Brought to you by:

CISCO
DUO

Identity Security

for dummies
A Wiley Brand

Identify identity issues

Deny access to attackers

Adopt next-gen authentication

Cisco Duo
Special Edition

Lawrence Miller

About Cisco Duo

Founded in 2010 by Dug Song and Jon Oberheide, Duo Security began as a secure access company focused on multi-factor authentication (MFA) that was dedicated to being kinder than necessary and building for the future. We expanded beyond our Ann Arbor, Michigan, beginnings in 2015 to meet the increased, international needs of over 2,000 customers. No matter how much we grew, we never stopped placing customer experience and customer trust first, expanding our data security offerings beyond MFA with tools that were easy, effective, and enduring.

Cisco acquired Duo Security in 2018, helping us bring industry-leading identity security to over 40,000 customers globally as part of Cisco's growing security portfolio.

At Duo, we put people first — whether that's enabling our customers' users to work securely from anywhere or supporting the people who work every day to make our products effective, user-focused, and intuitive. We don't thrive on fear, uncertainty, and doubt; we build identity security defenses you can trust.

www.duo.com

Identity Security

Cisco Duo Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Identity Security For Dummies®, Cisco Duo Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-30088-4 (pbk); ISBN 978-1-394-30089-1 (ebk); ISBN 978-1-394-30090-7 (ePub)

Publisher's Acknowledgments

Development Editor:
Rachael Chilvers

Project Editor:
Saikarthick Kumarasamy

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager:
Jeremith Coward

Introduction

In today's digital age, modern organizations' security needs have evolved far beyond firewalls, virtual private networks (VPNs), and antivirus software. With ongoing trends that include digital transformation initiatives, cloud adoption, hybrid work environments, and increased business interconnectivity, identity has emerged as the new perimeter.

As threat actors increasingly target identities, organizations must stay ahead by implementing a comprehensive identity security program. The right approach to identity security can enhance your organization's security posture, improve the employee experience, and deliver significant business benefits. In this book, you'll learn how to make identity security a cornerstone of your organization's defense strategy.

About This Book

Identity Security For Dummies, Cisco Duo Special Edition, consists of five chapters that explore the following:

- What identity security is and why it matters (Chapter 1)
- How identity breaches happen (Chapter 2)
- Current challenges with identity security (Chapter 3)
- Next-generation identity and authentication (Chapter 4)
- The business benefits of identity security (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but we assume a few things nonetheless!

Mainly, we assume that you are an IT leader such as a chief information officer (CIO), VP of infrastructure, or IT director. As such, we assume that you are somewhat technical and have at least a basic understanding of identity, networking, and security concepts and fundamentals.

If any of these assumptions describe you, then this is the book for you. If none of these assumptions describe you, keep reading anyway. It's a great book and after reading it, you'll be able to identify as someone who knows a great deal about identity!

Icons Used in This Book

Throughout this book, we occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin.

TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.

TIP

Tips are appreciated, but never expected — and we sure hope you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice.

Beyond the Book

There's only so much we can cover in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" visit the Cisco Duo website at `https://duo.com/`.

IN THIS CHAPTER

- Defining the new perimeter
- Closing the gap between identity and access management and identity security

Chapter 1
Getting Started: Identity 101

Identity is critical in our modern era of remote work and software-as-a-service (SaaS) applications: You can't protect your data and applications if you don't know who has access to them. Poor identity security can practically open the door for cybercriminals and make companies more vulnerable to potentially devastating cyberattacks.

In this chapter, we explain the basics of identity security, why it matters, and what you need to build an effective identity security strategy for your organization.

Identity is the New Perimeter

In the not-too-distant past, applications ran in on-premises datacenters or server rooms and were accessed over a company network by employees working in an office. The traditional "castle-and-moat" approach to network security used firewalls and other security technologies to create a boundary, or perimeter, around the "trusted" company network and the "untrusted" network.

All of this changed with the rise of cloud-hosted applications, remote and hybrid work, and distributed and extended workforces (including contractors, partners, vendors, and other third parties). Today, applications can run anywhere — on-premises or in the cloud — and users can access them from anywhere on any device. Thus, the notion of "trusted" and "untrusted" networks has all but disappeared. Instead, trust — and access — depends on who you are (that is, your identity) rather than your IP address.

TECHNICAL STUFF

An *identity* includes attributes such as user (or account) name, password (or passphrase or secret key), roles, access privileges, and historical context. This information identifies an individual or entity (such as a service, device, or application) in an organization's systems and networks.

Identity security protects human (and machine) identities to ensure that they are who they say they are (*authentication*) and that they only have access to what they are allowed to access (*authorization*). Effective identity security ensures that every user, device, service, and application that accesses an organization's resources is properly authenticated and authorized based on their identity. If a threat actor gains access to a user's credentials or a device is compromised, their access should be restricted (or better, denied entirely) based on least-privilege account permissions and defined security policies.

WARNING

Rather than developing exploits for system or application vulnerabilities, attackers can simply log in with stolen credentials. According to the 2024 Verizon Business Data Breach Investigations Report, 68 percent of breaches are the result of credential theft (that is, the "human element") from vectors including social engineering techniques (such as phishing, smishing, business email compromise, and pretexting) and brute-force dictionary attacks.

ENTERPRISE SOFTWARE COMPANY MIGRATING TO THE MICROSOFT CLOUD + DUO

An enterprise company that helps clients build out software applications and processes migrated the Microsoft cloud and chose Duo to secure its rapidly changing IT infrastructure.

The Challenge

A large company assisting clients in developing enterprise software applications and processes needed to secure its own rapidly changing IT infrastructure. After a number of acquisitions, the company found that different teams were using different software deployed in different locations, often serving the same purpose.

For example, the company inherited Microsoft 365 through one of its acquisitions but had not yet deployed cloud-based email to most of its original employee base, who were still using on-premises Exchange. As a result, a small fraction of the company was now using an entirely different email solution than everyone else.

This was also the case with its Active Directory deployment. The company had two primary Active Directory databases. One was hosted locally on its own premises and served its internal employee base. The other, which was used for partners and contractors, was hosted in the Microsoft Azure cloud. Hosting the latter in the public cloud made operational sense because of how scalable and elastic the Azure infrastructure is.

However, this made security operations difficult for a resource-strapped IT team, as it had to secure a hybrid public/private cloud environment while keeping the end user experience simple and intuitive for everyone. "We wanted to find a single solution that could easily secure access to any application regardless of where it was hosted. This turned out to be surprisingly more difficult than we originally thought," said the Manager of Information Services.

The Solution

The applications team at the company was already using Duo to protect some of its own engineering resources. Upon hearing that the

(continued)

(continued)

entire company was evaluating a two-factor authentication solution, they were quick to recommend Duo for its ease of use and reliability.

“We needed a security solution that every employee could use. As a forward-looking IT organization, we wanted whichever solution we picked to be entirely smartphone-based. Duo Push is great for our end-users because it’s quick, it’s easy, and most importantly, our employees don’t feel like they’re being overburdened.”

The company is quickly expanding its Duo deployment across its entire application infrastructure, for both on-premises and cloud applications. In addition to protecting its Microsoft environment, the company also uses Duo to secure remote access to its virtual private network (VPN) gateway and the internal network.

The manager concludes, “Seeing the support that Duo has for various Microsoft applications has been great for us. It helps us sleep better at night knowing that as we go through some of these public cloud migrations (Exchange and Microsoft 365, on-premises and Microsoft Entra ID), Duo can stay right there with us without any complications.”

Identity Security Requires More Than Just IAM

A significant gap often exists between an organization’s identity-responsible teams and security teams, which limits the effectiveness of its identity security program. Although identity and security are closely related, these teams often have different goals, priorities, and reporting structures. For example, many identity and access management (IAM) tools are implemented and managed by IT or identity teams, which can create significant blind spots for the organization’s security teams.

REMEMBER

According to the Identity Defined Security Alliance, only 53 percent of security teams have ownership of workforce IAM.

To close this gap, identity teams need to work closely with security team counterparts to manage the overall security posture of the organization, while security teams need to understand the importance of IAM. Together, identity and security teams can implement a successful identity security program based on the following four pillars and best practices:

- **Identify.** Build a centralized user and device inventory including guest access and non-human identities (NHIs), such as shared mailboxes, service accounts, and network devices.
- **Protect.** Implement comprehensive processes for identity lifecycle management (joiners, movers, and leavers), entitlements, and access reviews, as well as robust security controls such as single sign-on (SSO), strong multi-factor authentication (MFA), and access policies.
- **Detect.** Collect, store, and ingest logs from all appropriate sources into a security information and event management (SIEM) platform for correlation of security alerts, and develop an effective threat identification capability using different methods based on indicators of compromise (IOCs), anomalous activity, and tactics, techniques, and procedures (TTPs).
- **Respond.** Create an incident response plan for identity security that addresses key stakeholders, escalation actions, policies and exclusions, external communications, data sharing, legal and regulatory requirements, and operational resilience.

INTRODUCING DUO PASSPORT

To implement a truly secure, seamless user sign-in experience and lower the administrative burden for IT, you need to enforce user authentication, device verification, and risk-based policies in a manner that doesn't frustrate the user.

Duo Passport is a cloud-based identity security tool that verifies the user's identity and continually evaluates trust based on adaptive and risk-based policies. Fewer interruptions after authenticating reduces frustration and enables a better overall user experience. Key benefits include:

- **Improve workforce productivity.** End-users experience one authentication at the beginning of the workday, while device-bound private keys enable frictionless access across apps,

(continued)

(continued)

browsers, operating systems, and thick-clients like VPNs. Enabling Passport empowers your workforce to be more productive with fewer interruptions.

- **Strengthen identity security posture.** In suspicious situations, Passport will “step up” and require an authentication to re-establish trust or block the user entirely. Duo access decisions are enriched with identity data from Cisco Identity Intelligence, and layers on top of your existing policies. Reduce security gaps with strong authentication and risk-based access controls.
- **Reduce total cost of ownership (TCO).** Passport brings together Duo’s best-in-class tools including multi-factor authentication, passwordless, single sign-on, risk-based authentication (RBA), and device trust capabilities, helping consolidate identity security and maximize the value you get with Duo.

IN THIS CHAPTER

- **Goin' phishin' and other social engineering attacks**
- **Factoring in multi-factor authentication**

Chapter 2 Understanding Identity Breaches

An identity breach isn't the end game for cybercriminals. It's simply their opening move to gain access to the crown jewels — your business-critical applications and sensitive data. In this chapter, you learn about some of the techniques that attackers use to steal account credentials and bypass multi-factor authentication (MFA).

Hacking the Human

IT and security professionals often joke that "users are the weakest link in security." If you change the word "users" to "people" — including system administrators, application developers and, yes, even security folks — then you aren't far from the truth.

It isn't that people are necessarily lazy or don't care, it's just that we're all human. So, if you've ever wondered how anyone could possibly fall for a seemingly obvious phishing email scam, remember that generally speaking, it's human nature for us to want to trust others.

Fortunately, security awareness programs focus a lot of attention on how to spot phishing emails, so the click rate (that is, the success rate) for these types of attacks is decreasing. Not to mention, great strides have been made in email security technology to prevent the phish from even making it to your inbox.

However, cybercriminals are constantly evolving their tactics — for example, by using artificial intelligence (AI) to up their grammar game or craft more convincing pretexting scenarios for a phishing campaign — and they only have to get it right once. Users have to be vigilant always.

Beyond phishing, cybercriminals have a full arsenal of social engineering techniques they can use to steal user credentials, including:

- **Spearphishing:** This is a targeted phishing campaign that typically goes after company executives, but can also be directed at specific companies or individuals.
- **Smishing:** This is basically phishing with a short message service (SMS) text sent to a mobile phone, and many users mistakenly believe that text messages are somehow more secure than email — but they aren't.
- **Vishing:** Another spinoff on phishing, vishing involves calling a potential victim and using the powers of persuasion to convince someone to reveal their account credentials, perhaps by masquerading as a help desk tech or as a distressed user calling IT for a quick password reset.
- **Dumpster diving:** No, we're not talking about literally going through someone's garbage — although that does still happen. The modern equivalent of dumpster diving is collecting information about potential victims from publicly available sources such as a company website, social media, or job site (a resume can be a treasure trove of personal information).

WARNING

Social engineering techniques aside, cybercriminals can still go "old school" to steal credentials with more technical hacks such as stealing passwords stored in browsers, installing malware such as keystroke loggers and remote access trojans, session hijacking, and good old-fashioned brute force dictionary attacks — or simply purchase credentials on the dark web that someone else has stolen.

Once an attacker has stolen a user's credentials, they can log in to the network and get familiar with their new home, create a few more accounts (just in case the user changes their password), install some malware here and there, escalate their account privileges, and do their worst — perhaps steal some sensitive information, encrypt a few files, and/or crash the entire network.

MFA requires users to perform another step to successfully log in to your applications and networks — and an attacker has to do a bit more work.

Targeting Multi-Factor Authentication (MFA)

MFA, including two-factor authentication (2FA), is one of the simplest and most effective ways to make sure your users really are who they say they are. According to `research by Microsoft`, 99.9 percent of compromised Azure Active Directory accounts do not use MFA and 99.2 percent of account compromise attacks can be blocked by MFA. Yet despite the effectiveness of MFA, according to a `2024 JumpCloud Survey`, only 87 percent of large organizations use MFA, while only 78 percent of medium-sized and 34 percent of small companies use MFA.

REMEMBER

MFA requires some combination of *something you know* (such as a username and password), *something you have* (such as a mobile phone or authenticator app), and *something you are* (a biometric feature, such as a fingerprint or facial pattern). Each of these factors increases the difficulty in compromising an account.

The first, and most common factor — something you know — is of course the weakest authentication factor and the easiest to attack, as discussed in the previous section.

The second factor, something you have, is a bit more difficult, but not impossible for an attacker to defeat, typically using one of the following techniques:

- **MFA interception:** The attacker steals a one-time code that's sent through an SMS text or email and proceeds to log in with the user's credentials and MFA code.

- **Device registration:** The attacker uses stolen credentials to register a new, fraudulent MFA device to the account to gain persistent access.
- **MFA fatigue attack:** The attacker uses a legitimate user's stolen credentials to generate repeated MFA push requests until the frustrated user either accepts a request to stop the flood of MFA prompts or accidentally grants access to the attacker.
- **Sim-jacking:** In a subscriber identity module (SIM) hijacking (sim-jacking) attack, special spyware-like malware is sent to a mobile phone that allows the attacker to take control of the phone.
- **Adversary-in-the-middle (AITM):** The attacker steals the session cookies of an authenticated user to gain access to an already authenticated session, thus bypassing MFA.

TIP

The third factor, something you are, is practically impossible for an attacker to steal — unless they're Ethan Hunt. And good luck getting the *Mission Impossible* theme song out of your head now!

LEADING JOB SITE DEPLOYS DUO TO 400 USERS IN LESS THAN FOUR HOURS

With over 100 million unique visitors every month, a leading global job site drives millions of targeted applicants to jobs in more than 50 countries and is a source of high-quality candidates for thousands of companies.

The Challenge

With an expanding number of employees and a growing public presence, security was becoming a pivotal issue for this company. Every time they opened the pages of the Wall Street Journal, there was another story about a major security breach. So the VP of Operations made the decision to "lock down the access points into the company." They wanted to be known as the site where millions of people found a great job, not the site where millions of people's private information was stolen.

Stakeholders were in agreement that their system needed to be protected with security stronger than passwords. So they began looking at two-factor authentication (2FA) solutions, including Google Authenticator and traditional token-based 2FA from RSA.

The Solution

Duo was on the radar of the person who leads their security group. With strong authentication, a user-friendly interface, an affordable price structure, and no long-term commitments, Duo moved to the top of their list.

After initial testing with a couple of users, they called Duo to set up an account for 400 engineers and others who used the virtual private network (VPN) regularly. Using Duo's user self-enrollment feature, they were able to progress from testing to integration, then to full deployment to 400 users in under four hours. The deployment went so smoothly that they immediately began rolling out MFA to everyone in the company — more than 800 people.

After deployment, things were quiet on the help desk — so quiet that at first the IT team thought something might be wrong with the system. As the VP of Operations tells it: "I was expecting more calls when we deployed Duo. And when no calls came in, I thought, 'Nobody's using it, and they're so annoyed and they're not calling in.' But people were logging in, they were using it and it wasn't a problem. With Duo, everything just works."

Although MFA isn't necessarily foolproof, there are many things an organization can do to further enhance its security. For starters, SMS-, phone-, and email-based MFA are generally weak options — better than a username and password alone, but relatively easy for an attacker to compromise.

TIP

Token- and push-based MFA — including hardware and software tokens, as well as time-based one-time passwords (TOTP) and number-matching push notifications via a mobile authenticator app — offer more robust authentication security and provide an ideal balance between user experience and security.

Finally, WebAuthn-based, also known as phishing-resistant MFA, provides the most secure MFA method currently available. These methods use a roaming authenticator, such as a YubiKey or Fast Identity Online 2 (FIDO2) key that must be plugged into the user's device, or a platform authenticator that uses biometrics integrated into device hardware and operating systems, such as Windows Hello or iOS Face ID.

SECURE ACCESS FROM A WIDE RANGE OF DEVICES WITH THE DUO MOBILE APP

The Duo Mobile app supports multiple authentication controls — from push notifications to biometrics and passcodes — while maintaining a consistent, intuitive user login experience.

With Duo's single-tap, user-friendly interface, users can quickly verify their identity by approving push notifications before accessing applications. After logging in with a username and password (or, in the case of a passwordless authentication, just a username), a notification from Duo arrives seconds later on a second device, and they can simply tap 'Approve' to securely access their application. It's just as easy to deny an unfamiliar login attempt, so users can stop fraudulent attempts to access company data.

Duo Mobile can also generate time-based one-time (TOTP) passcodes that users can type into their login prompt to complete the two-factor authentication process, helpful for securing offline authentications. Duo also supports number-matching verified push and biometric authentication — an additional layer of security to verify your users' identities.

Duo Mobile is quick to deploy, simple to use, and works on Android and iPhone devices, tablets, and many smartwatches.

IN THIS CHAPTER

- **Looking at the problem of limited visibility across authentication silos**
- **Understanding the limitations of identity protection in identity management systems**
- **Making "all-or-nothing" access decisions**

Chapter 3 Recognizing the Problems with Identity Security

Identity management systems have some limitations that create identity protection challenges. From incomplete visibility across disparate identity management systems to weak protection capabilities and coarse, broad stroke access enforcement, these limitations often require IT, security, and identity and access management (IAM) teams to make risky tradeoffs that can potentially compromise the security of their users' identities.

Hopping Across Islands of Authentication

Identity management used to be relatively simple. Everything your users needed access to was in the corporate data center, so they simply needed to log into their network account that was authenticated by a centralized directory service, such as Active Directory (AD), Lightweight Directory Access Protocol (LDAP), or — going way back, Novell Directory Services (NDS).

Of course, managing a centralized directory service is challenging in itself, particularly for a large organization. IT has to manage provisioning and deprovisioning, role assignments, account lockouts and password resets, name changes, department changes, and more. It was a headache to say the least.

But then came the cloud. Today, more often than not, IT doesn't have the luxury of managing only a single, centralized directory. Instead, different software-as-a-service (SaaS) application providers may or may not offer federated access with single sign-on, and setting it all up can be a task unto itself. Or, they may have their own directory service which you'll need to manage for the users in your organization.

Other scenarios that may lead to multiple authentication silos include mergers and acquisitions, custom applications, legacy applications, and more. Compared to the headaches of managing a single directory service, this is a migraine.

Of course, multiple islands of authentication aren't just an administrative burden for IT. Users have to manage multiple accounts — and likely reuse their passwords, or some minor variation of their passwords — across these different authentication systems. User frustration often leads to poor security practices that can lead to account compromise.

WARNING

Beyond the challenges for IT teams and end users, security teams struggle to gain full visibility across all of these systems, increasing the risk that a compromised account will go undetected. Put simply, security teams can't see the (AD) forest for the (directory) trees. All of this creates a target-rich environment for threat actors.

TECHNOLOGY COMPANY DEPLOYS DUO SSO FOR SECURE ACCESS TO CLOUD APPS

A Silicon Valley-based tech company helps mid-market and enterprise companies reduce risk by organizing billions of public records into solutions that verify identities and check backgrounds while safeguarding the privacy of sensitive data. Because trust and safety are central to its mission, the company emphasizes security inside its organization.

The Challenge

In the company's early days, internal corporate applications were secured behind a firewall, and employees used devices locked down with tools like antivirus protection and a host-based firewall.

As the company grew, it took advantage of new technologies including cloud-hosted applications. Despite the efficiencies those applications allowed, they posed a significant challenge for the IT team: User identities began to sprawl.

Access management became challenging because IT had to keep up with several user directories to assign and revoke access, monitor and reconcile access privileges, audit and report user access, and more.

The Solution

The company started by consolidating user identities from several directories to a single on-premises directory service. With a single location to manage identities, they reduced time spent on user provisioning, deprovisioning, and access audit processes from several days to just hours per quarter.

However, a single identity increases the security risk of user credentials getting compromised. To mitigate the security impact of compromised user credentials, IT deployed Duo's secure single sign-on (SSO) with multi-factor authentication (MFA) to provide consistent, secure access to any cloud application.

The IT team further enhanced the company's security posture by applying policies based on the risks of each application, with consistent MFA usage and audit trails, while blocking risky devices and logins.

Duo's secure SSO also helps the company's employees get things done more efficiently. Users previously needed to enter credentials for multiple applications several times a day. With Duo's secure SSO, they can log in just once to access all their cloud apps from a single dashboard, using their existing credentials and strong MFA.

Identity Protection is Frail

Identity management systems are designed for creating identities, associating roles and permissions, and authenticating and authorizing identities. All of these tasks are relatively simple — albeit, greatly simplified in the example that follows: a user enters a username and password, the system compares the username and password to the credentials stored in the directory, and if the credentials match the user gets access based on the assigned roles and permissions stored for that user in the directory.

Beyond these functions, identity management systems provide some basic protections, such as enforcing minimum password requirements and locking out accounts if the wrong password is repeatedly attempted, but little else. Given the breadth of identity-based threats, from email phishing to password-stealing malware and more, the identity protections provided by most identity management systems today are inadequate.

Coarse Access Enforcement is Problematic

Many identity management systems take an “all-or-nothing” approach to access control. If a user successfully authenticates, they’re granted access to various applications and data based on their assigned roles and permissions. If not, access is denied. This coarse enforcement approach means that an attacker who successfully compromises an identity gets access to all of the roles and permissions associated with the account.

Manually managing a minimum set of permissions for every user based on their job requirements — the principle of least privilege — would be impractical for even the smallest of organizations. Role-based access control (RBAC) is a common method for addressing the need to assign similar permissions to various groups of users within an organization. Unfortunately, RBAC permissions are usually broad and overly permissive, and users are assigned roles based on instructions from human resources or a department head to “just set up their account the same as so-and-so’s.”

REMEMBER

The principle of least privilege requires that users are only assigned the minimum set of permissions necessary to perform their job functions. It’s a key part of a zero trust strategy.

Attribute-based access control (ABAC) and risk-based access control are evolutions of RBAC that provide more granular control of access permissions.

REMEMBER

In both ABAC and risk-based access control, highly adaptable and dynamic access control permissions are granted based on a range of attributes or risk factors, including:

- *User attributes*, for example, user ID, department, job position, security clearance, and group memberships
- *Resource attributes*, for example, resource type, resource owner, classification, and creation date
- *Action attributes*, for example, action type, hypertext transfer protocol (HTTP) commands, and create, read, update, and delete (CRUD) operations
- *Environment attributes*, for example, time of day, date, location, device type, and device compliance status

WARNING

Many identity management systems today do not support ABAC or risk-based access control.

DYNAMICALLY ASSESS RISK WITH DUO RBA

Duo's Risk-Based Authentication (RBA) evaluates potential threat signals at each login attempt and adjusts security requirements, in real time, to protect trusted users and frustrate attackers. This dynamic solution offers granular controls that provide organizations with a more nuanced and effective approach toward secure access.

At login, Duo examines signals such as user location, browser, and network from web access requests, as well as device attributes and status from the Duo Mobile app and the Duo Desktop app. Duo's patent-pending Wi-Fi Fingerprint technology can also evaluate change in location through anonymized network data, protecting user privacy.

(continued)

(continued)

Duo automatically responds to those threat signals at login to determine if the situation is high-trust or low-trust. This can involve identifying threats based on known attack pattern data (such as a high volume of push requests in a row) or contextual risk signals (like an unknown Wi-Fi account).

Based on the risk evaluation, the user will experience a corresponding amount of friction at login. Duo RBA only steps up security requirements if there are potential threats. If the situation is high-trust, the user can complete a Duo Mobile Push or forgo an additional MFA altogether with Duo Passport. If the evaluation indicates low-trust, the user will be asked to step up to a more secure authentication method, like Verified Duo Push, passwordless authentication, or be blocked entirely from access.

Duo RBA enables organizations to make access security decisions based on their risk appetite and organization's needs.

IN THIS CHAPTER

- **Getting away from passwords**
- **Improving identity security with artificial intelligence (AI) and analytics**
- **Making zero trust a reality with continuous monitoring and verification**
- **Looking at common identity management use cases**

Chapter 4 Reimagining Identity with Next-Gen Security Tools

Passwords have been used throughout human history to identify friendly troops, restrict access to buildings, and secure computer accounts, among other things. However, modern computing power and evolving threats have rendered even the strongest passwords largely ineffective and obsolete. It's time to reimagine identity with a new approach to authentication — without passwords.

The Future of Authentication: Passwordless

Multi-factor authentication (MFA), discussed in Chapter 2, requires a combination of two or more of the following factors: something you know, something you have, and/or something you are. Traditional MFA methods almost always include the weakest of these factors: a username and password (something you know).

Passwordless authentication, also known as modern authentication, establishes a strong assurance of a user's identity without relying on passwords. Instead, users authenticate with biometrics, security keys, or a mobile device. While this may seem counterintuitive because it removes one possible authentication factor (something you know), it instead greatly enhances security by only allowing stronger authentication factors: something you have and something you are.

Passwordless authentication also extends the concept of something you have and something you are beyond the solutions typically associated with traditional MFA. For example, *something you have*, in addition to a mobile device, could be a compliant laptop computer, a security certificate, or a hardware token, and *something you are* includes biometric features like a fingerprint, voice recognition, or iris scan — just like in the movies!

TIP

Passwordless authentication can't be achieved with a single solution. It requires a compatible IT and application ecosystem that puts security at the forefront. Platforms like Windows Hello, Touch ID, Face ID, and fingerprint application programming interfaces (APIs) must work in tandem with hardware-based biometric authenticators, supporting open standards like WebAuthn, Security Assertion Markup Language (SAML), and Client to Authenticator Protocol (CTAP). To achieve passwordless authentication is a journey with many steps, but at the end of the road lies an unmatched authentication experience.

This approach balances usability with stronger MFA authentication. Passwordless authentication gives users a frictionless login experience, while reducing administrative burden and overall security risks for the organization.

CISCO'S 130,000-USER PASSWORDLESS DEPLOYMENT

Cisco fully rolled out Duo Passwordless to over 130,000 users in August 2023. As a modern enterprise, the Cisco IT security team faces a complex and hybrid IT environment, regulatory and compliance requirements, and a general need to keep administrative and management costs to a minimum.

The Challenge

Password resets and account lockouts result in lost time and resources, and standard MFA increases security but at the expense of repeated user friction. Streamlining and consolidating authentication workflows became a priority for the Cisco IT team.

The Solution

With Duo Passwordless, Cisco was able to implement a Fast Identity Online (FIDO2)-based login flow that utilized Duo Single Sign-On (SSO) and built-in hardware biometric platforms like Touch ID and Windows Hello to improve the overall login experience without compromising security.

Responsive and adaptive access policies also contribute to a smoother end-user login experience and stronger zero trust security practices. Cisco deployed risk-based authentication (RBA) alongside passwordless. RBA steps up authentication to a more secure method when risk factors or novel attack patterns are detected such as impossible travel, push harassment, and push spray. Risk is assessed at each authentication request, even if the end user doesn't interact with Duo directly.

Another component of Cisco's zero trust strategy is to define device trust standards, especially with a hybrid bring-your-own-device (BYOD)-accessing workforce. Duo enabled Cisco to limit sensitive application access to only trusted endpoints like corporate-managed devices. This adds another layer of defense if credentials are compromised.

With thorough planning, alignment with leadership, and active communication and feedback practices, Cisco's rollouts saw high levels of adoption with minimal related helpdesk tickets — a resounding success in enterprise security.

Using AI and UEBA for Context-based Identity Security

Next-generation authentication will also leverage AI and user and entity behavior analytics (UEBA) to add rich context about users, their activities, and the applications they use in real time, and use that information to make security and access control decisions.

TECHNICAL STUFF

UEBA uses data to baseline what "normal" behavior is for each individual user and can trigger alerts when something abnormal is detected.

A sophisticated UEBA system models multiple data dimensions at once and uses machine learning (ML) to get better over time. You don't need to set up and manage a list of alert triggers; all you need is activity data — and the more the better. Instead of reacting to problems by creating new rules, this approach enables security teams to be proactive by investigating unusual behavior at an individual level.

Verifying Trust with Continuous Monitoring

Zero trust is a security framework based on the principle of "never trust, always verify" rather than granting implicit trust to all users inside a network perimeter. As discussed in Chapter 1, identity has become the new perimeter as cloud-hosted applications, remote and hybrid work, and distributed and extended workforces have become the norm.

WARNING

But traditional identity and access management (IAM) systems that only verify a user's identity during authentication, then grant overly-broad access (authorization) to your applications and data based on a "one-size-fits-most" role for the duration of the session, inherently violate the basic tenet of zero trust which is to never trust, always verify.

REMEMBER

Next-generation authentication must have continuous monitoring capabilities to enable organizations to successfully adopt a zero trust security posture. Both user and device identities must be continuously monitored and seamlessly verified over the full lifetime of the session.

An AI-powered next-generation authentication system can enforce the principle of least privilege with granular, just-in-time permissions that are granted only when necessary and can be immediately revoked, along with session termination when suspicious activity is detected.

Exploring Identity Management Use Cases

Next-generation authentication supports many important use cases that are common today, including:

- **User and device inventory.** You can't protect what you don't know about, so you need to know who your users are and what resources they need to access. Building and maintaining an accurate inventory that includes employee accounts, guest access, non-human identities (NHIs, such as service accounts), and devices, will help you identify inactive and orphaned accounts, excessive permissions, and authorized (known) and unauthorized (unknown) devices and access.
- **Non-employee account monitoring.** Every business has a supply chain that often includes consultants, contractors, vendors, partners, and other third parties that require access to your applications, systems, and data. As supply chain attacks become increasingly prevalent, it's critical that organizations apply additional scrutiny to non-employee accounts that may not have the same security controls as employee accounts, such as strong MFA, login restrictions, and device compliance.
- **MFA adoption and usage.** The goal for every organization today should be 100 percent MFA adoption and usage — for everyone, not just privileged admin accounts. Identity management systems can help organizations not only collect data about MFA enforcement and compliance, but also provide context-rich, risk-based authentication to support the journey to a passwordless future for all.
- **IAM reporting and analytics.** IAM systems are a rich source of data for reporting and analytics, providing organizations with visibility into comprehensive, cross-platform data and context about identities and devices. This, in turn, allows for more effective detection of identity breaches and improved security posture.
- **User or session investigation.** IAM systems can be integrated with other platforms — such as extended detection and response (XDR), cloud access security brokers (CASB), security information and event management (SIEM), and security orchestration, automation, and response

(SOAR) — to enhance security investigations with user and session information.

- **Continuous threat detection.** Continuous monitoring and trust verification before, during, and after login enables continuous threat detection and rapid incident response to mitigate the impact of an identity breach.

FUTURE PROOF YOUR IDENTITY PERIMETER WITH CONTINUOUS IDENTITY SECURITY

Continuous Identity Security from Cisco Duo, powered by Cisco Identity Intelligence, dramatically improves identity security without sacrificing user experience. It uses sophisticated AI to analyze identity and device context before, during, and after every authentication — creating a continuous evaluation that adapts to user behavior and invokes the right controls at the right time.

The result is more informed real-time enforcement not just at initial access but continuously throughout each session. Security is better because decisions are enriched with relevant identity context. User experience is better because continuous analysis means trust can be seamlessly shared between authentication checkpoints — resulting in longer sessions.

By leveraging data from across the identity infrastructure, Continuous Identity Security gains deep insights into access patterns and can swiftly detect anomalies. This intelligence is then applied across all authentication points, ensuring that security measures are responsive, targeted, and effective.

With the integration of Cisco Identity Intelligence, Duo is now a comprehensive identity security solution that complements any IAM stack. While Duo has traditionally focused on preventing identity-based attacks, Cisco Identity Intelligence expands Duo’s scope to a full solution that not only protects against but also identifies, detects, and responds to threats.

Continuous Identity Security provides visibility, support, and protection for organizations as they continue to improve and iterate their authentication environment — moving toward a passwordless future.

REMEMBER

Next-generation authentication, built on a foundation of passwordless authentication, provides a single strong assurance of users' identities to achieve user trust and empowers organizations to:

- **Improve user experience.** By eliminating reliance on passwords, users enjoy fewer logins and MFA prompts, leading to an increase in user satisfaction and productivity.
- **Reduce IT costs.** IAM administrators and help desks can benefit from reduced administrative burden due to password-related issues and resets.
- **Enhance security posture.** Eliminating passwords makes identity-based threats and vulnerabilities such as phishing, stolen or weak passwords, password reuse, brute-force attacks, and more, irrelevant for your organization.

IN THIS CHAPTER

- **Preventing breaches and maintaining compliance**
- **Reducing third-party risk**
- **Increasing operational efficiency and employee productivity**
- **Enabling greater visibility and defining roles and responsibilities**
- **Moving toward zero trust with risk-based access and device trust**

Chapter 5
Ten Key Business Outcomes of Identity Security

A strong identity security program can deliver significant benefits beyond reducing security risks. Here are ten key business outcomes that can result from a strong identity security program:

- **Breach prevention:** By improving network security and account hygiene, an identity security program can help prevent breaches before they occur. They can also help organizations respond quickly when compromised accounts are discovered, reducing the impact of any potential breaches.
- **Regulatory compliance:** Maintaining compliance with regulatory mandates and standards — such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), and Sarbanes-Oxley (SOX) — is a constant challenge for many organizations. An identity security

program can help ensure compliance by providing better visibility into access controls and simplifying reporting.

- **Third-party risk:** Many organizations struggle to manage third-party access to their systems and data. A strong identity security program can help an organization better manage guest accounts and monitor third-party activities, reducing the risk of data breaches caused by third-party access.
- **Operational efficiency:** A well-designed identity security program can decrease resource strain on IT and help desk teams by streamlining identity and access management (IAM) workflows such as account provisioning, permissions management, multi-factor authentication (MFA) enrollment, password resets, and reporting.
- **User experience:** Employees can benefit from an identity security program that provides quick and seamless access to their applications and devices, increasing productivity and reducing user frustration.
- **Cross-environment visibility:** Organizations can locate identity storage overlaps and discrepancies with a "birds-eye-view" to maintain good identity hygiene across complex IT environments and ecosystems.
- **Organizational structure:** You can define the roles and responsibilities of different stakeholders such as security teams, IAM/IT, help desk, and others and then set up precise management privileges that support a cohesive identity security strategy.
- **Risk-based access:** A strong identity security program adaptively responds to changes in risk level by requiring a stronger authentication factor when risk increases, while providing seamless access in trusted scenarios.
- **Device trust:** You can move beyond user authentication alone, to include device trust. Organizations can improve device visibility and support bring-your-own-device (BYOD) without requiring mobile device management (MDM) by allowing access only from trusted devices that have a health posture compliant with your organization's security policy.
- **Zero trust:** You can make progress towards zero trust strategy goals with robust identity protection that stays ahead of the threat landscape and prepares organizations against novel attack methods.

REMEMBER

By defining clear objectives and tying them to known business drivers and risks, organizations can ensure a strong identity security program that delivers measurable business value.

Protect your enterprise against identity breaches

With data breaches constantly in the news and on the rise, identity security has never been more critical. But in an ever-evolving threat landscape — and considering the majority of breaches involve the human element — how can you stay ahead of the attackers, educate your staff, and protect your organization from the devastating financial and reputational losses associated with identity breaches?

Identity Security For Dummies is your must-read guide to implementing a comprehensive identity security program to enhance your organization's security posture, improve employee experience, reduce the IT burden, and deliver significant business benefits. Dive in to discover how to keep identity security easy for users but tough for intruders.

Inside…

- Know the building blocks of an identity attack
- Understand the problems with current identity security
- Adopt the four pillars of a successful identity security program
- Explore the options with next-generation authentication and continuous monitoring

CISCO DUO

ISBN: 978-1-394-30088-4
Not For Resale

9 781394 300884

for dummies®
A Wiley Brand