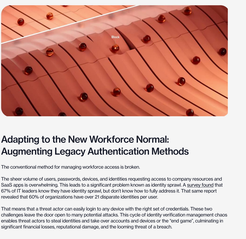
infinipoint

Rethinking Workforce Access: Augmenting Authentication with Zero Trust

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



Adapting to the New Workforce Normal: Augmenting Legacy Authentication Methods

The conventional method for managing workforce access is broken.

The sheer volume of users, passwords, devices, and identities requesting access to company resources and SaaS apps is overwhelming. This leads to a significant problem known as identity sprawl. A survey found that 67% of IT leaders know they have identity sprawl, but don't know how to fully address it. That same report revealed that 60% of organizations have over 21 disparate identities per user.

That means that a threat actor can exploit just one such gap in the right set of circumstances. These two challenges leave the door open to many potential attacks. This cycle of identity verification management chaos enables threat actors to access sensitive data from unauthorized accounts and devices or the "end game", culminating in significant financial losses, reputational damage, and the looming threat of a breach.

To combat security threats, organizations have started developing zero trust strategies and methods of implementing them into their main pillars :

- Identity
- Device
- Network
- Data
- Applications

Adopting the zero trust framework entails trusting no one and verifying everyone who requests access to any of these five pillars.

Where Legacy Authentication Methods Fall Short

There's just one problem.

Adopting zero trust is easier said than done.

IAM tools were not built to authenticate and verify devices, not to mention the fact that MDMs don't work on-access.

These approaches leave IT teams with two bad options: Blocking users from access when posture is misaligned or assuming devices are safe and compliant as they access their data and resources.

This is why organizations have been susceptible to a rise of threats and breaches by unknown or unpatched devices.

The time for a new approach is long overdue.

However account takeovers still remain a growing concern.

Access Sprawl: Account Takeovers on the Rise

Account takeovers are a form of identity theft and fraud where cybercriminals exploit stolen user credentials, stolen session cookies and employee accounts to gain unauthorized access to data and resources.

Research revealed that ATO attacks have soared by 354% YoY in 2023 with Fintech being the most targeted industry during that time frame (800% YoY increase).

ATO attacks have grown even more sophisticated with the rise of AI-generated tools and prompts, enabling cybercriminals to generate more advanced phishing messages and create highly personalized social engineering attacks.

Here are 3 common ATO attack methods, not taking into consideration the multitude of combinations a threat actor might use to gain unauthorized access:

Credential Theft & prompt attacks

Credential theft, the act of stealing login credentials (usernames and passwords), allows unauthorized access to sensitive data, accounts, and systems.

Attackers often combine this with social engineering tactics like phishing emails or fake login pages.

These tactics aim to bypass multi-factor authentication (MFA) security by tricking users into approving rapidly sent MFA approval prompts (prompt bombing). By approving these prompts, users unknowingly grant malicious attackers access to their accounts, applications, and other company resources.

Phishing and Man-in-the-Middle (MITM) Attacks

Phishing and Man-in-the-Middle (MITM) attacks are common threats. Phishing tricks individuals into clicking malicious links or attachments to steal sensitive information like PII (Personally Identifiable Information) and login credentials. A shocking 94% of organizations fell victim to phishing attacks in 2023!

In a MITM attack, the attacker acts like a hidden eavesdropper in your communication with others. The attacker can also pose as your bank, an login details, by intercepting the communication.

They might achieve this by setting up a fake website or even a reverse tunnel disguised under a familiar domain. This tunnel intercepts the communication between you and the real website, allowing the attacker to steal your session cookie (along with other data) as everything is exposed to them.

Vulnerable Devices

Keeping every device safe and compliant is virtually impossible. Corporate-managed devices security posture is extremely user-dependent and users can change device configuration, have security agents such as disabling firewalls, or fail to update their OS, browser, or 3rd party SaaS apps with critical zero-day updates.

Not to mention BYOD (Bring Your Own Device) and third-party contractors' devices that are even harder to control and protect from malicious takeovers by attackers lurking for these opportunities to gain unauthorized access to your sensitive resources.

6 Major Breaches and How They Could Have Been Prevented

But how can you protect what you don't know?

Traditional security access verification methods just won't cut it anymore.

Access and authentication methods must verify the identity and posture of endpoints requesting access, completely separate from the users themselves.

As you'll discover in the next section, it only takes one compromised account to trigger a massive breach.

Uber

How it happened:

On August 15th, 2022, a hacker obtained stolen credentials belonging to an Uber employee from the dark web. The attacker employed a tactic known as MFA fatigue or MFA bombing, flooding the user with a barrage of push requests asking the employee to repeatedly sign into their account.

Overwhelmed, the employee eventually approved the request, allowing the attacker to access Uber's intranet, VPN, and internal network.[1] cnbcpulse.com.

Once inside, the attacker discovered PowerShell scripts that contained the hardcoded credentials of an admin user in Thycotic, the company's Privileged Access Management (PAM) solution. This compromised Uber's entire cloud ecosystem, as well as the personal information of 77,000 Uber employees.

Although the identity of the attacker was never disclosed, Uber attributed the breach to the international hacking group Lapsus$.

slack

How it happened:

On December 29, 2022, Slack disclosed that threat actors had gained unauthorized access to private GitHub code repositories and that a minimal number of Slack employee tokens had been stolen.

Slack's security team believed no customer data had been impacted directly in the breach. Slack also rotated all relevant credentials as a further precaution.

MGM RESORTS

How it happened:

MGM Resorts was breached in September 2023. Scattered Spider group was behind the attack. The threat actors gained a foothold into the hotel and casino giant's internal network through a misconfigured IdP in the Okta tenant and Azure cloud environment. Once inside, the cybercriminals further escalated their privilege access and deployed credential harvesting techniques.

The ransomware encrypted hundreds of ESXi servers and disrupted VMs, which created a cascading domino effect for EDR hosts. This prevented hotel room keys from functioning and MGM's systems from processing payment and checkout transactions. The breach cost the hotel and casino giant an estimated $10Mil in damages.

okta

How it happened:

In April 2024, Okta announced yet another breach with a huge uptick in credential stuffing attacks targeting its IAM solutions, with a score of customer accounts compromised.

The threat actors relied on brute force and password spraying attacks to exfiltrate the data.

Okta noted that the attacks were more successful for those using the Okta Classic Engine with Threatinsight set to Audit-only mode instead of Log and Enforce mode.

LastPass

How it happened: The LastPass breach occurred in November 2022. A threat actor used valid credentials stolen from a senior DevOps engineer to access a shared cloud storage environment.

The attackers captured the employee's master password, easily bypassing MFA to gain access to the engineer's LastPass corporate vault which included encrypted and unencrypted customer data.

jumpcloud.

How it happened: JumpCloud experienced a breach in June 2022. The attack was traced back to a spear phishing campaign on June 22 led by a nation-state-sponsored threat actor. The attacker gained unauthorized access to a small part of JumpCloud's IT.

JumpCloud discovered suspicious activity two weeks later on July 5 in the commands framework for a small group of customers, indicating that customer data had been compromised. JumpCloud then force-rotated all admin API keys and notified affected customers immediately.

How These Breaches Could Have Been Prevented

These breaches could have all been prevented with several key security capabilities:

1. **Phishing Resistant Authentication:** Stopping phishing attacks, leaked credentials, and MFA bombing by combining user and device authentication.
2. **Device-Based Access Control:** With Complete Authentication, you can grant access only to authenticated users from their explicitly approved devices, leveraging cutting edge passwordless coupled with device authentication.
3. **Zero Device Trust:** This enables IT teams to enforce granular access controls and compliance at every login request and continuously through every session, so only safe and compliant devices gain access.

Move Beyond Traditional Authentication Methods and Augment Your IdPs with Zero Device Trust

There is a better way to prevent data breaches and access sprawl.

As shown from the small sample of breaches covered herein, it only takes one unpatched device or leaked credential for an attacker to gain access to your company's resources with their own device and cause a major breach.

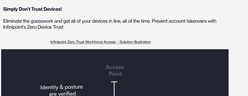
The new era of device and access security is here. Bring device and passwordless user authentication together with Zero Device Trust. Give yourself peace of mind knowing that all access is verified, across all devices and users.

How?

Simply Don't Trust Devices!

Eliminate the guesswork and get all of your devices in line, all of the time. Prevent account takeovers with Infinipoint's Zero Device Trust.

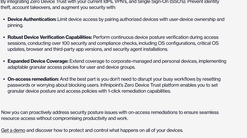
Infinipoint Zero Trust Workforce Access - Solution Illustration



Access Done Right with Device Zero Trust

By integrating Zero Device Trust with your current IdPs, VPNs, and Single Sign-On (SSOs). Prevent identity theft, account takeovers, and augment you security with:

- **Device Authentication:** Limit device access by pairing authorized devices with user-device ownership and pairing.
- **Robust Device Verification Capabilities:** Perform continuous device posture verification during access sessions, conducting over 100 security and compliance checks, including OS configurations, critical OS updates, browser and third-party app versions, and security agent installations.
- **Expanded Device Coverage:** Extend coverage to corporate-managed and personal devices, implementing adaptable granular access policies for user and device groups.
- **On-access remediation:** And the best part is you don't need to disrupt your busy workflows by resetting passwords or worrying about blocking users. Infinipoint's Zero Device Trust platform enables you to set granular device posture and access policies with 1-click remediation capabilities.

Now you can proactively address security posture issues with on-access remediations to ensure seamless resource access without compromising productivity and work.

Get a demo and discover how to protect and control what happens on all of your devices.