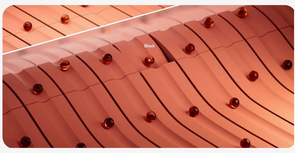
infinipoint

Integrating Device and User Authentication to Achieve Zero Trust Workforce Access

By Ran Lempert.
This article was originally published on Infinipoint's blog.
21/05/2024



Authenticating Users Alone is Not Enough

Threat actors are increasingly focusing their attention on identity-based attack vectors. And there's one big reason for this. It works.

This can seem counterintuitive for many security leaders, particularly those who have invested heavily in stronger authentication practices in recent years, yet still, account takeover and device takeover continue to be frequently recurring themes in successful breaches.

The reality is that most legacy authentication is User-based, and identity verification based on user credentials alone is simply not enough. Users alone don't access your systems. Access requests are always a combination of users logging in through their devices.

Attackers have found ways to circumvent additional factors as SMS, Push notifications, number matching and TOTP's, through phishing, MFA prompt spamming and social engineering attacks.

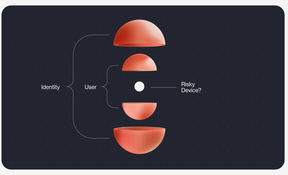
Account Takeover through MFA Attack - Illustration

Through these methods attackers have breached leading companies with advanced tech stacks by targeting employees, third party suppliers and their devices, and have gained unauthorized access to resources with their own devices.

A Wider View of Identity is required

The only way to change this is to think bigger about identity.

Every access request is an assertion of a digital identity. Authenticating the full identity of every access request means you need to verify the users, and the devices they are requesting access from, and make sure the devices are known, approved and safe to login.



The Zero Trust Workforce Access Paradigm Shift

That's where Zero Trust Workforce Access comes in.

Zero Trust Workforce Access is based on the principle that no entity, whether inside or outside the network, should be trusted by default. Instead, trust must be continuously earned through rigorous verification processes.

The core idea of Zero Trust is simple yet powerful: "Never trust, always verify." In the context of identity, this boils down to two simple but important ideas:

1. Don't assume the user is who they say they are.
2. Don't assume that the device of origin is safe and can be trusted.

Zero Trust Workforce Access combines next-generation user authentication with device-based access control to

- Block account takeovers.
- Minimize authentication friction for users.
- Reduce help desk calls for IT.

How did we get here?
The Evolution of Authentication Methods

The industry's move to Zero Trust Workforce Access is informed by earlier generations of identity security technology and seeks to address the limitations that have allowed identity threats to thrive even as enterprises have made substantial investments in identity security technologies over the last decade.

First-Generation: User Credential Focus

User-based Authentication

User Authentication Via Passwords + 2FA

The first wave of authentication methods focused primarily on user credentials, often relying on passwords and, eventually, broad use of two-factor authentication.

These methods are inherently flawed due to their susceptibility to social engineering, phishing attacks, and brute force tactics. Additionally, they operate under the assumption that once authentication occurs, the user can be trusted implicitly, which is a risky and outdated security perspective in today's dynamic threat environment.

Second-Generation: Loosely Patched Integrations of User+Device Authentication

Loosely patched Integrations

MFA or Passwordless user authentication

Integrated with MDM's, struggling with certificates

Over time, vendors and enterprises began introducing at least some device-focused workforce access checks.These included certificates and mobile device management (MDM) platforms. While these measures added a layer of security by authenticating some of the devices used to access resources, they still were flawed in numerous ways.

Certificates, though useful, can be stolen or spoofed. Managing a sprawling collection of device certificates is also a logistical nightmare, particularly for larger organizations with a diverse device footprint.

MDM solutions have limitations as well. They are not suitable for many use cases, most notably workforce personal devices and 3rd party contractors. Additionally, both methods only provide a snapshot of device security at the time of access, lacking continuous verification.

Another major drawback and barrier for adoption of this approach is the user experience. If an issue is discovered with the device, the user is likely blocked and forced to seek IT assistance due to the lack of self-service recovery options. This disrupts the workflow and burdens IT teams, failing to meet modern workforce demands for a seamless login process. Ultimately, this approach creates a security posture that is cumbersome, inflexible, and ultimately insufficient for today's dynamic work environments.

Next-Generation: Zero Trust Workforce Access

Zero Trust Access

Complete User & Device authentication (pass/MFA)

Device posture Verification & Remediation

Zero Trust Workforce Access platforms overcome the limitations of first and second-generation authentication models, by augmenting the way workforce access is done to meet challenges of the modern threat landscape with the following capabilities, which must work in concert:

1. Next-Generation User Authentication
Traditional passwords are both insecure and inconvenient, representing a significant vulnerability in cybersecurity. Zero Trust Workforce Access approaches typically incorporate passwordless authentication methods, which enhance both security and user experience. Implementations that align with the FIDO2 standards, for example, can use strong, cryptographic login credentials that are unique across every website and never leave the user's device, drastically reducing the risk of phishing. Real-world implementations like passkeys are already allowing users to authenticate seamlessly across devices and platforms without ever entering a password.

2. Device-Based Authentication
Under a Zero Trust Workforce Access model, device authentication and security checks are just as important as user authentication. Every device is authenticated before access to corporate resources is allowed. And more advanced implementations take this a step further by verifying that the device is not compromised, has up-to-date security patches, and meets the organization's compliance standards.

3. Ensuring Flowing Access and User Buy-In
User experience must be a central design principle in order for a Zero Trust Workforce Access strategy and implementation to gain traction. Take advantage of innovations like passwordless user authentication and make device authentication as frictionless as possible, momentum will build and both business productivity and security will improve in parallel.

Ultimately, Zero Trust Workforce Access marks a significant evolution in enterprise security, integrating device and user authentication to mitigate today's sophisticated identity threats, by providing:

- **Active defense against account takeover:** Pinning users to specific devices by policy makes it more difficult for threat actors to hijack user accounts.
- **Access limited to pre-enrolled devices:** Device enrollment constrains the attack surface to a predefined set of known devices.
- **Granular device access policies:** Conditional access further reduces device risk by enabling precise control over the number, type, and classification (e.g., corporate, personal, etc.) of devices that can assess specific resources.
- **Broad applicability across use cases:** Zero Trust Workforce Access has the flexibility to accommodate a wide range of use cases, including corporate managed and personally-owned devices, or Third-party contractor devices, and cover all the operating systems of your workforce devices.
- **Frictionless user experience:** Passwordless authentication achieves a superior experience even as more comprehensive user and device checks are performed.
- **Reduced IT burden:** Fewer roadblocks for users also means lower help desk ticket volume for the IT team.

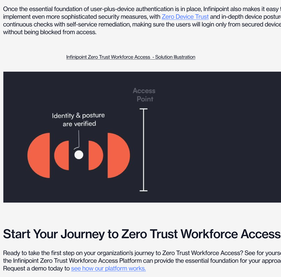
Infinipoint is Leading the Evolution to Zero Trust Workforce Access

The Infinipoint Zero Trust Workforce Access Platform makes it easy for security teams to bring Zero Trust Workforce Access from concept to operational reality. It brings together passwordless user phishing resistant authentication and device-based access control.

Infinipoint integrates seamlessly with existing cloud and on-premises infrastructure, along with any existing identity and access management technologies in use.

Once the essential foundation of user-plus-device authentication is in place, Infinipoint also makes it easy to implement even more sophisticated security measures, with Zero Device Trust and in-depth device posture continuous checks with self-service remediation, making sure the users will login only from secured devices without being blocked from access.

Infinipoint Zero Trust Workforce Access - Solution Illustration



Start Your Journey to Zero Trust Workforce Access

Ready to take the first step on your organization's journey to Zero Trust Workforce Access? See for yourself how the Infinipoint Zero Trust Workforce Access Platform can provide the essential foundation for your approach. Request a demo today to see how our platform works.