Whitepaper

jumpcloud

Zero Trust Security

Contents

A Transformative Way to Secure Your Hybrid Workplace

Introduction

Zero Trust security is an adaptable security architecture that has emerged to manage the risk of an increasingly fragmented hybrid workplace. The hybrid workplace can be defined both by where we work and by how we work — cloud services, mobile devices, and remote work are three of its biggest trends.

Case in point, Internet traffic spiked in 2020, as organizations adopted new remote work policies, 50 percent of Internet traffic comes from mobile devices, and 83 percent of Internet traffic comes from the API calls that enable cloud services. With many employees refusing to return to the office and many companies planning to reduce their office space, the hybrid workplace has become the new normal.

Whereas the legacy security model was focused on protecting the user, their device, and the services they use within a network perimeter; Zero Trust security assumes that the user, their device, and the services they use could be the entry point for an attack, so it shifts security from the perimeter and adds a critical layer of identity, authorization and access management.

Zero Trust secures more than just the networks, devices, applications and data we use — it secures how we work, wherever that is. And with the growing usage of cloud services, mobile devices and hybrid workplaces, Zero Trust Security represents a transformative way to secure our businesses, and our overall economic recovery.

This whitepaper examines the development of Zero Trust Security, why it's so important to understand and adopt, how it's being used, and how it can make a fundamental difference in your business. And it all starts with the rise of the hybrid workplace.

2020 Hindsight — The Rise of the Hybrid Workplace

The consumerization of corporate IT is a trend that goes back decades. As technology became more pervasive, and more and more employees began using their own personal devices and networks for work, IT leaders have been challenged to maintain governance and control over the security and reliability of their systems.

Even before the pandemic, a new generation of digital-native employees came to expect their employers to be able to handle this trend, expecting seamless onboarding, business app stores and do-it-yourself helpdesk calls. In short, the employee experience, not just the customer experience, became incredibly important.

And then the pandemic hit, accelerating many of these trends and introducing new dynamics that nobody could have predicted. During lock-down, with employees quarantined at home, we saw a sea change in how our technology infrastructure worked, or at times, did not work.

As we emerge from the pandemic, many employees are opting not to return to the office because they have grown used to working from home and many companies are reducing their office space to minimize their operating costs. In short, thanks to the events of 2020 and the first half of 2021, the hybrid workplace has quickly become the default model for small and medium-sized enterprises (SMEs) everywhere.

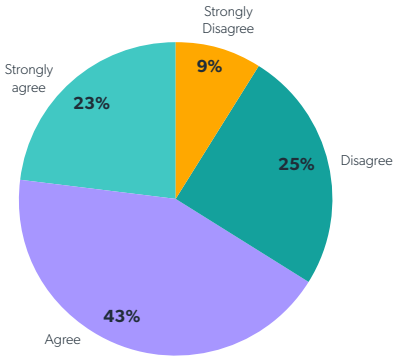
A recent survey of small and medium enterprise (SME) IT leaders shows exactly how common the new hybrid workplace is, and how important it is to find new ways to secure it.

SME IT Trends Survey Report Highlights

IT Challenges

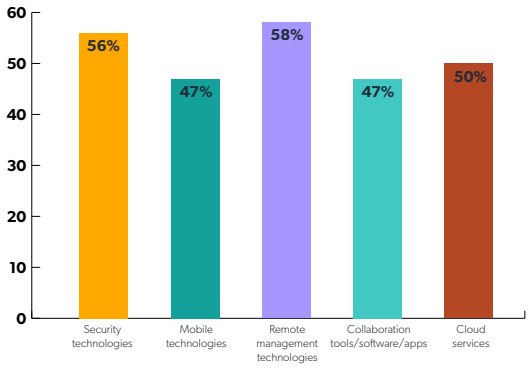
Source: SME IT Trends Survey

Overwhelmed?



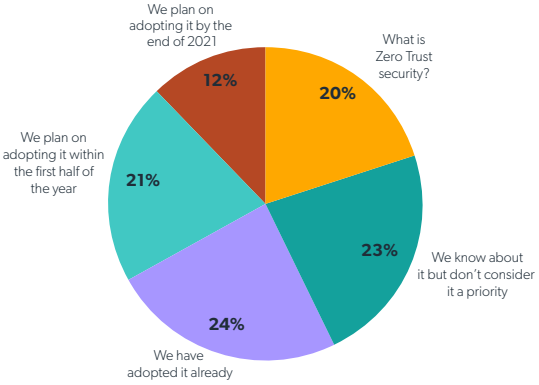
Source: SME IT Trends Survey

IT Spending



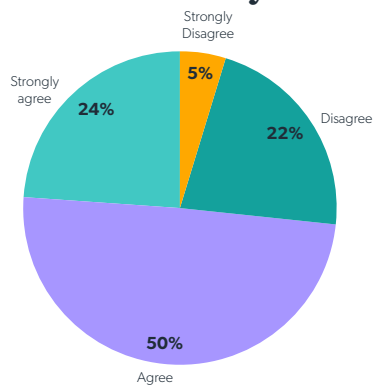
Source: SME IT Trends Survey

Zero Trust Approach



Source: SME IT Trends Survey

Remote Work Security



Source: SME IT Trends Survey

IT Priorities

Item	Overall Rank
Adding layered security so work-from-anywhere is truly secure	1
Making remote work easier for end users	2
Making device management easier	3
Easier management of user devices	4
Making remote work easier for admins	5
Implementing SSO of unifying identity management	6
Gaining analytical insight into user access	7
MFA	8

Source: SME IT Trends Survey

Download the full analysis from the *IT Trends Report: Remote Work Drives Priorities in 2021* here.

Boundary Issues: The Shortcomings of Perimeter Security

If 2020 catalyzed the shift to the hybrid workplace, organizations are now looking for solutions to galvanize it. It was difficult for many organizations to make the switch in 2020 because they were still relying on legacy solutions. Two of the most common legacy solutions are the virtual private network (VPN) and the virtual desktop infrastructure (VDI), both of which suffer from a poor user experience and can be susceptible to performance issues when overused or misconfigured.

VPNs are used to establish a secure connection to the Internet, so that employees can safely access their corporate network. If a corporate network is like a castle protected by its walls, then a VPN is like a drawbridge that can be raised and lowered to grant access.

However, as cloud services have propagated resources beyond the corporate network, the VPN has become a hurdle, creating an extra hop between the user and the service. It is like flying from Boston to New York, but with a layover in Chicago.

VDI follows a similar model to VPN, enabling its users to connect to a centralized server that is hosting a virtual machine. But once again, requiring remote users to connect into the corporate network, only for their data to be sent to a cloud service elsewhere, makes for a slow experience.

The problem with these legacy solutions is that they are predicated on a perimeter security model — just like our castle example. However, with the rise of the hybrid workplace, corporate resources are in the cloud, employees are connecting from anywhere, and the walls have come tumbling down. And it's nearly impossible to secure a post-perimeter workplace with a security approach predicated upon perimeters, as the world quickly learned. Unfortunately, many malicious actors learned this lesson a little faster than the businesses they attacked.

One of the biggest cyberattacks of 2020, the SolarWinds breach, exploited the APIs of cloud services to enable unauthorized access. One of the biggest cyberattacks of 2021, the ransomware shutdown of Colonial Pipeline, used a compromised password to gain unauthorized access.

Organizations should still be concerned with protecting their confidential data, but they need to rethink this protection in terms of preventing unauthorized access.

That's why legacy solutions are a stop-gap measure to secure the transition to the hybrid workplace. SMEs can be especially sensitive to these growing pains, since they may not have a full-time CISO or a dedicated team of security experts at their disposal, or they might lack the budget to invest into security platforms beyond their IT management solutions.

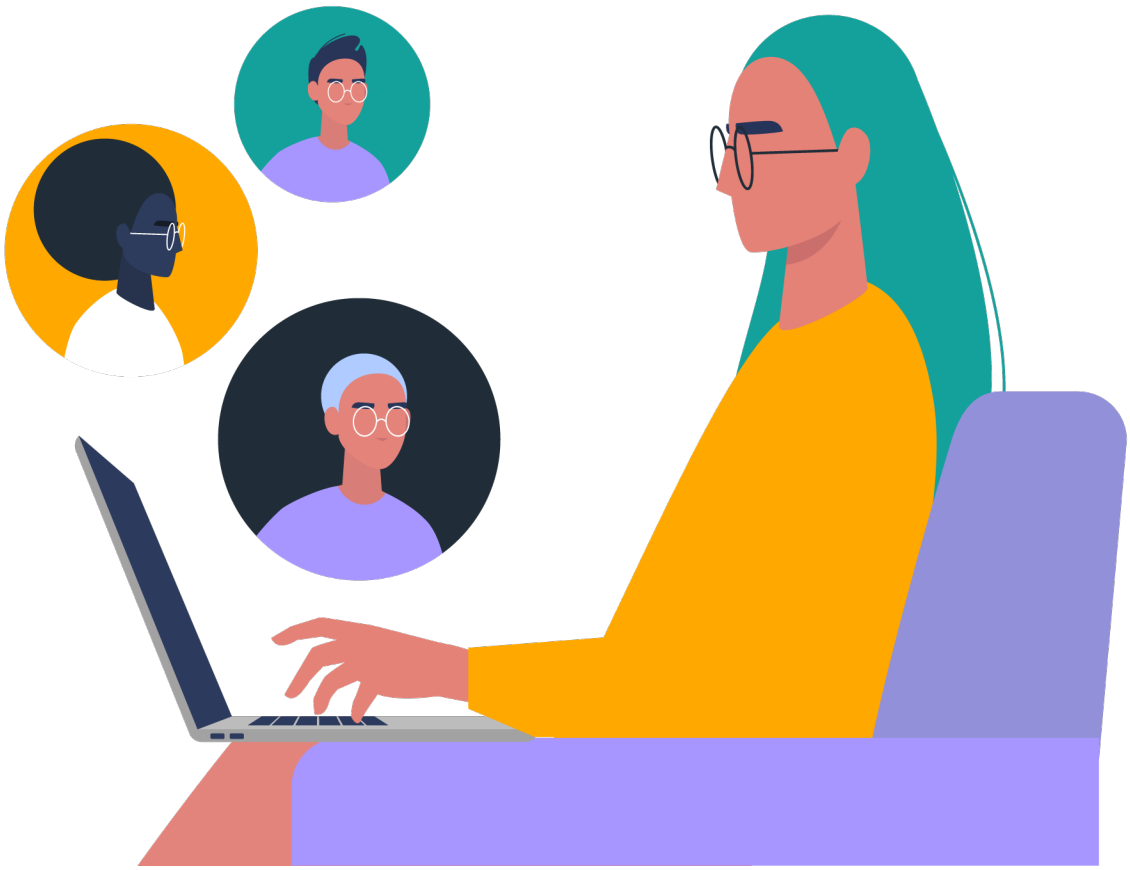
Fortunately, Zero Trust Security is a proven and well-established approach to security whose time has come — and not a moment too soon.

Absolute Zero – The Foundations of a Zero Trust Architecture

The origins of Zero Trust Security can be traced back more than a decade. In 2010, a Forrester security analyst at the time, John Kindervag, popularized the use of the term and set forth many concepts that still serve as its foundation today. Around the same time, Google began developing its own Zero Trust Security architecture, BeyondCorp. In 2018, the National Institute of Standards and Technology (NIST) issued a special publication (SP) 800-207, *Zero Trust Architecture*.

With so many giants involved in Zero Trust, and hundreds of pages of technical papers written about it, it is easy to become overwhelmed. However, the essence of Zero Trust Security is highly intuitive: when an organization trusts the validity of its users, its devices, and its network at face value, that trust creates a security risk; it is far too easy for criminal hackers to compromise, mimic, and otherwise falsify their identity and behaviors to gain illicit access by taking advantage of that inherent trust.

To put it succinctly: trust nothing, verify everything.



More precisely, Zero Trust Security is focused on establishing trust whenever access is requested, which can be simplified into a straightforward framework:

- **Trusted Identity** — Confirm the user is who they say they are
- **Trusted Devices** — Ensure the device is healthy, secure and managed
- **Trusted Network** — Secure the network path
- **Authorization Policies** — Enforce correct authorization to access IT resources

Authorization policies, which are also referred to as **conditional access,** are essential to managing Zero Trust. A user must demonstrate that their identity, device, and connection are trustworthy before they can gain access to enterprise resources. Behavioral anomalies, such as connecting from a new device or a new location, may require a user to re-establish trust before access is granted.

Closely related to conditional access is the **Principle of Least Privilege,** which states that a user should be granted the minimum access required to complete their job. For example, a sales team member should not have access to HR systems.

Managing conditional access and least privilege can be complex in cloud and hybrid workplace environments. According to ESG Research, *Trends in Identity and Access Management: Cloud-driven Identities,* the average organization says 30% of their cloud identities are overly permissive.

There are a variety of solutions to help manage the Zero Trust Security framework, but as the hybrid workplace has become increasingly fragmented, it has become increasingly challenging to manage.

Divided by Zero: Limitations of Current Approaches to Zero Trust Security

As easy as it is to outline a framework for Zero Trust Security, complications can sometimes arise when you deploy it across a traditional technology stack. Using multiple services from multiple vendors can also increase complexity and costs. Some of these more traditional Zero Trust solutions include:

- **Identity and Access Management (IAM)** — Solutions that establish and manage the identity of users and their access privileges
- **Identity Governance and Administration (IGA)** — Solutions that centralize the management and enforcement of user-based identity and access policies (i.e. least privilege)
- **Multi-Factor Authentication (MFA)** — Solutions that require a user to provide multiple forms of identification (more than just a password)

- **Device Management and Mobile Device Management (MDM)** — Solutions that enable IT administrators to manage and enforce policies on laptops, smart phones, and tablets
- **Network Authentication** — Solutions that verify the user's identity before granting access
- **Access Controls** — Solutions that enable and enforce group policy and granular policy for entitlements and access levels (i.e. conditional access and least privilege)

Active Directory (AD) has served as the de facto identity management and authentication solution for Windows environments for many years. But with the shift to cloud and hybrid workplaces, each new service requires managing new identity bridges, which add additional costs and complexity. The rise of remote workers has further complicated these management issues.

AD was designed to create internal networks — called domains — to secure on-premise resources and data. However, cloud and hybrid workplaces don't follow this model. And of course, AD does not even support Mac, mobile and Linux environments easily.

That's why today's IT leaders need new and more efficient ways to expand the domain to users, devices, and resources located beyond the perimeter. An emerging-cloud based architecture integrates with AD to securely extend AD identities to virtually all resources beyond the traditional domain, while still centrally authenticating users and systems.

And the most obvious and clearly proven approach to reducing the cost and complexity of managing Zero Trust Security is to unify access to all resources into a single secure platform.

One Directory to Rule Them All

One reason that Zero Trust Security requires so many solutions is because cloud and hybrid workplaces are so fragmented with services and devices. However, a cloud-based directory addresses these issues of fragmentation because its infrastructure is available anywhere and its open standards integrate with any service or device.

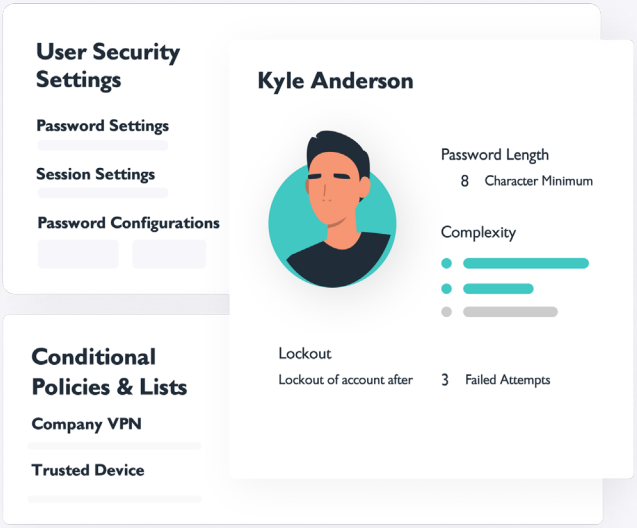
Organizations can manage the full breadth of identity, devices, and network access through a cloud-based directory, so it's a simple step to enforce the conditional access of Zero Trust security. The most important elements to look for in any Zero Trust solution are:

- **The Right Authentication** — A cloud based-directory can streamline IAM and MFA
- **The Right Device** — A cloud-based directory can link the identity of a user to the identity of a device through MFA
- **The Right Access and Privileges** — A cloud-based directory can manage and enforce access rights (i.e. conditional access and least privilege)
- **The Right Location** — A cloud-based directory can detect behavioral anomalies, such as a user connecting from an unusual location, to enforce conditional access

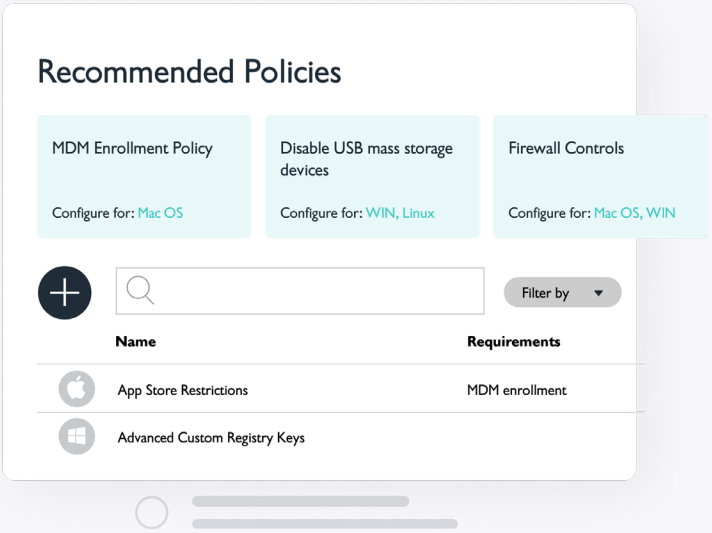
What's more, by utilizing a cloud-based directory, organizations of all sizes can realize the benefits of a domainless enterprise, as more and more SMEs are discovering:

- **Build Unified Identities** — View and manage users across directories, services, devices and networks
- **Configure and Control Devices** — Manage devices across multiple operating systems (OS)
- **Securely Access Anything from Anywhere** — Verify identity, verify devices, verify networks, authenticate, and authorize access
- **Transform Logs into Insights** — Centralize data, monitor and troubleshoot, and establish an audit trail for forensics and compliance

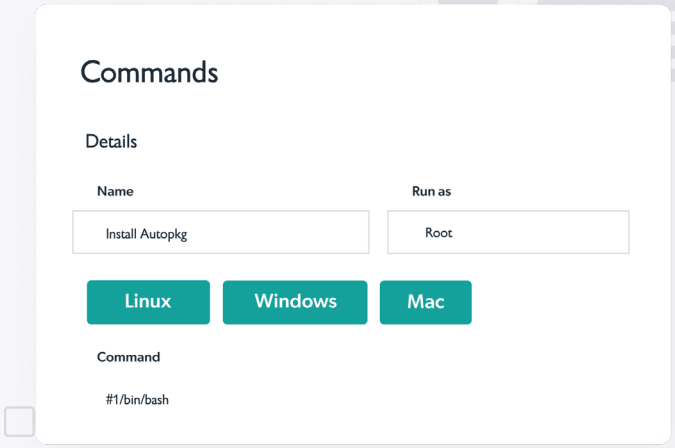
View & Manage Users Across Everything



Freedom to Manage Every Device



Deploy Powerful Tools to Manage IT



Conclusion – Zero Trust with Zero Friction

The events of 2020 catalyzed a shift to cloud and hybrid workplaces that will drive the next decade of innovation and shape the future of work — a future that still needs to be secured. Organizations that have not already adopted a Zero Trust Security architecture have already felt the pinch of legacy solutions as they strain to support their workers and secure cloud and hybrid workplaces. And even early adopters of Zero Trust would agree that there's room for improvement within older Zero Trust models. They need to continually reduce complexity, lower costs, and enhance the experiences of their employees and IT leaders — things that the right approach to Zero Trust can help with.

So the questions to ask are:

- How can your organization implement Zero Trust with the lowest cost and the least friction?
- If you're a small to medium-sized business with less time and money to spare, how can you leverage this proven approach to streamlining security and securing your workers, no matter where or how they're working?
- What's the cost of not adopting this technology now? What risks are you taking by delaying the deployment of Zero Trust security in your organization?
- And what would it do for your people, your business and your own personal reputation to be able to deliver a seamless, frictionless approach to securing your own hybrid workplace?

When you think about it, people in charge of securing businesses are often seen as "Dr. No." But with a smart, streamlined approach to Zero Trust, they have an opportunity to develop a new reputation as "Dr. No Problem." Even better, a unified directory of cloud-based identities enables security to become the "Dr. Knowing," since they can trace events back to any user, device, application, and location.

But to reach this point, organizations need to rethink their approach to information security and adopt a mindset of Zero Trust.

jumpcloud

JumpCloud's mission is to **Make Work Happen**® by providing people secure access to the resources they need to do their jobs. The JumpCloud Directory Platform gives IT, security operations, and DevOps a single, cloud-based solution to control and manage employee identities and their devices, and apply Zero Trust principles. JumpCloud has a global user base of more than 100,000 organizations, with over 3,700 customers.