate apps, profiles and policies. UEM (Unified Endpoint Management) is the foundation – the first step in achieving zero trust security for mobile.

2. Grant access
based on full context: verify the user, posture of the device, app authorization, network type, presence of threats and a variety of other signals. This adaptive access control check is the basis of the zero trust model.



4. Enforce security policies
with ongoing monitoring; any change in signals will trigger adaptive policies to mitigate threats, quarantine devices and maintain compliance.

3. Protect data
at rest and in motion with state-of-the-art encryption and threat monitoring to detect device, network and app-level attacks.

The Ivanti solution

What powers trust security for the Everywhere Workplace?

Ivanti UEM

Our award-winning unified endpoint management (UEM) product provides the visibility and IT controls needed to secure, manage and monitor any corporate or employee-owned mobile device or desktop that accesses business-critical data. With Ivanti, secure a vast range of employee devices coming into the enterprise and manage their entire lifecycle.

Mobile Threat Defense

We provide zero trust security using built-in threat detection and remediation across devices, apps, and networks – without the need for internet connectivity or concerns about user adoption. Sophisticated, location-agnostic security is essential for success in the Everywhere Workplace.

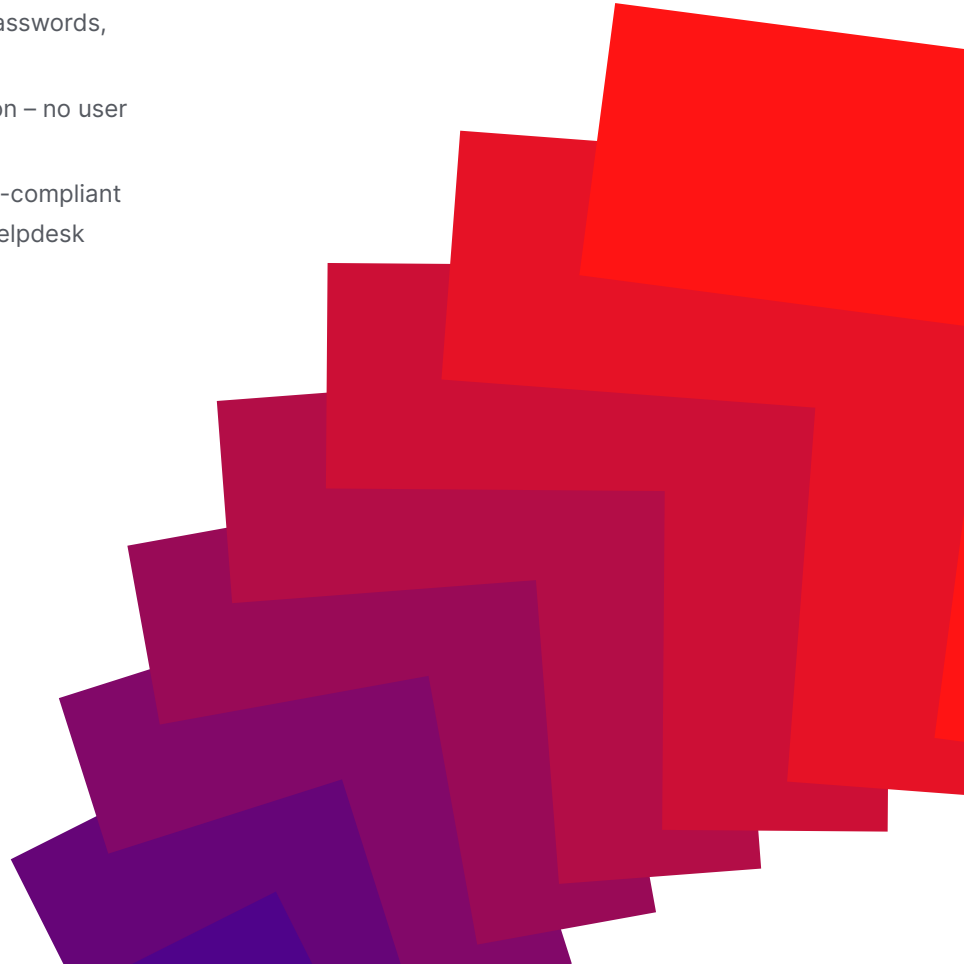
Access

Seamless, conditional access is achieved through passwordless single sign-on (SSO) and multi-factor authentication (MFA). This supports a zero trust framework by ensuring only authorized resources can access and share corporate data from any device, OS or location to any service.

Seamless security for the Everywhere Workplace

Not only are employees unaware of all the checks going on in the background, but we've created an enhanced experience that makes life easier for both IT and end users:

- Easy device on-boarding and automatic configuration – no lengthy employee set-up guides.
- Zero password for instant access – no more fumbling, retyping or remembering passwords, ever.
- Continuous on-device threat detection – no user action required.
- Intuitive remediation workflows – non-compliant devices can be easily fixed without helpdesk involvement.



ivanti

The takeaways

The security strategy for the everywhere workplace

Mobile and cloud have both transformed business and complicated security by creating a perimeterless environment that traditional security solutions weren't designed to address. Many organizations are adopting a zero trust security model, which assumes the threat is already inside the network. Gateway- and identity-centric approaches are two variations on zero trust, but both fall short in several key areas. As more organizations shift their workloads to the cloud, it's clear that today's security strategies need to start with mobile at the center.

Ivanti has redefined enterprise security with the first zero trust platform built for the Everywhere Workplace that turns the mobile device into a user's secure ID for enterprise access. Built on an award-winning UEM foundation, this approach provides the enterprise with a modern security strategy that allows it to:

- Drive business innovation by confidently adopting mobile and cloud technologies.
- Provide users with the best experience to drive productivity.
- Provide the right level of security from all points of access.

If you'd like to learn how Ivanti can help your organization thrive in the Everywhere Workplace with a zero trust security strategy, let's talk.

ivanti

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

I. "Americans check their phones 80 times a day: study." Newyorkpost. com, November 8, 2017, https://nypost. com/2017/11/08/americans- check-their-phones-80-times-a-day-study/
II. "State of Enterprise Cloud Computing, 2018." Forbes. com, August 30, 2018, https://www.forbes.com/sites/louiscolumbus/2018/08/30/ state-of-enterprise-cloud-computing-2018/#446d48e0265e
III. "Percentage of all global web pages served to mobile phones from 2009 to 2018." Statista, 2019, https://www.statista.com/ statistics/241462/global-mobile-phone-website-traffic-share/
IV. "Enterprises on average use up to 1000 cloud apps but their CIOs think it's just 30 or 40 apps." ETCIO.com, April 28, 2017, https://cio. economictimes.indiatimes.com/news/strategy-and-management/ enterprises-on-average-use-up-to-1000-cloud-apps-but-their-cios-think-its-just-30-or-40-apps/58410934