THE ESSENTIAL GUIDE TO

Securing Remote Access

Building Trust in a Modern Remote World

DUO

CISCO The bridge to possible

THE ESSENTIAL GUIDE TO

Securing Remote Access

Building Trust in a Modern Remote World

Table of Contents

Remote Access: The New Reality

Remote access reality check:

Remote access reality check: How prepared was your organization for the pandemic of 2020? If your answer is “not very,” you are not alone. Few could have predicted the circumstances that sped up the work from home (WFH) movement and catapulted remote access to the forefront for many organizations. Prior, there was a steady trend by some to support geographically diverse workforces with an emphasis on remote access. For most companies, however, a 100% virtual workforce was never the intention nor were there infrastructures and architectures designed to support it. Then came 2020 where, like it or not, remote access became the norm and organizations had to support entirely remote workforces as a requirement to continue to do business.

Mandatory work from home orders forced employees, students, teachers and government officials to update their technology proficiencies in real time, presenting a stressful, hyperfast learning curve; and implementing an additional layer of secure remote access should not increase their mental burden. Organizations need employees to be productive and stay connected without friction. Workers need flexibility to work on their own devices (tablets, phones, or laptops), and access all their applications, both SaaS apps in the cloud and on-premises.

As the world replaced face-to-face business with online only interactions, the challenges of allowing access from anywhere dramatically increased the risk surface. After the initial scramble to enable people to work remotely, questions started to be raised around:

- How can you secure all users and devices accessing your applications and services amid the rapid adoption of virtual access?
- How can users gain access at any time from anywhere from any device?
- How can you provide global access while maintaining security?

As many organizations plan to continue to support remote workforces beyond 2021, making sure this can be done securely is critical.This guide will explore some of the challenges faced with supporting remote access and the solutions available to address them. We will walk you through how Duo can help to protect your remote workforce.

Security Challenges With a Remote Workforce

The rapid transition to remote work resulted in a window of opportunity for bad actors interested in compromising systems for financial gain. The shifted perimeter exposes many different vulnerabilities in multiple vectors. As the perimeter is now everywhere and anywhere users are (or where access happens), security has to move with it and needs to be in place at the point of access.

Targeting Users Remotely

When thinking about security, there is one thing that's predictable: the unpredictable human factor. Despite a company's best security efforts, the human element is still low hanging fruit for criminals to exploit and remains the most difficult factor to control. We're quick to click when lured by the right messaging. It's a low-tech, easy yet effective way to get access to apps and remain undetected by logging in as a legitimate user.

Security Magazine reports **88% of data breach Incidents**[1] were caused by human error and employees responding to socially engineered attacks.

It's worthwhile to spend a little time considering the different types of attacks that target users.

Phishing Campaigns

What's old is new again, or in reality it never really went away, it simply became more sophisticated. Phishing, for example, continues to flourish. The Cisco 2021 Threat Report found that in 2020, **86% of organizations had at least one user try to connect to a phishing site. The Verizon 2021 Data Breach Investigations Report**[2] (DBIR) found 36% of breaches were due to phishing. The same report shared that 61% of breaches involve credential data and 85% of social engineering attacks involve credential data. Also, for web applications, 89% of hacking incidents involved credential abuse (either use of stolen credentials or brute force).

The bottom line is securing credentials helps prevent the majority of hacks. Humans will be humans, but through **multi-factor authentication** (MFA) and good security practices, we can help thwart human error and maintain secure access. An Executive Order signed in May 2021 by U.S. President Biden mandates government agencies implement MFA to mitigate risk and enable a zero trust security model.

Increased Video Conferencing Means New Pools to Phish

An increase in remote work typically results in a reduction of face-to-face, in person meetings. Thus, much of the workforce turns to video conferencing solutions. Almost immediately in 2020 we bore witness to the problems with free and virtual web meeting tools. Attackers were quick to exploit vulnerabilities in the service and leak user data.

In 2020, **Forbes reported**[3] more than half a million video conference tool credentials were for sale – for a single cent per ID – and **Webroot (via Channel Futures) reported**[4] that it saw a 2,000% rise in malicious files containing the name of one popular free conferencing service.

The Verge reports[5] in May 2020 alone 2,449 domains related to one video conferencing service were registered with 32 malicious domains and 320 deemed "suspicious." And in one instance of attempted phishing, hackers sent an email that looked like an official email from a chat service, but a button in the email to "open" the chats was actually a malicious URL that downloaded malware to the user's computer.

Securing the remote workforce, the network, the applications and the devices with access quickly and seamlessly has never been more crucial.

Phishing for Cold Hard Cash: Ransomware

Ransomware is one of the most troublesome cyber threats. In 2021, one of the most high-profile ransomware attacks was on the **Colonial Pipeline**[6]. That attack caused a company shut down, disrupted its fuel distribution operations and compromised personal information of about 6,000 individuals. The company paid $4.4 million to the adversary group, DarkSide, The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CIS) have **observed an increase in highly impactful ransomware attacks occuring on holidays and weekends** in the USA. The frequency and impact of ransomware attacks is a wake-up call for the importance of cybersecurity.

The way ransomware typically works is attackers use various nefarious techniques like phishing, spear phishing and social engineered attacks to plant malicious code on a computer. They hold the network hostage and ask for a ransom, typically in Bitcoin because it is untraceable.

Cybercriminals now steal data before they issue ransom and threaten to sell it on the dark web in case a victim decides not to pay – as a way to make paying the ransom a more attractive option than having their info up for auction on the dark web. ZDNet.com reported **ransomware accounted for 41%**[7] of all cyber insurance claims in the first half of 2020.

According to **Coalition**, one of the largest cyber insurance service providers in North America, the average ransom demand made to policyholders in the first half of 2021 was an incredible $1.2 million! Per the Ponemon Institute **Cost of a Data Breach report**, the average total cost of a ransomware breach was $4.62 million. Notably, this refers to the total costs associated with escalation, notification, lost business and response – not the cost of the ransom.

The best defense against ransomware is a strong security offense.

Brute-Force Attacks

Brute-force attacks use a persistent trial and error-based technique of decoding passwords or other encrypted data. If attackers can't steal a password, they can use dictionary attacks and automated tools to guess weak passwords.

"According to the DBIR report, for web applications 89% of the attacks involved brute force or the use of stolen passwords. If we can collectively shift towards utilizing MFA, while keeping an eye towards the future with passwordless technology such as WebAuthn and biometrics, we will embrace a safer future," said David Lewis, Duo's Advisory CISO.

Password-Stealing Malware

The U.K. National Crime Agency (NCA) report found computer-related crime recently surpassed all other crime types for the first time, partly due to the use and sale of financial Trojan malware.

A few types of these Trojans, named Dridex and Neverquest, include a **keylogger**[8] component (malware that records keystrokes of unsuspecting users) to record and harvest stolen credentials used for bank accounts and financial processing systems. Criminals could log into their accounts remotely and conduct fraudulent money transfers.

In addition to keylogging, new malware like **MosaicLoader** steals Windows passwords through advertisements in search results.

Keylogging is hard to detect and effective, but not against a strong MFA method. By requiring a variety of factors to be verified before granting access, MFA can shut down password-stealing malware before it starts.

Targeting Devices Remotely

With bring your own device (BYOD), users are using their own devices (like smartphones, laptops and tablets) to log into work applications remotely, from home, at school and while traveling. The growth in remote work has led to an increase in BYOD, which many companies are trying to get a handle on.

The problem is IT departments can't manage these unknown devices. With no insight into how secure or up to date they are, unmanaged devices can bring with them the risk for malware or exploitation – providing an entry point into an organization's environment. Out-of-date software and devices also pose the risk of zero-day attacks. A remote workforce typically relies heavily on a mix of devices. **Mobile phishing rates are 200% higher**[9] for users of Office 365 and G-Suite than those without mobile access to these apps, according to Lookout data.

The Risk Lifecycle of an Out-of-Date Device

1. An emergency update is released
2. User ignores it and goes about their workday
3. Attacker recodes an exploit kit to include the new vulnerability
4. User opens a phishing email, clicks on a malicious link
5. Drive-by download launches an attacker's exploit kit
6. Exploit kit checks user's device for outdated version
7. Exploits vulnerability to download malware on device
8. Malware contains keylogger that tracks username/password
9. Sends that and other sensitive data (financial) to a command and control server
10. Attacker success!

Exploiting Out-of-Date Devices

How quickly do your users update their smartphones? Typically, there's a window of time between when a new vulnerability is reported, and when an attacker attempts to exploit it (before a user updates their software).

Duo's 2020 Trusted Access Report[10] revealed that Android mobile device users are 350% less likely than Apple users to have the latest security patch installed within a month's time. Why does this matter? Attackers often integrate new software vulnerabilities into their exploit kits, which are designed to execute payloads and install malware on users' devices.

In early 2020, browsers by **Google Chrome** and Firefox both patched zero-day bugs that enticed users to visit a specially-crafted web site booby-trapped with an exploit that took advantage of a browser memory corruption flaw to execute code remotely.

An exploit kit can be triggered when a user visits a malicious site, or clicks a link. The kit checks a user's machine for what version they're running before serving up an exploit that installs malware on their machine, which may give them control over their system or the ability to steal data.

Spreading Malware

If users are logging into your company's applications with outdated devices, there's a chance they could also be unwittingly spreading malware and using keyloggers to record your keystrokes. Meaning any data you type, including your username or password, can be recorded and sent to an attacker's command and control servers.

That means your company's data could be at risk if just one out-of-date device logs in, potentially spreading malware to your environment. Or worse, spreading ransomware that will keep your files hostage until a ransom is paid to decrypt them.

Remote Access Goes Both Ways

Even before the spikes in remote work in 2020, many organizations had contractors or remote employees who used remote access software to gain access to the applications or work resources needed to do their jobs. Attackers can take advantage of the convenient access to compromise your environment.

Remote Desktop Protocol Security Risks

Remote Desktop Protocol (RDP)[11] is a protocol that connects a user to another computer remotely over a network connection. For example, an employee can access all of their work computer's programs, files and network resources from their home computer using RDP. It's also often used by tech support to remotely access workstations that need repair.

According to **CSO Online who cited a McAfee study**[12], 4.5 million RDP servers are exposed to the Internet alone. Also, the percentage of businesses that had insecure remote access enabled when they applied for insurance grew by 175% or nearly doubled from H12020 to H12021, according to **Coalition**[13]. RDP usage may be one of the greatest sources of financial losses incurred by organizations and while insurance may give some temporary relief, it is certainly not the cure for proactively mitigating risks associated with RDP access.

Unfortunately organizations will often unknowingly leave RDP client ports open to the internet, leaving themselves vulnerable to attackers that scan blocks of IP addresses for open RDP ports. In one instance, attackers located internet-facing RDP servers of corporate networks storing payment card information, then brute-forced the passwords in order to spread ransomware.

New Malware

The biggest problem is the massive increase of new endpoints (that cannot be accounted for) trying to connect to a network, expanding the threat surface exponentially. **DarkReading.com**[15] reports one particular malware that emerged in 2020 that the FBI is concerned with, called Ryu. This attack is deployed through RDP endpoints. It uses a powerful kind of data encryption that targets backup files to infect users. A single infected user can spread the virus to an organization's servers making it extremely difficult to contain.

Cashing in Through a Backdoor

In 2020 hackers also harvested and sold as many as 250,000 RDP server credentials in an underground marketplace, **xDedic**[16]. These credentials gave buyers access to all of the data on the servers and the ability to launch future attacks using the servers. Attacks against RDP grew by 768% in 2020, according to **ESET**[17].

Virtual Private Network Risks

VPNs, or virtual private networks, are another way to provide remote users an encrypted connection over an internet network. While logging into these networks helps users securely and remotely access work resources and applications, they can be exploited by hackers seeking to steal login credentials.

VPNs are software, and like any other kind of software, they sometimes have bugs and could leak private user information. In one case, **several VPN providers were leaking IP and DNS addresses**[18] that could allow an attacker to identify users and locations.

Another vulnerability could allow an attacker to hijack web traffic through a VPN to a proxy server, which could then give them information about a user's browsing activity. This could occur if an attacker convinced a user to click on a malicious link.

VPNs do provide overall better security, but they are not infallible when it comes to potential security risks, and supporting large scale remote workforce efforts can result in poor performance due largely to increased loads they were never designed to support. As a result there has been a shift towards looking for VPN alternatives or replacements that offer a direct tunnel to applications that remain behind on the traditional corporate network.

> VPNs protect the connection, but they need protection as well.

Security Considerations for Vendor and Contractor Access

It is not uncommon for organizations to employ contractor services from outside organizations. This means these external, or third-party, users also need access to corporate resources, both in the cloud and on-premises. Generally these users are set up with accounts within corporate systems to enable access to the tools they need, and there must be appropriate controls in place to support this.

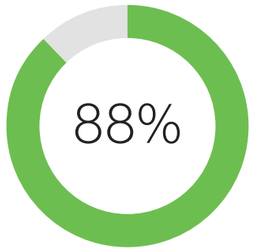
One common tactic is a hacker will steal the credentials of a contractor or smaller vendor to get access to a larger organization. They can do this by impersonating the user, using the stolen credentials to access expected resources and then moving laterally through the system to obtain the valuable data they can monetize.

Some recent examples include:

- **Saudi Aramco**[19], one of the world's largest oil and natural gas firms, said that some corporate data was leaked after adversaries breached one of its suppliers. The hackers "Zerox296" obtained access to information on 14,000 employees -- their passport details, phone numbers and ID numbers, as well as invoices, contracts, client data and documentation about Saudi Aramco's network, by exploiting a zero-day vulnerability in a cloud storage platform.
- **Morgan Stanley**[20], a renowned investment banking firm, reported a data breach after attackers stole personal information of customers by hacking into the Accellion file sharing service of a third-party vendor. This vendor, Guidehouse, provides account maintenance services to Morgan Stanley's StockPlan Connect business. The stolen documents included information on stock plan participants' names, their last known addresses,dates of birth, social security numbers and corporate company names.
- **Multiple Managed Service Providers (MSPs) and clients**[21] were impacted by an attack on Kaseya Virtual System Administrator (VSA) software. The ransomware gang, known as "REvil" (aka.Sodinokibi), used the Kaseya VSA tool as an attack vector to inject ransomware into the systems of around 1,500 end-customers of approximately 30 MSPs at the start of the USA's Independence Day weekend. By compromising the Kaseya VSA software, the ransomware operators compromised the MSPs and gained privileged access to thousands of the MSPs' customers' devices, given the high level of trust that IT monitoring software usually requires. However, this ransomware supply-chain attack's main targets were the MSPs from whom the operators demanded $5 million each.

Data breaches caused by third-parties[22] cost millions of dollars to large companies and are often devastating to small businesses. A recent survey conducted by the Ponemon Institute revealed data breaches caused by a third-party cost an average of $4.33 million to remediate.

The Cloud is Great — Until It's Not



Organizations using cloud infrastructure in 2020

There has been a massive increase in the adoption of Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) cloud solutions. Web applications can be accessed via a browser, and include services such as email, data storage, collaboration and productivity apps. In fact, 80% of organizations are predicted to migrate toward cloud, hosting, and colocation services by 2025, according to **Computerworld UK**[23]. The events of **2020 accelerated cloud adoption**[24].

According to the Verizon 2021 DBIR, web applications accounted for 80% of breaches while 61% of breaches involved credential data. There are security concerns to be addressed with this increased adoption of the cloud, as they can be compromised and used to host or send malware. Attackers can also get access to billing information, cloud data and password controls if they steal your root account credentials. Some cloud vendors recommend that you **don't use root account credentials for everyday access**[25].

The **"Cloud Adoption in 2020"**[26] report found that even before the pandemic began, 88% percent of organizations were using cloud infrastructure in some form, while 45% reported they expect to move 75% or more of their applications to the cloud over the next year. The report also found that a critical business need – cited by 65% of the respondents – is more IT workers who are fully-trained in cloud-based security for migrating applications and implementing cloud-based infrastructure. Security is not nice to have, it is necessary.

> Security is not nice to have, it is necessary.

Securing the Modern Workforce

There is no denying that 2020 profoundly impacted the way in which we work and these changes are likely to remain. Securing the modern workforce and protecting core business assets, regardless of where they are hosted, requires verifying the users and establishing trust in the devices requesting access. No matter where the request originates from, applications that could be anywhere, there is a need for access controls to protect against the risks associated with different attack methods, such as phishing, credential theft and vulnerability exploitation.

Security should not be complicated or painful. It also shouldn't create barriers to user productivity, or require a complete redesign of your environment. Duo Security, now part of Cisco, aims to make security radically simple for everyone by providing features and functionality to support organizations, no matter their size or what they have in their environment. Duo's mission from the very beginning has been to democratize security – our goal is to remove the barriers of security by making it accessible, affordable and attainable for all.

Zero-Trust Security

Traditional security relies on location-based trust. **A zero-trust model**[27] establishes trust for every access request — regardless of location. It enforces adaptive controls, and continuously verifies trust. From the start, the principles of zero trust were baked into Duo's ethos. We entered the market with a strong MFA solution that provided a balance between usability and security. Since then we have evolved with our customers to offer a security solution with full coverage.

Our goal is to secure how users and devices access applications — which is the foundational cornerstone of a zero-trust security approach. We establish trust at the point of access by verifying users, assessing the trustworthiness of devices (managed and unmanaged) and protecting applications with access controls and by only allowing access when security requirements are met. Using a holistic security solution can defend against an exploit aimed at multiple vectors and help organizations meet various regulatory frameworks and compliance requirements.

Duo is positioned to help protect organizations from ransomware on three fronts:

1. Preventing ransomware from getting an initial foothold in an environment

2. Preventing or slowing down the propagation of ransomware if it manages to infiltrate an organization

3. Protecting critical assets and parts of the organization while an attacker still has a presence in the environment and until full remediation is achieved

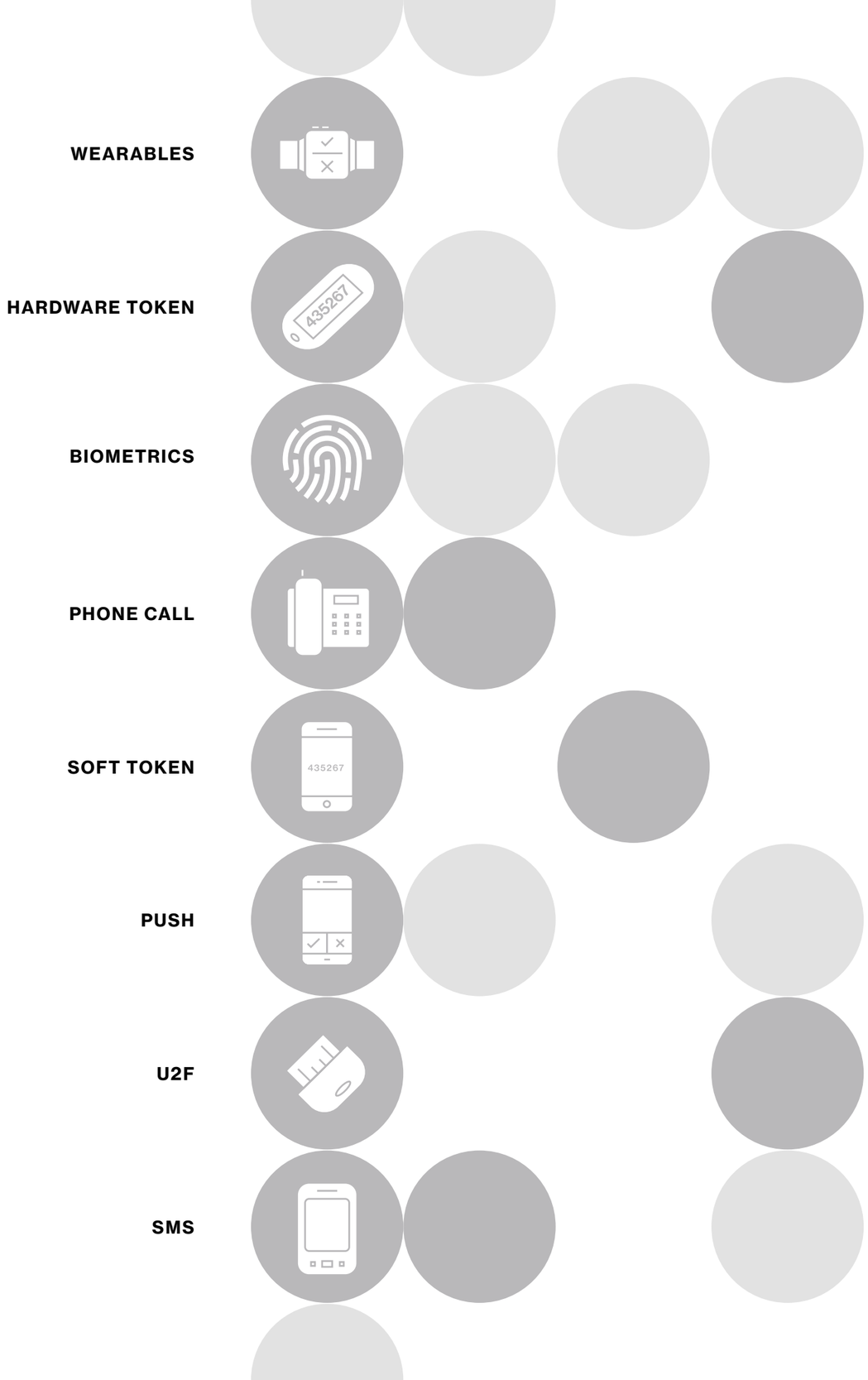
Trusted Users

Ensuring the trust of your users whenever they attempt to access applications remotely is the first step toward secure access and zero trust. This requires leveraging strong authentication controls, like **MFA**[28],monitoring user behavior, employing context-based access controls, and providing a streamlined user experience through things like single sign-on (SSO).

In this section let's take a look at how Duo can help you establish trust in your users.

Broad Authentication Options - Protect Against Phishing

Adding MFA to your security stack doesn't have to be disruptive to your users. Duo is fast and easy for users to set up, and with several available authentication methods, they can choose the one that best fits their workflow. No headaches, no interruptions – it just works. Administrators can set up enrollment options that best fit your organizational needs to ensure a successful adoption.



Contextual Authentication Policy Controls - Limit Access to Resources

Use an authentication solution that also gives you **detailed data and logs**[29] about your users, including their name, IP address and location, time of authentication attempt, integration/application type, authentication method and result (authentication success or failure).

With this data, you can create custom authentication controls to restrict access based on your organization's needs – for example, set up a **geolocation policy**[30] based on user location parameters and block all users from countries you don't do business in.

Trust Monitor - Monitor for Risky User Behavior

We developed **Trust Monitor**[31] to shorten the time administrators need to spend sorting through logs, while simultaneously highlighting suspicious logins automatically. The goal is to help organizations find and remediate access threats early. By leveraging data and Duo's unique insight into devices, users and context when accessing applications, Trust Monitor can quickly surface actionable anomalies which make your business more secure without having to invest in your own machine learning program.

Single Sign-On (SSO) — Simplify Access to Applications

Single Sign-On (SSO)[32] allows users to access any and every application, whether it's on-premises or cloud-based, with the same username and password. Access can be further simplified by consolidating all end-user facing applications into a single website or launcher. Users login just once and access all their applications without having to login again. By combining this with strong authentication and access policy controls, access attempts are validated and logged for each access attempt, but the friction to users is reduced through streamlined workflows.

SSO lets organizations reduce the number of passwords needed and improve user experience and security, and WebAuthn uses biometrics as an authentication method without requiring a password. When you protect SSO with strong MFA and access policies, organizations can provide a streamlined user experience that is secure and doesn't add friction to their workflows.

Establishing Device Trust

Organizations need to enable secure and direct access to business applications for a diverse set of users (remote workers, vendors and contractors) and their devices that typically reside outside of the control of corporate EMM (enterprise mobility management) and MDM (mobile device management) solutions. Enforcing consistent security policies across managed devices, bringing your own devices (BYOD) and third-party (contractor or partner) devices poses a significant challenge for security teams. IT security teams often lack the insights and an enforcement mechanism when making an access decision on endpoints, particularly among unmanaged devices. This is when **device trust** is important to establish.

Duo can automatically flag out-of-date devices based on your security profile, saving your administrators upkeep time and allowing them to focus on your core business objectives. Duo identifies risky devices, enforces contextual access policies, reports on **device health** using an agentless approach or by integrating with your device management tools, and offers **self-remediation**.

Here's how we do it.

Endpoint Visibility - Protect Against Out-of-Date Exploits

Visibility is important to verify and enforce device trust policies. When organizations deploy Duo, device trust becomes a part of the authentication workflow during the user login process for protected applications. This enables Duo to provide in-depth visibility across any device, irrespective of how and from where the users connect to these applications.

Duo's logging and reporting enables organizations to maintain an inventory of all devices accessing corporate resources, even BYOD (bring your own device)

The dashboard helps administrators understand the overall organizational security posture, and a quick drill-down with just a few clicks allows them to identify users who are using risky devices (running out-of-date operating systems (OS), browsers, Flash and Java versions). All of this data can be easily exported to any log management and analysis tools. And, administrators can schedule reports, making it easy to prove compliance.

In addition with Duo's **Self-Remediation**[33], admins can also notify users to update the software on their mobile or desktop device when they log into Duo-protected applications, via the authentication prompt. The prompt provides context on what is out of date, a link or instructions on how to update, and the number of days the user has to update until they'll be blocked from accessing the application.

Trusted Endpoints - Differentiate Managed and Unmanaged Devices

Duo helps you distinguish between unmanaged and managed endpoints that access your browser-based applications.

Duo's **Trusted Endpoints**[34] allows you to identify corporate IT-managed devices and can use existing device management infrastructure to establish and enforce device trust with integrations with Active Directory, Airwatch, Google, Jamf, Landesk, MobileIron and Sophos to deploy certificates. The Trusted Endpoints policy tracks whether clients accessing the applications have the Duo device certificate present, or can block access to various applications from systems without the Duo certificate. Secure your BYOD environment by differentiating between company and employee-owned devices that access your applications with the **Duo Mobile app.**

The **Duo's Device Health Application**[36] is a native client application for MacOS and Windows that checks the health of devices when a user authenticates to Duo-protected applications. The application provides visibility into device health and blocks unhealthy devices based on granular policies.

Secure Application Access From Anywhere

Strong access controls and device security checks are only effective if they're applied to **every application**[37]. While there is a strong move towards increased cloud adoption, your organization is most likely running a hybrid environment with a mix of self-hosted, co-located, cloud-hosted, and/or cloud native applications. To ensure user adoption of the security controls you put in place, it is optimal if you can deploy solutions which streamline access and provide a consistent experience regardless of where the application lives. Duo integrates to protect existing infrastructures, adding security at the front door:

- **VPNs**[38] - Juniper, Cisco and Palo Alto and more
- **Cloud apps**[39] - Microsoft Office 365, Salesforce, Google Apps, AWS, Box and more
- On-premises and **web apps**[40] - Epic, SSH, RDP, UNIX, WordPress and more
- **Custom apps and services** - Use APIs and client libraries like Python, .Net, Ruby and more

Provide Modern Remote Access - Secure VPN and RDP

Duo provides flexible **access solutions** that can be used in conjunction with existing VPN solutions, reverse proxies and bastion hosts. Alternatively, organizations can leverage the **Duo Network Gateway (DNG)**, a remote access proxy, to provide remote access and a consistent login experience for users without exposing sensitive applications to unnecessary risk and ensuring only authorized users can gain access.

Providing a remote access proxy option combined with SSO improves the flexibility, agility and scalability of application access and enables organizations to provide remote access without exposing internal applications directly to the internet, reducing risk of attack. Leveraging technologies like a remote access proxy also alleviates the burden on hardware and bandwidth employed by traditional VPN access solutions for remote access. Many organizations are adopting a hybrid approach to providing secure remote access, complementing traditional VPN deployments with remote access proxies.

Create Custom Remote Access Policies - Prevent Lateral Movement

Create **custom access policies and controls**[41] on a per-user group and per-application basis to restrict remote user access. Give your users access to only what they need to do their job. This principle of least privilege can reduce the scope of risk if their account or device is compromised.

Additional Security Recommendations

Security Education Is Mission-Critical

One of the most effective ways to combat cyber crime is ongoing **security education**[42] and training. Communication solely online makes social engineered attacks easier, and organizations must ensure their remote end users are aware of that. **Fortune.com reports**[43], hackers may call into a department and pretend to be another department of an organization or a government official to gain access or direct users to install malware. They may pretend to be employees having remote access problems thus tricking IT staff into giving them access. Regular security education has proven to work according to the findings in the Verizon 2021 DBIR report.

Here are some other ways you can protect against remote access attacks targeting your users, devices and applications.

Eliminate Unnecessary Software
Uninstall any unused software on your devices, including potentially unsafe third-party plugins on your browsers to reduce the attack surface.

Timely Patch Management
Install patch updates as they are released to prevent an attacker from exploiting any known vulnerabilities against the old version.

Set a Lockout Policy
Set an account lockout policy that locks accounts after a certain number of incorrect guesses, to prevent the success of brute-force attacks. Enable this for your multi-factor authentication as well.

Encourage Supported Devices
Educate and encourage users to choose secure personal devices that receive security updates in a timely manner. Other devices rely on their manufacturers to update for security, which is not always reliable or timely.

Delegate by Creating Roles
Instead of sharing your cloud credentials, **create Identity and Access Management (IAM)**[44] roles with specific permissions for separate users that need access to your account resources.

Use Least Privilege
Organizations should apply the zero-trust principle of least privilege by only allowing access to the applications their workers need using policy controls and securing applications. This prevents lateral movement throughout the infrastructure and reduces the risk of exposure or exfiltration of protected data.

References

1. *Moving to measure a cyber-aware culture* (https://www.securitymagazine.com/articles/95247-moving-to-measure-a-cyber-aware-culture); TechRadar; May 19, 2021
2. *2021 Data Breach Investigations Report* (https://www.verizon.com/business/resources/reports/dbir/); Verizon; 2021
3. *Zoom Gets Stuffed: Here's How Hackers Got Hold Of 500,000 Passwords* (https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/#3fa8ffd5cdc4); Forbes; April 28, 2020
4. *10 Destructive COVID-19 Data Breaches* (https://www.channelfutures.com/mssp-insider/10-seriously-destructive-covid-19-data-breaches); Channel Futures; July 20, 2020
5. *Hackers are impersonating Zoom, Microsoft Teams, and Google Meet for phishing scams* (https://www.theverge.com/2020/5/12/21254921/hacker-domains-impersonating-zoom-microsoft-teams-google-meet-phishing-covid-19); The Verge; May 12, 2020
6. *Colonial Pipeline ransomware attack* (https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html);
7. *Ransomware accounted for 41% of all cyber insurance claims in H1 2020* (https://www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/); ZDNet; Sept. 10, 2020
8. *Keystroke logging* (https://en.wikipedia.org/wiki/Keystroke_logging); Wikipedia
9. *Credential Harvesting Attacks Take Aim at Video Meeting Apps* (https://www.technewsworld.com/story/86820.html); Tech News World; APril 27, 2020
10. *The 2020 Duo Trusted Access Report* (https://duo.com/resources/ebooks/the-2020-duo-trusted-access-report); Duo Security; 2020
11. *Remote Access Integrations* (https://duo.com/solutions/features/supported-applications/rdp-remote-desktop-protocol); Duo Security
12. *Attacks against internet-exposed RDP servers surging during COVID-19 pandemic* (https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html); CSO Online; May 8, 2020
13. *Cyber Insurance Claims Report* (https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf); Coalition Inc; H1, 2021
14. *Remote spring: the rise of RDP bruteforce attacks* (https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/); Secure List; April 29, 2020
15. *Safeguarding Schools Against RDP-Based Ransomware* (https://www.darkreading.com/risk/safeguarding-schools-against-rdp-based-ransomware/a/d-id/1338943); DarkReading; Sept. 28, 2020
16. *The tip of the iceberg: an unexpected turn in the xDedic story* (https://securelist.com/blog/research/75120/the-tip-of-the-iceberg-an-unexpected-turn-in-the-xdedic-story/); Secure List; June 20, 2016
17. *ESET issues its Q4 2020 Threat Report recording a massive increase in RDP attack attempts since Q1* (https://www.eset.com/int/about/newsroom/press-releases/research/eset-issues-its-q4-2020-threat-report-recording-a-massive-increase-in-rdp-attack-attempts-since-q1-1/); ZDNet; Feburary 8, 2021
18. *Several privacy-busting bugs found in popular VPN services* (https://www.zdnet.com/article/more-privacy-busting-bugs-found-in-popular-vpn-services/); ZDNet; March 13, 2018
19. *Saudi Aramco Traces Data Leak to Attack on Supplier* (https://www.bankinfosecurity.com/saudi-aramco-says-supplier-leaked-company-data-a-17130); Bank Info Security; July 22, 2021
20. *Morgan Stanley reports data breach after vendor Accellion hack* (https://www.bleepingcomputer.com/news/security/morgan-stanley-reports-data-breach-after-vendor-accellion-hack/); IT News; July 8, 2021
21. *Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware* (https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/); Block & Files; July 4, 2021
22. *Data Breaches Caused By Third Parties* (https://normshield.com/data-breaches-caused-by-third-parties/); NormShield
23. *Cloud computing trends for 2019* (http://www2.computerworld.co.nz/article/651173/cloud-computing-trends-2019/); Computer World; Jan. 2 2019
24. *Why Enterprises Are Accelerating Cloud Adoption* (https://www.forbes.com/sites/forbestechcouncil/2020/07/17/why-enterprises-are-accelerating-cloud-adoption/#2a11a3bdf498); Forbes; July 17, 2020
25. *Lock away your AWS account root user access keys* (http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials); AWS
26. *Cloud Adoption in 2020* (https://www.oreilly.com/radar/cloud-adoption-in-2020/); O'Reilly; May 19, 2020
27. *Zero Trust Security for the Workforce* (https://duo.com/use-cases/industry-solutions/zero-trust-security); Duo Security
28. *Multi-Factor Authentication from Duo* (https://duo.com/product/multi-factor-authentication-mfa); Duo Security
29. *By-the-Minute Security Reporting* (https://duo.com/solutions/features/reporting-and-alerts/security-logs); Duo Security
30. *Give Every User the Right Access* (https://duo.com/solutions/features/policy-and-controls/geolocation); Duo Security
31. *Duo Trust Monitor - Preview* (https://duo.com/docs/trust-monitor); Duo Security
32. *Simple Secure Single Sign-On* (https://duo.com/product/single-sign-on-sso); Duo Security
33. *Close Security Gaps* (https://duo.com/product/trusted-devices/self-remediation); Duo Security
34. *Security Starts With Transparency* (https://duo.com/product/trusted-devices/device-access-policies/trusted-endpoints); Duo Security
35. *Secure Authentication With the Duo Mobile App* (https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile); Duo Security
36. *Duo Device Health Application* (https://duo.com/docs/device-health); Duo Security
37. *Remote Access Integrations* (https://duo.com/solutions/features/supported-applications); Duo Security
38. *Protect Your VPN With Duo* (https://duo.com/solutions/features/supported-applications/secure-vpn); Duo Security
39. *Streamlined Login for Any and Every Application* (https://duo.com/solutions/features/supported-applications/cloud-services); Duo Security
40. *Single Sign-On (SSO) Integrations* (https://duo.com/solutions/features/supported-applications/web-apps); Duo Security
41. *Strong Endpoint Security* (https://duo.com/solutions/features/policy-and-controls); Duo Security
42. *Security 1-2-3* (https://duo.com/security-123); Duo Security
43. *How hackers are exploiting the coronavirus—and how to protect yourself* (https://fortune.com/2020/03/18/hackers-coronavirus-cybersecurity/); Fortune; March 17, 2020
44. *AWS Identity and Access Management User Guide* (http://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#delegate-using-roles); AWS

About Duo Security

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of Cisco Secure's Zero Trust offering, the most comprehensive approach to securing access for any user, from any device, to any IT application or environment. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.

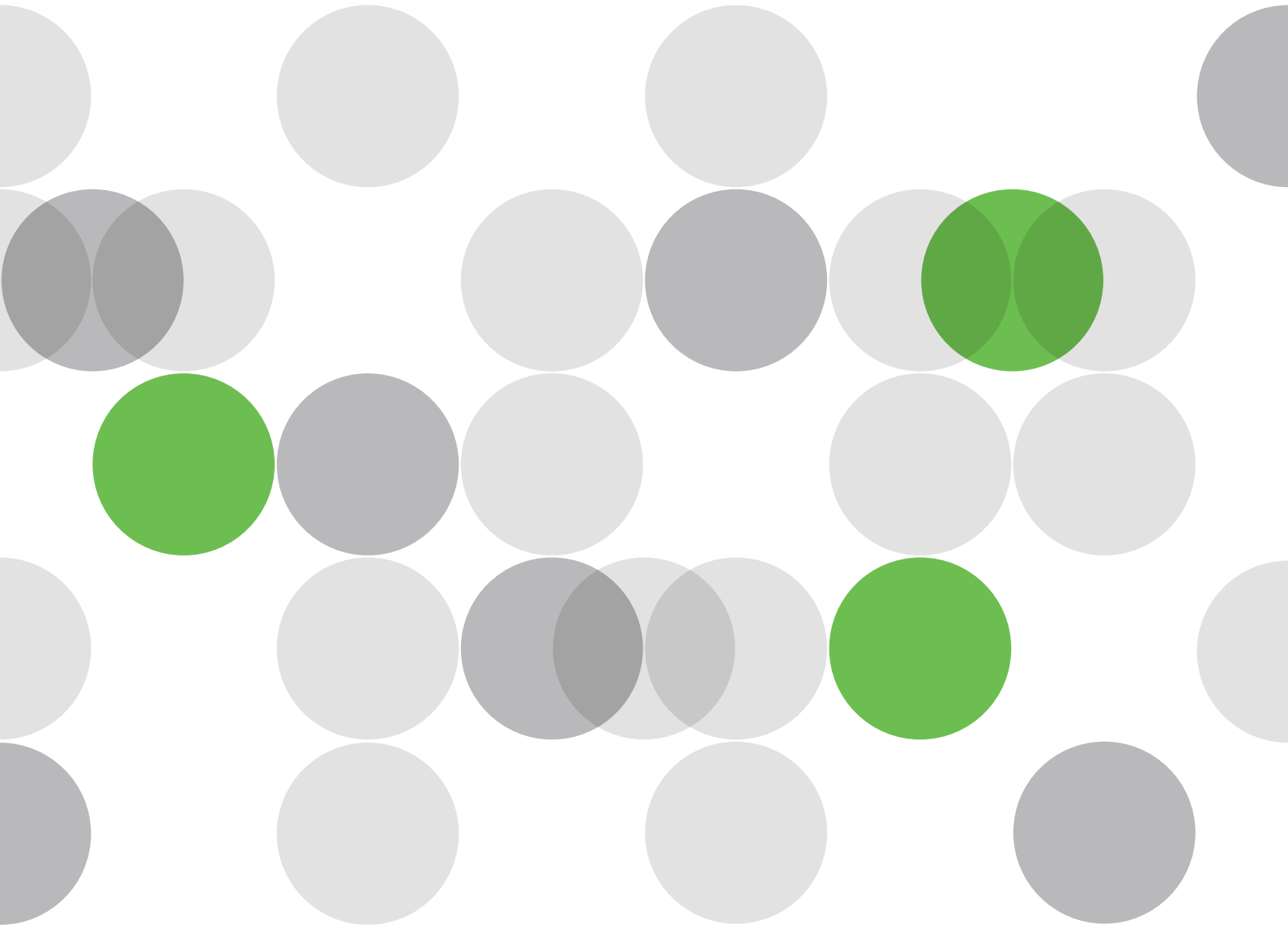
Contact Duo

We'd love to hear from you!
Tweet to us at **@duosec**
Or **send us a message**
Give us a ring. You can find our business phone numbers on this page: **https://duo.com/about/contact**

More Resources

Want to learn more? Check out our other ebooks, guides, reports, videos, infographics and more at **duo.com/resources**.

Try it for free at **duo.com**



The bridge to possible