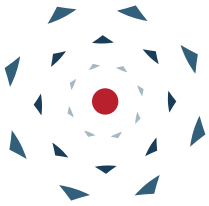

IDENTITY DEFINED
SECURITY ALLIANCE

WHITEPAPER

SECURING YOUR REMOTE WORKFORCE THROUGH IDENTITY-CENTRIC SECURITY

INTRODUCTION

For countless U.S. workers, the corporate office has moved from a multi-story building downtown to a four-walled room in their home. As the coronavirus spread, the number of stay-at-home orders for non-essential businesses spread as well, bringing a new challenge to many IT organizations across the country.

In the early days of the pandemic, many businesses went from a small portion of their workforce being remote to virtually all of it. This shift brought new complications to teams charged with controlling network access and ensuring compliance and security. Suddenly, there were new factors to account for: an uptick in users logging in from personal devices, attempts to access network resources from places that would normally be considered unusual, and more.

As jolting as that may have been, the workplace was already trending this way. According to a report from the U.S. Bureau of Labor Statistics, 24 percent of employed people did some or all of their work at home on the days they worked in 2019. The pandemic, however, appears to have pushed the needle forward even further. A Gallup poll released in October 2020 revealed that while many Americans are returning to their workplaces, 58% work from home either "sometimes" or "always." In addition, the Gallup survey reported that roughly two-thirds of those who worked from home during the pandemic would like to continue doing so once public health-related restrictions were lifted.

Whether IT organizations were ready or not, the coronavirus pandemic has become a test case for enabling a remote workforce. With the traditional network perimeter almost fully eroded, empowering employees to work remotely requires rethinking security, and many organizations have shifted toward a Zero Trust approach that puts identity at its center.

By prioritizing identity as a core element of security, organizations can get a handle on the challenges created by the remote workforce. In this report, the Identity Defined Security Alliance will examine how each of our Identity Defined Security Outcomes—the desired results of an identity-focused strategy—can help you better secure your organization as its employees go virtual.

WHY YOU SHOULD THINK IDENTITY FIRST

As companies balance realities such as cloud adoption, remote workers, and the use of personal devices, a growing realization has emerged: identity is the connective thread between the enterprise and its users. Regardless of what device they are using or what service they are consuming, identity follows employees everywhere. To threat actors, those identities are worth their weight in gold. They can be used to access sensitive applications, move laterally throughout a compromised network, access sensitive applications and systems, and ultimately exfiltrate data. Investigate enterprise data breaches, and stolen credentials will often be at the center. Protecting identities and effectively managing access, therefore, must be at the center of security.

When enabling a remote workforce, the importance of effective identity and access policies and controls is clear. Remote work brings new risks. If nothing else, there will be a surge in workers attempting to interact with network assets from unprotected networks and personal devices. By forcing so many workers to go remote, the COVID-19 pandemic has provided businesses with an opportunity to reexamine security and how best to empower their staff to be productive. To dive deeper, let's look at some real-world scenarios.

EMPLOYMENT ELIGIBILITY VERIFICATION IN A REMOTE WORK WORLD

Meet Marcy. She is a new employee at her company, just starting to adjust to her new quarantine work life. Due to social distancing and a stay-at-home order in her state, she was hired virtually—no face-to-face meetings, and no physically handing over documents to the Human Resources department (HR) for examination. As part of the process, she was given a username, password, and a laptop. From the job interview to completing paperwork to creating her login, this process was all done digitally— adding a twist to the hiring process for her new employer.

It is always critical for organizations to quickly provision users and devices without compromising security—not just during the hiring and firing process, but in the face of job changes and organizational shakeups as well. In all cases, moving too quickly can result in employees having either too much or too little access.

With a largely remote workforce, the joiner-mover-leaver cycle becomes more complex; companies that rely on physical boundaries or assets to help enforce access rights will no longer be able to do so. For example, if a staff member is taking on a new role within their company that requires them to switch offices, they may need to use different applications or require access to specific network resources as part of being in a new office. All this now has to be handled virtually, and the more automation IT can bring to bear, the better.

Then there is the stickier issue of verifying Marcy is who she says she is. In a survey released earlier this year by ResumeLab found 36% of respondents openly admitted to lying on their resume when asked directly. Other findings in the study indicate the real percentage could be as high as 56%. It might seem unlikely that someone would try to impersonate someone or falsely represent their actual identity to get a job, and perhaps it is. But in the category of the strange but true, in 2019, a woman in Australia was sentenced to 25 months in prison after using fraudulent information to get a job that paid $185,000 (USD) a year. The kicker—she also used a photo of supermodel Kate Upton on her LinkedIn page. The woman reportedly worked in the position for more than a month before she was fired.

Being able to trust newly onboarded employees requires being able to verify their identification documents. In practical terms, this may require businesses to rely more on identity verification services. Organizations need to establish an authoritative identity record that can drive downstream identity data and access. This information will serve as a single source of truth and be used as part of the identity-proofing process throughout the life cycle of the identity.

Securing through Identity Defined Security Outcomes

This scenario touches on several of the security outcomes promoted by the IDSA, particularly:

- Granting and removing user accounts and privileged access through governance-driven provisioning
- Ensuring the user's identity is systemically proven throughout the identity's lifetime

In the world of remote working, businesses need to exercise extreme diligence in identity-proofing and ensuring employees get the permissions they need.

EMPLOYEE OFFBOARDING IN A REMOTE WORK WORLD

One of the many unfortunate realities of the pandemic is layoffs. Just as the onboarding process changes for remote employees, so too does the offboarding process. Once an employee is let go, step one for businesses is to recover any company-issued laptops and devices. Normally, the employee could drop these assets off at the front desk as they left the building. However, when workers are remote, the IT and HR departments must coordinate closely to ensure any items given to employees are returned. Another critical step is to revoke a terminated employee's access to the network and corporate data, reducing the risk of malicious activity by the fired employee or an attacker abusing their credentials.

Consider the case of Tony. Tony was a marketing specialist at his company. He was laid off due to budget cuts after the pandemic caused sales to fall short. Because of his position, he has access to sales documents and confidential data about customer profiles. He also has access to a myriad of customer relationship management (CRM), project management, and social media management tools. All of these access privileges need to be identified and rolled back.

Securing through Identity Defined Security Outcomes

As remote employees like Tony come and go, IT and HR should have a checklist of what needs to be done. Effective deprovisioning of users touches on multiple IDSA recommendations, including:

- Removing user accounts and entitlements through governance-driven provisioning
- User access rights are continuously discovered
- Device characteristics are used for authentication

Onboarding and offboarding, however, are only two areas impacted by the surge of remote workers. Organizations also face an increased use of personal devices, a change that, if left unaddressed, could punch holes into an enterprise's layered defense.

ENDPOINT SECURITY AND SECURITY'S ENDPOINT

Juan is a longtime employee of a financial services company. Working in a regulated industry, his company was in the process of implementing a Zero Trust architecture when the pandemic hit. The move was largely in response to the adoption of mobile technologies and cloud services and the need to maintain security and compliance across an increasingly complex environment. As he works from home, he switches between his work laptop and his wife's computer and uses the latter to access his Salesforce account.

Unfortunately for Juan, his endpoints of choice are not equally secure. Suddenly, a new level of risk has been introduced to Juan's company. Such is the world of personal devices in the workplace, where this type of occurrence is far from uncommon. Devices outside the control of IT are often not subject to the same security policies and enforcement. In this scenario, if his wife's computer is infected, Juan may have just had his password compromised along with corporate data.

Security policies for remote workers have to account for users doing things they would not do if they were in the office. Juan would not have access to his wife's computer normally; he would be using his own machine, which had been provisioned by IT. He would also be accessing resources from a common location—his office. Since he is telecommuting, however, he will be requesting access to systems and data from off-site, changing the profile of his normal user behavior.

Organizations adjusting to having a larger percentage of employees working remotely should be prepared to modify some of the criteria they use to determine the legitimacy of an access request. For example, if an employee is now working at a different geographical location or during different hours of the day, it may not warrant the alert that it would raise under old circumstances. Still, certain types of behavior should set off a red flag. For example, an unusually high number of log-in attempts to certain applications could indicate a compromise. Strong security will require the proper correlation of information about a user's activity and history.

This is particularly important in scenarios where physical security is used as a control to protect sensitive systems. Consider the case of a data center administrator who previously could only access a certain set of machines with a physical badge that permitted him entry into a room. Those machines, however, may now have to be accessible remotely, meaning those rules will have to be safely relaxed. To enable secure monitoring and management of critical systems remotely, IT security teams need a layered defense that prevents unauthorized activity.

One of the most basic and critical layers of this defense involves implementing the principle of least privilege. This policy ensures employees do not get permissions and privileges they do not need to do their job, and hampers attackers' efforts to move throughout the network if a computer is compromised. To reduce risk, this same standard should carry

over from the corporate office to the home office. If someone in Juan's family utilizes his work laptop to visit a malicious site or inadvertently downloads malware, administrator-level permissions will increase the company's risk of damage.

Securing through Identity Defined Security Outcomes

Answers to these challenges all map to security outcomes promoted by the IDSA to keep organizations safe, particularly:

- Using device characteristics for authentication decisions
- Analyzing user behavior to determine if it is normal
- Enforcing the principle of least privilege

Implementing these outcomes reduces risk, whether employees are remote or on-site. Organizations adjusting to having a larger percentage of employees working off-site should be prepared to modify some of the criteria they use to determine the legitimacy of an access request. For example, if an employee is now working at a different geographical location or during different hours of the day, it may not warrant the alert that it would raise under old circumstances. Depending on the sensitivity of the systems or information the user is trying to access, it may be best to restrict access to machines provisioned by IT.

SECURE REMOTE COLLABORATION

The fact that employees like Juan and Marcy will be out of office makes confirming their identity that much more important. Multifactor authentication (MFA) is a common solution to this problem and should be a critical part of the strategy for enabling remote workers. Even if Juan's password is stolen due to him unwittingly using an infected computer, with MFA, any threat actor would need the second mechanism to authenticate. The explosion in the use of collaboration tools like Zoom and Cisco Webex by business users means these solutions may need an extra layer of protection. Tying MFA capabilities to these applications can save businesses a number of potential headaches, particularly in light of media reports of attempts to hack video conference calls.

There was a similar surge in attacks targeting Remote Desktop Protocol (RDP) that coincided with the rise of the pandemic in the U.S. RDP is used to connect Windows machines to each other so that a remote user can access a system. It is typically used in Help Desk situations for troubleshooting. Its capabilities make it a juicy target for attackers and preventing exploitation by ensuring it can only be accessed through a VPN connection and MFA offers an additional level of protection.

Securing through Identity Defined Security Outcomes

MFA challenges can be triggered for many reasons, including a new login attempt, password changes, or suspicious activity. One of the more commonly implemented security outcomes on the IDSA's list, MFA is one of several identity-focused recommendations that can empower secure collaboration, including:

- Enabling re-attestation or revocation of user rights after the detection of a high-risk event
- Ensuring access rights to sensitive data are attested

Secure collaboration may also involve using VPNs more extensively. While some companies may have only enabled a limited number of employees to use a VPN, the realities of the pandemic may lead to increased usage. To keep pace, organizations should consider tracking metrics about VPN health and performance. Additionally, security teams should be aware of the increased threat of phishing attacks targeting VPN credentials, as well as attacks on VPN servers themselves. On Oct. 9, 2020, the FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) warned that threat actors were using a recently disclosed Windows Netlogon vulnerability, commonly called Zerologon, in conjunction with VPN vulnerabilities in a spate of sophisticated attacks. Most of these attacks were aimed at government entities, but that could change at any time.

The prospect of data leaks in the event of a compromised VPN credential is real. Ensuring that users with access to sensitive data do not have excessive permissions and are not sharing confidential information with unauthorized internal or external parties is critical for preventing data leaks. When a user leaves the organization or changes position, their permissions should be revoked to prevent a potential breach. This process should be automated as much as possible to reduce the potential for manual errors.

From a strategic perspective, enabling IDSA's security outcomes strengthens efforts to create a more secure environment for remote workers to thrive. The approach to enabling these actions, however, must be dynamic and adaptable. What if a managed device is not available to an employee? What if security updates that required administrator rights or physical access to a machine are not doable? Policies may need to change drastically between today's situation and tomorrow's, and different scenarios require that be taken into consideration.

SECURING REMOTE WORKERS IS SECURING THE FUTURE

The growth of the remote workforce has long been predicted. Few, however, would have projected that its growth would involve a pandemic. COVID-19 may have pushed businesses further down this road, but the road was paved long ago and had been attracting higher levels of traffic for years. As more workers look for opportunities to go remote, businesses will have to find ways to balance cybersecurity with the ability to promote increased productivity for all their employees.

ADDITIONAL RESOURCES

IDSA Blog: Privileged Access Management Starts with Endpoint Privilege

Dark Reading: Top 5 Identity-Centric Security Imperatives for Newly Minted Remote Workers

IDSA Blog: BYOD Doesn't Have to Mean Bring Your Own Vulnerability

IDSA Blog: Customer Advisory Board Conversations: Zero Trust and the Remote Workforce

ABOUT IDSA

The IDSA is a group of identity and security vendors, solution providers and practitioners that acts as an independent source of thought leadership, expertise and practical guidance on identity centric approaches to security for technology professionals. The IDSA is a nonprofit that facilitates community collaboration to help organizations reduce risk by providing education, best practices and resources.

We deliver on our mission through…

1. Cross vendor collaboration
2. Thought leadership content
3. Identity Centric Security Framework
4. Customer implementation stories
5. Virtual community for sharing experiences and validation

For more information about the IDSA visit www.idsalliance.org.