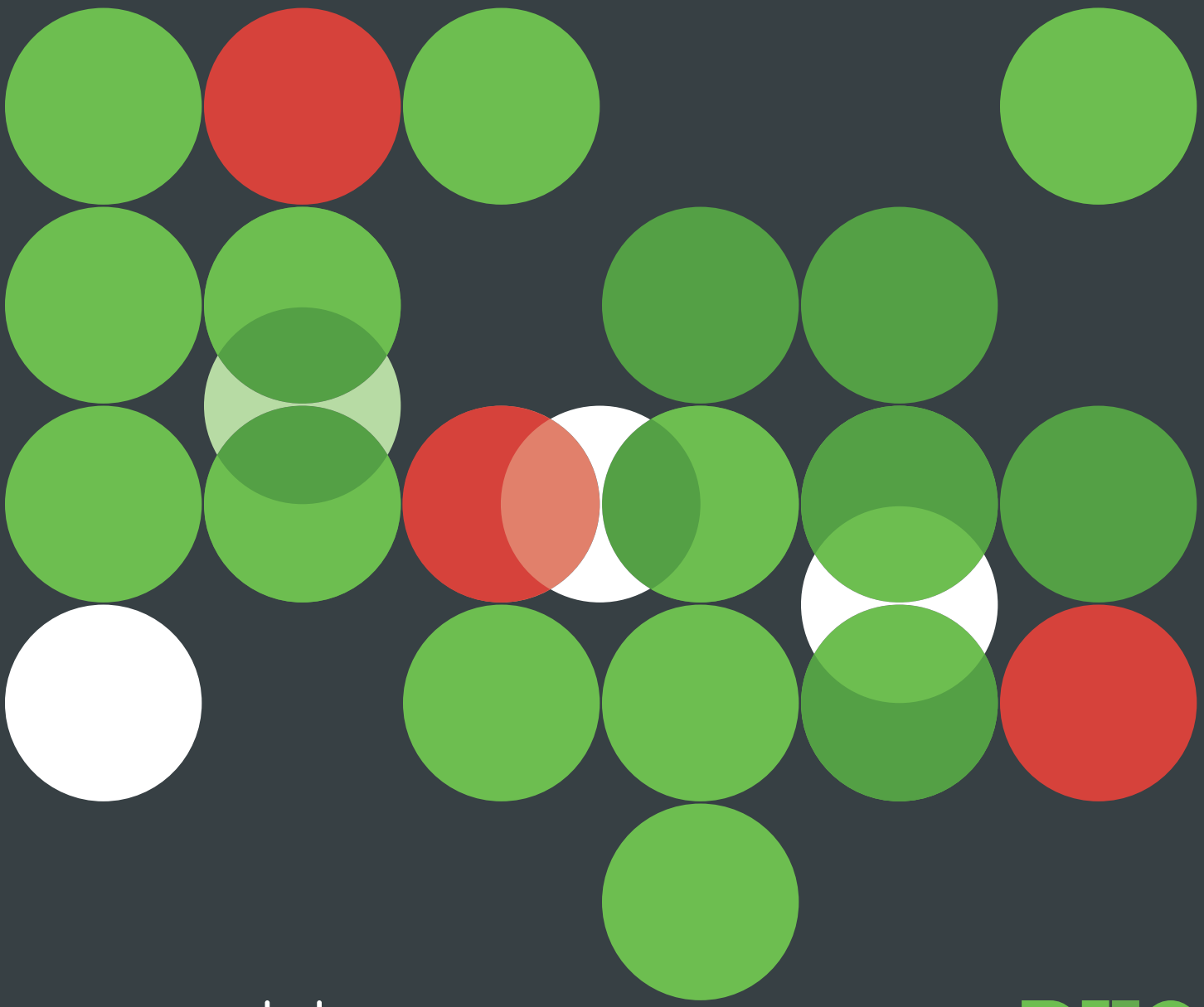
The Essential Guide to

Securing Remote Access

Ensuring User, Device and Application Trust



Duo Security is now part of Cisco.

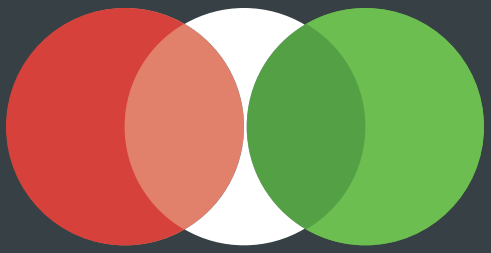
Contents

Author: Thu T. Pham

Designer: Chelsea Lewis

Producer: Peter Baker

Version 2.1



Navigating the New IT Model

While some say it's inevitable, it may just be that new threats and our new IT model requires an entirely different security approach to prevent breaches.

The new IT model brings with it a greater attack surface, comprised by employees that use their own devices for work, while working remotely. The proliferation of cloud applications for nearly every business need has also contributed to increased technical complexity.

These days, attackers can expose many different vulnerabilities in multiple vectors — in a single attack. Traditional security is designed to address separate, siloed attacks, making these solutions ineffective against modern threats.

With this new threat model, we need to shift focus to securing users, devices and apps holistically; with one solution to manage your access security instead of multiple, disparate security solutions.

These new threats center on gaining remote access to your apps and data — whether it's with stolen passwords or exploited known vulnerabilities targeting your users, their out-of-date devices, cloud applications and remote access software.

This guide will cover the different threats to each area with real-world examples, including exploits that affect remote access software and storage, and provide solutions and security best practice recommendations to help your organization protect against a data breach.

The Threats of Remote Access

How are attackers targeting users, devices and applications to gain remote access? Learn about the specific threats in our analysis of each one.

Targeting Users Remotely

The most difficult aspect to secure and control – the human element, continues to remain so, and online criminals know it. It's a low-tech, easy yet effective way to get access to apps and remain undetected by logging in as a legitimate user.

The *2016 Verizon Data Breach Investigations Report (DBIR)* found that 63 percent of data breaches involved weak, default or stolen passwords.[1] Stolen credentials was the top threat action type, followed by malware, phishing and keyloggers.

Phishing Campaigns

By carefully crafting emails that target their users, attackers may send emails with subject lines of urgency to get users to open them. Phishing emails typically include a link that may redirect users to a malicious site that downloads malware on their devices, or link to a spoofed website with a login form to steal user credentials.

And the threat is only increasing – 85 percent of respondents in Wombat Security's 2016 State of the Phish Report said they were the victim of a phishing attack in 2015 (a 13 percent increase from 2014).[2]

While these campaigns span industries, one recent example involved lawyers, high-value targets for online criminals, as they have troves of confidential client, business transaction and case information. Attackers sent phishing emails to lawyers' email addresses found on state bar websites, claiming they had unpaid bar dues and discipline complaints, some stating "Past Due Invoice" in their subject lines.[3]

They looked real, as they were signed by presidents of state bar associations, but they served up links to download malicious software. In Florida, the emails included ransomware, variants of Cryptolocker – a software that encrypts files on a Windows machine, requiring that a ransom is paid before decrypting them.

Phishing Campaigns

(cont.)

Phishing led to a breach of 80 million customer records

The FBI reports a $3.1 billion loss due to email scams.

Post-Breach Opportunities for Phishing

In January 2015, one of the largest health insurers, Anthem reported a data breach that affected the personal information of up to **80 million** customers.[4]

An investigation surmised that a phishing campaign may have given the attackers the credentials of five different Anthem employees. An Anthem computer system administrator realized that an unauthorized individual was using his security credentials to log into the system to steal customer data.

But the phishing didn't stop there — less than a week after the data breach was reported to customers and the media, reports of phishing messages that appeared to be from Anthem were sent to current and former customers. The emails offered credit monitoring to users, urging them to click on a link and submit personal information.

However, Anthem didn't send those messages – they were the work of scam artists attempting to steal personal data, leveraging the timeliness of the breach to gain user trust.

Phishing for Cold Hard Cash

Business email compromise (BEC) or CEO fraud are pseudonyms for what is essentially a singular phishing email attack. This refers to a more targeted attack against foreign suppliers or any business that performs wire transfer payments, instead of a more general, mass email.

In one method, a criminal may send an email to a specific employee, pretending to be their boss and asking them to conduct a wire transfer. Other attack paths include compromising employee email accounts to send transfer requests to their bankers, financial advisors, suppliers, etc.

A traditional phishing scam may involve an attacker interacting with the bank directly, but a BEC scam involves tricking the victim into do it for them, to avoid detection.

These scams work — very well. In August 2015, the networking firm Ubiquiti Networks, Inc. lost $46.7 million due to employee impersonation and fraudulent money transfer requests to overseas accounts held by third parties.[5]

In June 2016, the FBI released a public service announcement about BEC. According to the PSA, since January 2015, there has been a 1,300% increase in losses due to the scam, with a combined dollar loss of **3.1 billion** across domestic and international victims.[6]

Brute-Force Attacks

If attackers can't steal a password, they can use dictionary attacks and automated tools to guess weak passwords. In February, nearly 21 million accounts on the Chinese Alibaba e-commerce site Taobao (similar to eBay) were compromised due to password reuse and brute-force.[7]

The criminals gained unauthorized access into millions of Taobao accounts by acquiring a database of 100 million credentials, as well as brute-forcing accounts with weak passwords, getting access to accounts to commit fraud.

Password-Stealing Malware

The latest U.K. National Crime Agency (NCA) report has found that computer-related crime has surpassed all other crime types for the first time - and partly due to the use and sale of financial Trojan malware.[8]

A few types of these Trojans named Dridex and Neverquest include a keylogger component in order 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.

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, working from home and while traveling.

The problem is — IT departments can't manage these unknown devices. With no insight into how secure or up to date they are, these devices can bring with them the risk for malware or exploitation — providing yet another entry point into an organization's environment.

Exploiting Out-of-Date Devices

How often do your users update their smartphones on time? 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).

In Duo's 2016 Trusted Access Report, we analyzed our dataset of two million devices to find out how many were running out-of-date software.

We found that 60 percent of enterprise devices were running out-of-date versions of Flash.

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.

Within two weeks of Adobe releasing an emergency patch to address a critical vulnerability (CVE-2016-1019) in Flash Player, two exploit kits, including Magnitude and Nuclear were exploiting it in early April.[9] And just a few short months later, another critical Flash vulnerability (CVE-2016-4117) popped up just one week later in exploit kits Angler, Magnitude and Neutrino, affecting version 21.0.0.226 and earlier.[10]

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 of Flash they're running before serving up a Flash exploit that installs malware on their machine, which may give them control over their system or the ability to steal data.

Spreading Malware

If your users are logging into your company's applications with their outdated devices, there's a chance they could also be unwittingly spreading malware to your network.

As mentioned earlier, many forms of Trojans contain a keylogger component that records your keystrokes, meaning any username or password you enter, or data typed into your browser can be recorded and sent to an attacker's command & control servers.

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

How Attackers Exploit Out-of-Date Devices

1. 

An emergency update for Adobe Flash Player is released

2. 

Attacker recodes an exploit kit to include the new Flash vulnerability

3. 

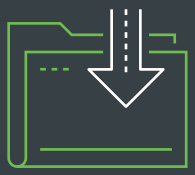
Out-of-date user opens a phishing email, clicks on a malicious link

4. 

Drive-by download launches an attacker's exploit kit

5. 

Exploit kit checks user's device for outdated version of Flash

6. 

Exploits vulnerability to download malware on device

7. 

Malware contains a keylogger that tracks username/password

8. 

Sends that and other sensitive data (financial) to a command & control server

9. 

Attack success

Remote Access Goes Both Ways

Many organizations have contractors or remote employees that must use remote access software in order to gain access to the applications or work resources they need to do their jobs. However, many attackers also take advantage of the convenient access to compromise your environment.

RDP Security Threats

Remote Desktop Protocol (RDP) is a Microsoft 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.

In June, the Microsoft Access databases of three different healthcare organizations across the country were compromised by a hacker that exploited a RDP implementation vulnerability. The hacker held some clinical and medical data for ransom, while putting up over 600,000 records for sale on the dark web.[11]

Unfortunately, companies 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 May, attackers located Internet-facing RDP servers of corporate networks storing payment card information, then brute-forced the passwords in order to spread ransomware.

Hackers also harvested and sold as many as 250,000 RDP server credentials in an underground marketplace, xDedic. These credentials gave buyers access to all of the data on the servers and the ability to launch future attacks using the servers.[12]

Virtual Private Network Threats

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

Unfortunately, VPNs are software, and like any other kind of software, they sometimes have bugs and do leak private user information. In one case, several VPN providers were leaking IP and DNS addresses that could allow an attacker to identify users and locations.[13]

Yet another vulnerability would allow an attacker to hijack web traffic through a VPN to a proxy server, which could give them information about a user's browsing activity. This could occur if an attacker convinced a user to click on a malicious link. While VPNs do provide overall greater security, they are not infallible when it comes to potential security risks.

The Risks of Third-Party Reliance

Web applications can be accessed via your browser, and include services such as email, data storage, collaboration and productivity apps that require no local hardware or software installation to use. It makes it fast, easy and reliable for users to log into resources with just a browser and Internet connection. Plus, it's easy for remote contractors and third-party vendors to access your web apps with a set of credentials in order to do their jobs.

But it also offers a fast, easy and reliable way for online criminals to target access to these apps through third-party accounts to steal customer, employee, healthcare and other personal data. According to the Verizon 2016 DBIR, web application attacks rose rapidly from 7 percent in 2015 to 40 percent in 2016 – they are also the single biggest source of data loss.[14]

Last year, the breach of a contractor of OPM (Office of Personnel Management) affected 21.5 million personnel records, as well as highly sensitive background investigation documents. An attacker compromised a set of the contractor's user credentials, getting remote access to OPM's network.[15]

This is commonplace in most breaches – typically a hacker will steal the credentials of a contractor or smaller vendor in order to get access to a larger organization. While large companies may have the budget for better security, contractors often don't, making them an easy target of hackers.

Similarly, compromised credentials are often the cause for many retailer and franchisor data breaches of customer data. Attackers typically go after the point-of-sale (POS) vendors that provide POS systems for restaurants, hotels, and other retailers.

For example, the fast food franchise Wendy's reported that malware was installed on several locations nationwide through the use of compromised third-party vendor credentials.[16] The massive Target breach was also caused by an HVAC vendor's stolen credentials that gave an attacker access to Target's billing system, affecting more than 110 million consumers.[17]

Attackers can also exploit web application and system vulnerabilities to access, install malware and gain control over systems. More often than not, the vulnerabilities they exploit are known vulnerabilities that affect older applications and systems that haven't been updated or patched to the latest version. Updating all software to the latest version, applying all security patches and identifying out-of-date devices early is the best form of risk reduction and breach prevention.

The Cloud is Great – Until It's Not

One aspect of the cloud refers to virtual server space, also known as cloud computing or cloud hosting. **Amazon Web Services (AWS)** and Microsoft Azure are popular providers of scalable cloud computing services, and are used by many companies to host and support their critical operations, applications and data.

But there are security concerns with access to AWS accounts, as they can be compromised and used to host or send malware. Attackers can also get access to your billing information, cloud data and password controls if they steal your root account credentials. AWS recommends that you don't use root account credentials for everyday access.[18]

Many developers have also mistakenly embeded and uploaded their AWS keys along with their source code to Github. In 2014, ITNews.com reported that thousands of AWS secret keys were found on Github, uploaded by developers along with their code.[19] Anyone that found the keys could access and delete their entire environment. It can happen very quickly, since hackers run bots that scan Github for these keys automatically.[20]

A Holistic Approach to Securing Remote Access

Nowadays, securing against a remote attack requires ensuring the trust of your users and devices for every application they access, in order to protect against the risks associated with different attack methods, such as phishing, credential theft and vulnerability exploitation. Use a holistic security solution that can defend against an exploit against multiple vectors.

Trusted Access

Our approach to securing against new threats is called **Trusted Access** – verifying the identity of your users and the security health of their devices *before* they access the applications you want them to access.

Trusted Users

Ensuring the trust of your users whenever they attempt to access your applications remotely is the first step toward complete Trusted Access. This requires strong authentication controls.

Two-Factor Authentication

Two-factor authentication provides a second check after your user enters their username and password to verify their identity. Employ a cloud-based two-factor solution and use secure methods, like push notifications or a U2F device to complete authentication.

SMS-based two-factor authentication is no longer considered secure by the National Institute of Standards and Technology (NIST) standards, as SMS messages can be easily intercepted or redirected by remote attackers.[21]

Using an authentication app, users can log in with their primary credentials, and then their app will prompt them with a **push notification** to complete the secondary authentication by approving the request. This method is more difficult for attackers to intercept and offers a convenient way for users to log in by using their smartphone or other device.

U2F (Universal Second Factor) is a strong industry standard for two-factor authentication created by the FIDO (Fast IDentity Online) Alliance. It requires the use of a tamper-resistant USB device that allows users to log in by tapping the physical device plugged into their laptop.

Contextual Authentication Controls

Use an authentication solution that also gives you **detailed data and logs** 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 should be able to create custom authentication controls to restrict access based on your organization's needs – for example, set up a **geolocation policy** based on user location parameters and block all users from countries you don't do business in.

Trusted Devices

Ensure your users' devices meet your organization's security standards by using an endpoint solution that collects **detailed data** about the security health of every device used to log into your applications.

It only takes one device running out-of-date software to expose your company to potential malware infection or a compromise, resulting in data loss.

Endpoint Visibility

To avoid the risks associated with known vulnerabilities, use an **endpoint visibility** solution to check every device for the latest software, including operating systems, browsers, and plugins like Flash and Java.

Check devices to ensure they have important security features enabled, like screen lock, fingerprint identification and a passcode to keep intruders out.

Device Access Controls

Administrators should use endpoint controls to **warn users** and **block any device** that doesn't meet your minimum security requirements, eliminating the risk of spreading malware and unauthorized access.

Admins can also use an endpoint solution that lets them notify users of outdated devices, and allows them to **update their own devices** before connecting to your apps. Making users active participants of updating their own devices can involve them in the security process and make the time-to-security much faster for your organization.

Every Application

Strong access controls and device security checks are only effective if they're applied to every application. Deploy these solutions and integrate them with:

VPNs	Juniper, Cisco and Palo Alto
Cloud apps	Microsoft Office 365, Salesforce, Google Apps, Amazon Web Services and Box
On-premises and web apps	Epic, SSH, UNIX, WordPress
Custom apps and services	Use APIs and client libraries like Python, .Net, Ruby and more

Finally, **create custom access policies and controls** 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

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

Simulated Phishing Attacks

To protect against user-targeted attacks, try running a **simulated phishing email campaign** internally. Use the results to educate your users to identify a potential phishing email, and establish a process for reporting it.

Eliminate Unnecessary Software

Uninstall any unused software on your devices, including potentially unsafe third-party plugins on your browsers. This reduces the attack surface and minimizes the chance of a compromise.

Timely Patch Management

The window of time between a new software version release and updating all of your users' devices and your company's systems is when an attacker can exploit any known vulnerabilities against the old version. Watch for any emergency, out-of-cycle patches released by your software vendors (or better yet, use a reporting tool that tracks new security events for you).

Encourage Secure Devices

Educate and encourage users to choose more secure personal devices, such as the **Google Nexus** for Android users, which receives monthly security updates. Other devices rely on their manufacturers to update for security, which is not always reliable or timely.

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 two-factor authentication as well.

Delegate by Creating Roles

Instead of sharing your cloud credentials, create Identity and Access Management (IAM) roles with specific permissions for separate users that need access to your AWS account resources.[22]

References

[1] *Verizon DBIR: Over Half Of Data Breaches Exploited Legitimate Passwords In 2015*; DarkReading.com; April 26, 2016

[2] *2016 State of the Phish Report*; WombatSecurity.com; 2016

[3] *Email Scam Targets Lawyers With Fake Disciplinary Warnings, Bar Announcements*; ABAJournal.com, June 23, 2016

[4] *Anthem Data Breach: Leaked Information, Phishing Attacks and Security Best Practices*; TrendMicro.com; February 22, 2015

[5] *Business E-Mail Compromise: The 3.1 Billion Dollar Email Scam*; ic3.gov; June 14, 2016

[6] *Tech Firm Ubiquiti Suffers $46M Cyberheist*; KrebsonSecurity.com; August 7, 2015

[7] *Massive Brute-Force Attack on Alibaba Affects Millions*; Infosecurity-Magazine.com; February 8, 2016

[8] *U.K. NCA Cyber Crime Assessment 2016 Report*; NationalCrimeAgency.gov.uk; July 7, 2016

[9] *New Adobe Flash Player Exploit Used by Magnitude and Nuclear Exploit Kits*; Symantec.com; April 12, 2016

[10] *A Recently Patched Flash Player Exploit is Being Used in Widespread Attacks*; PCWorld.com; May 23, 2016

[11] *655,000 Healthcare Records Being Sold on Dark Web*; ThreatPost.com; June 28, 2016

[12] *The Tip of the Iceberg: An Unexpected Turn in the xDedic Story*; SecureList.com; June 20, 2016

[13] *Several Privacy-Busting Bugs Found in Popular VPN Services*; ZDNet.com; March 13, 2018

[14] *Verizon DBIR 2016: Web Application Attacks Are The #1 Source Of Data Breaches*; VerizonDigitalMedia.com; June 21, 2016

[15] *Contractor Breach Gave Hackers Keys to OPM Data*; FederalTimes.com; June 25, 2015

[16] *The Wendy's Company Reports Strong First-Quarter 2016 Results*; Wendys.com; May 11, 2016

[17] *Email Attack on Vendor Set Up Breach at Target*; KrebsonSecurity.com; February 12, 2014

[18] *IAM Best Practices*; AWS Documentation – Amazon.com; 2016

[19] *AWS Urges Developers to Scrub Github of Secret Keys*; ITNews.com; March 24, 2014

[20] *Attackers Scrape GitHub For Cloud Service Credentials*, Hijack Account To Mine Virtual Currency; Forbes.com; January 14, 2014

[21] *DRAFT NIST Special Publication 800-63B: Digital Authentication Guideline*; NIST.gov; 2016

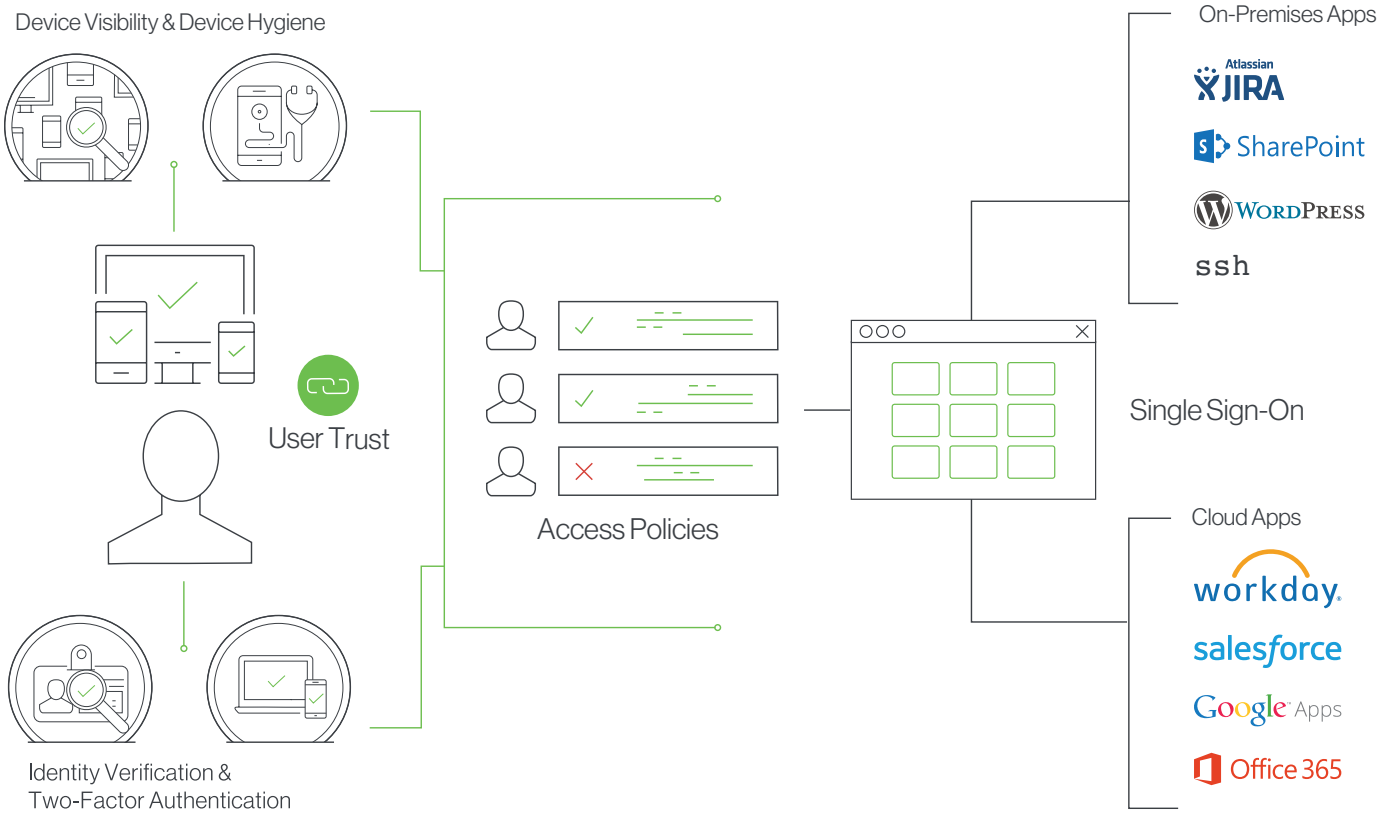
Our mission is to protect your mission.

The Trusted Access Company

Beyond

Trusted Users. Trusted Devices. Every Application.

Duo Beyond has made the BeyondCorp journey possible for companies such as **KAYAK**, allowing them to tighten their security controls both inside and outside the perimeter, and saving them months or years of effort piecing together their own solutions.



ABOUT DUO SECURITY

Duo Security helps defend organizations against data breaches by making security easy and effective. Duo Beyond enables organizations to provide trusted access to all of their critical applications, for any user, from anywhere, and with any device. The company is a trusted partner to more than 10,000 customers globally, including Dresser-Rand, Etsy, Facebook, K-Swiss, Random House, Yelp, Zillow, Paramount Pictures, and more. Founded in Michigan, Duo has offices in Ann Arbor and Detroit, as well as growing hubs in Austin, Texas; San Mateo, California; and London, UK. Visit **duo.com** to find out more.