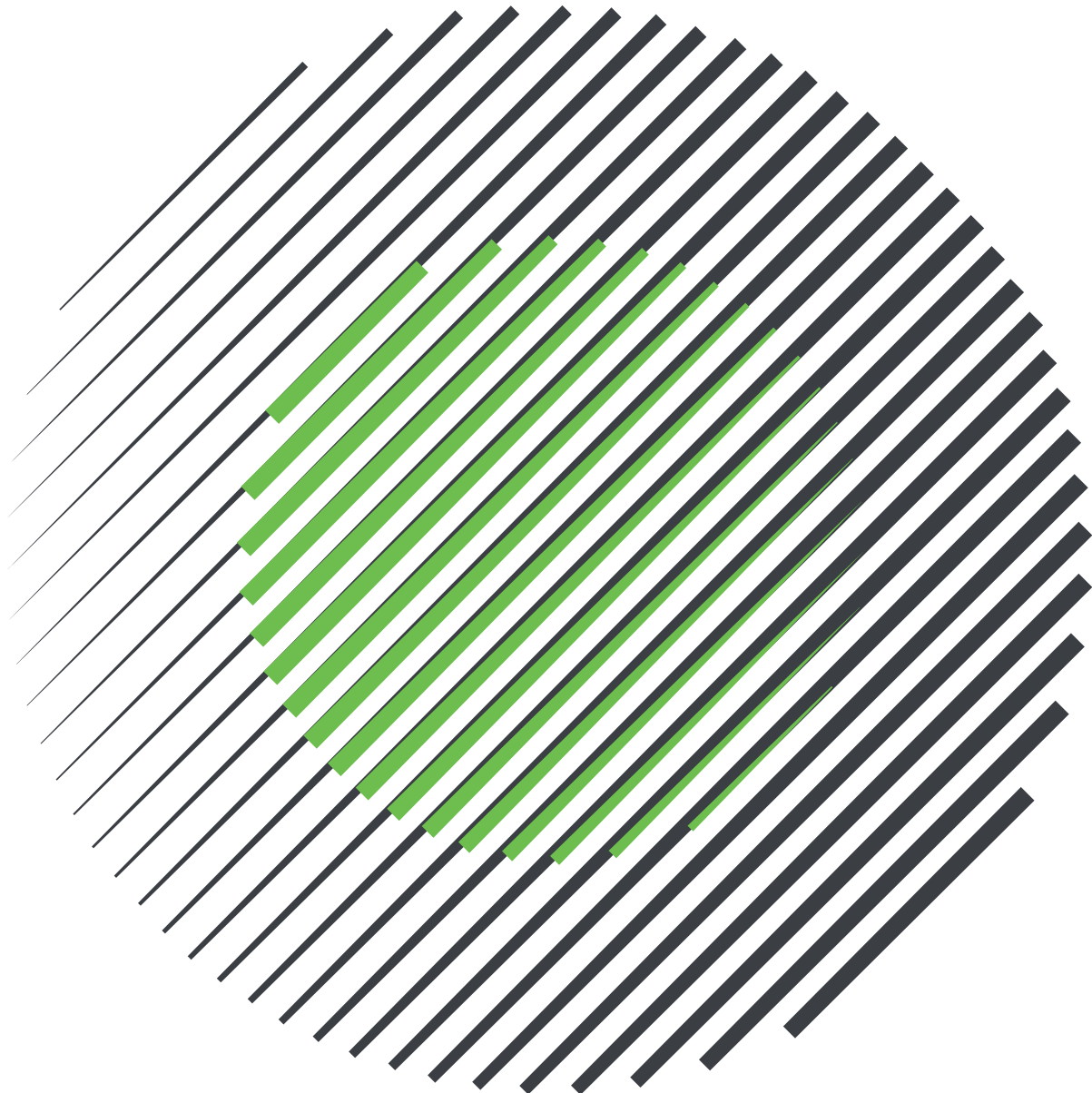


FIVE STEPS TO

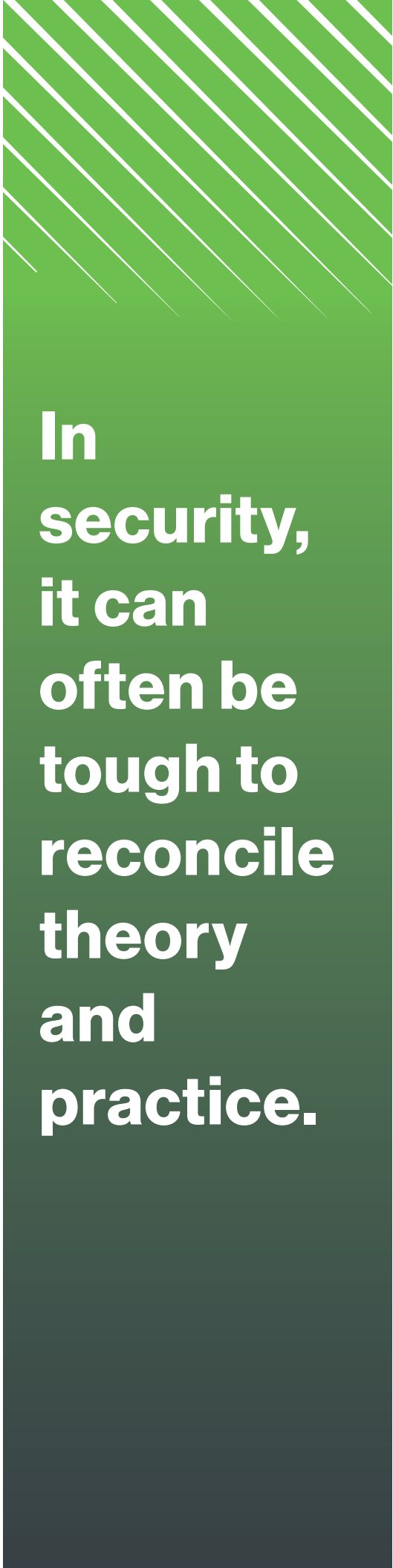
# Perimeter-Less Security

Adopting a Zero-Trust Model for Secure Application Access




Duo Security is  
now part of Cisco.






**In  
security,  
it can  
often be  
tough to  
reconcile  
theory  
and  
practice.**

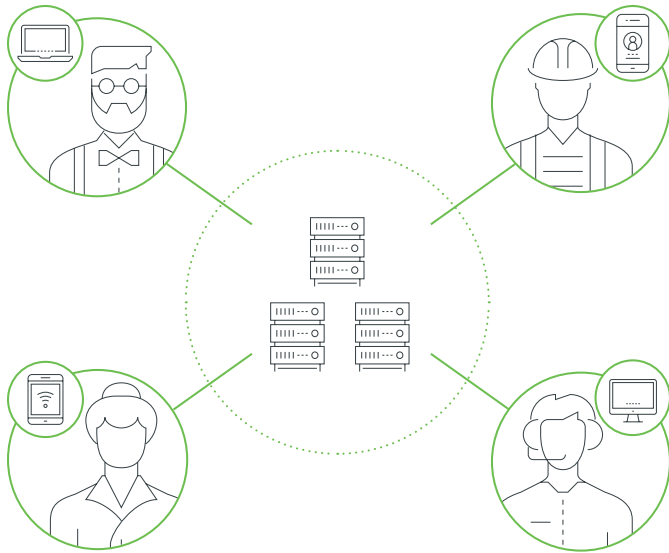


The traditional perimeter-based security model – centralizing key data and applications, then managing access through virtual private networks (VPNs), firewalls and mobile device management (MDM) solutions – should be an effective way to protect your network, in theory.

In practice, however, the old approach isn't aging well, particularly as users are bringing their own devices to work and sensitive company data is being stored in third-party cloud services. And with threats on the rise that exploit the old model's vulnerabilities, evolving beyond perimeter security isn't just a good idea for the future: it's essential for any organization that wants to stay competitive.

This shift has driven the need for a new paradigm – originally conceived by former Forrester Research analyst John Kindervag in 2010 and later adopted by Google with its “BeyondCorp” architecture, it's often described as a “zero-trust” model. In this paper, we'll talk about what that means, and share the five crucial steps you can take to adopt the zero-trust model in your organization.





Traditional Approach

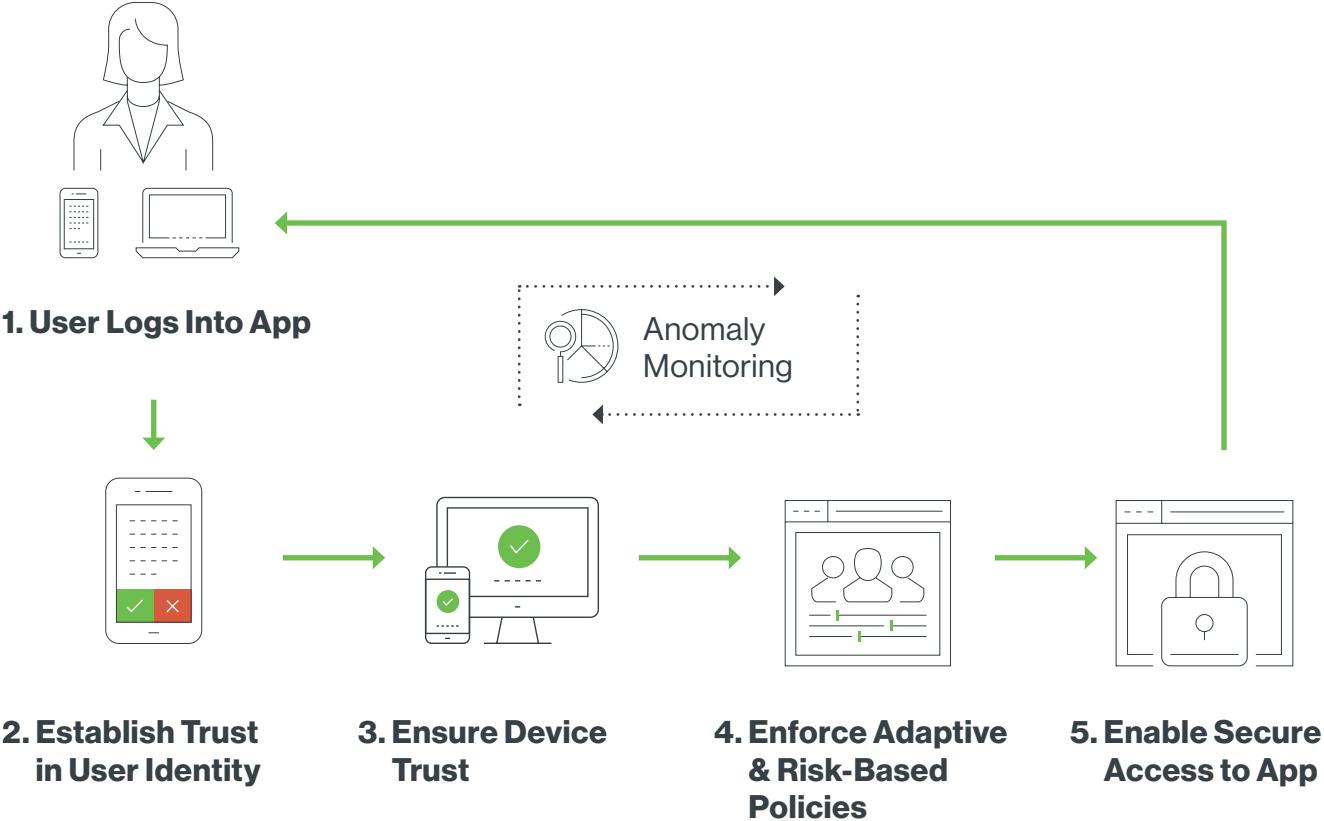


Modern Approach

# The New “Zero-Trust” Paradigm

When it was first established, a centralized web security approach made sense, because every business network had clear, defined security perimeters. That's not the case anymore: your security perimeter is now where your users and their devices are – and they can be anywhere.

# Zero-Trust Workflow



Where it was once manageable to spend time determining who should have trusted access and who shouldn't, the zero-trust paradigm instead embraces the reality that users need frictionless access from any device, and treats every access attempt as if it were originating from an untrusted network. A zero-trust model can be used to understand which devices are company-managed and which are not, and allow access based on device trust.

The migration to a zero-trust model is similar to how many offices have evolved from having a front desk manage building

entry to using security badges. The older model typically relies on a front-desk admin to determine who to let in and who to keep out, where using a badge means only people with proper credentials are allowed access. (We have nothing against front desks – we simply embrace the improved security and ease of using a badge to get in to work).

Zero trust creates user-centered security by taking multiple data points into consideration – instead of validating against a single criterion such as, “Do they have the right password?” security

is based on multiple factors, effectively asking, for example, “Do they meet the access requirements of multi-factor authentication (MFA), AND do they have an up-to-date mobile operating system, AND do they adhere to the right business-specific security policies?” By combining all of your security measures in a coordinated way to drive access policy, you're able to effectively enforce security measures on any access device, at any time.

Enough theory! Let's dive into the five steps to follow to go perimeter-less and adopt a zero-trust security paradigm.

# 1

## Establish Trust in User Identities

A username and password aren't enough anymore: a whopping 81 percent of reported web security breaches leveraged either stolen and/or weak passwords, according to Verizon's *2017 Data Breach Investigations Report*! To properly establish a user's identity, you'll need strong authentication policies, including MFA.

Your first mission is to deploy MFA to all of your users and applications. That's easier than it sounds, and as a bonus, you'll end up with a complete inventory of your users and devices, which will be helpful for future steps.

As a first effort, deploying MFA is also a good way to ease users into the transition toward the zero-trust model. While administrators may need time to adapt to the idea perimeter-less security, users will similarly need time to get accustomed to taking additional security measures each time they log in as part of a zero-trust environment.

# 2

## **Extend Visibility Into Users' Devices & Activity**

Now that you have a system in place to determine whether you trust your users' identities, it's time to get visibility into the devices they're using to access applications.

At its heart, this step is about creating and maintaining an inventory of all user devices, both personal and corporate-managed. That'll give you visibility into the existence of the devices themselves and also capture critical information about the security posture of those devices. This is critical to distinguish between devices that your organization owns and manages and the devices your users own and manage. Why's that important? It helps you gauge the security risks associated with users and devices to get a better handle on exactly what types of devices are accessing apps.

# 3

## Ensure the Trustworthiness of User Devices

We've talked about how zero trust can manage security based on multiple coordinated data points – and in the new paradigm, many of those key data points tell you more about the endpoint device requesting access. For your third step, you'll define and review the endpoint device characteristics that will get cross-referenced upon each login.

For example, many businesses use the zero-trust paradigm to establish the trustworthiness of a device in two key ways: (1) by verifying that it's a device that has been given access in the past, and (2) by mandating that it meets your security requirements (like a minimum version of the device's operating system or having encryption enabled).

It's also important to understand whether or not device is corporate managed.

Keep in mind that the “trustworthiness decision” for both users and devices takes place before a user is allowed access to the app. For example, if a user has the right credentials, but is trying to log in to their work email from a device that in some way doesn't meet your minimum criteria, they'll still be denied access.



# 4

## Enforce Risk-Based & Adaptive Access Policies

Next, you'll create the security policies that take both the user and the device into account. For example, instead of saying "Logging in to corporate email requires the user's name, password and a successful MFA," you can coordinate your device and user policies to say "Logging in to corporate email requires a username, password and MFA, but is only possible for devices that meet our minimum security criteria."

For example, if a remote user logs in from home at 9 a.m. to check email, that can be considered typical behavior and is within policy. But say that same user logs in over the weekend and checks customer data in Salesforce that they haven't accessed before, that can be considered anomalous, and a risk-based model can catch that.

And because the risk associated with users and their devices can change between access attempts – say, a user's device software goes out of date – your access policies must also adapt to changing conditions to maintain acceptable levels of risk.

# 5

## Enable a Secure Connection to All Applications

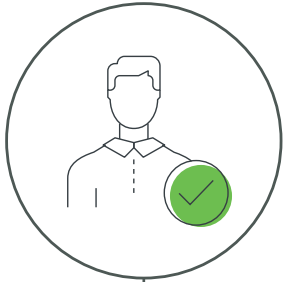
Once a user has validated both their identity and the validity of their device, and user-device policies have been enacted, users are then able to establish a secure connection between their devices and your applications.

Start by rolling out the zero-trust model to the applications that represent the highest risk. You'll need to protect all of your apps eventually, so start with the most important and make your way down the list. While in some cases, enabling a secure connection will be just a matter of "flipping a switch," in other cases, you may need access proxies to get certain applications functioning correctly. (An access proxy manages the connection between the end user, the zero-trust platform in use and your network).

It's important to note that connectivity to apps doesn't infer trust based on the network from where access originates, but instead by verifying the trust in users and devices.

When you combine secure connections to applications with adaptive policies, trust in user identities and trustworthiness of devices shifts access decisions from the network to the applications, which is a core component of a zero-trust security model.

# Zero-Trust Maturity Model



1

**Establish Trust in User Identities**



2

**Extend Visibility Into Users' Devices & Activity**



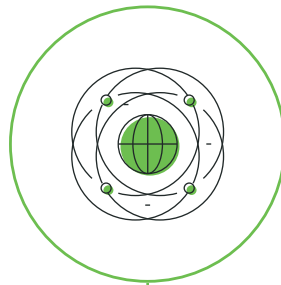
3

**Ensure User Device Trustworthiness**



4

**Enforce Risk-Based & Adaptive Access Policies**



5

**Enable a Secure Connection to All Applications**

**Zero Trust**

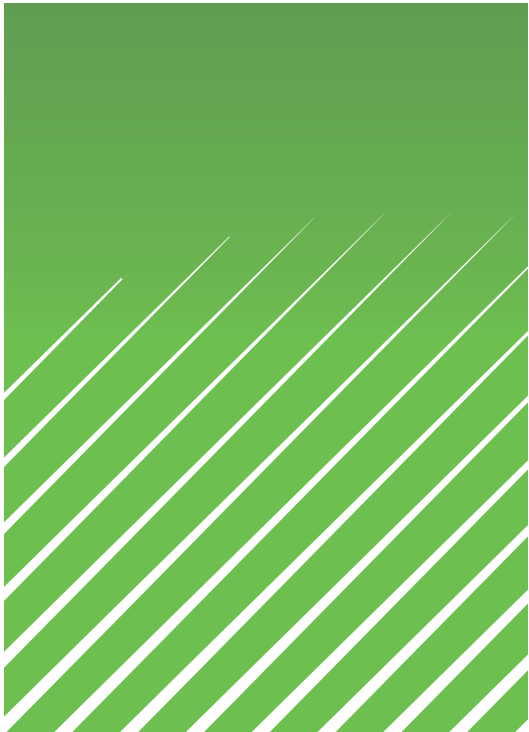
## What's Missing From This Picture?

Lastly, as you're considering when and how to move to zero trust, consider what's missing from the new model. There's no VPN, Network Access Control (NAC) or MDM solution needed – and that means all of the overhead from caring for and feeding those products is gone, too. As you're weighing your own next steps, be sure to take into consideration the time, money and effort you're saving by moving past the traditional model.



# Conclusion

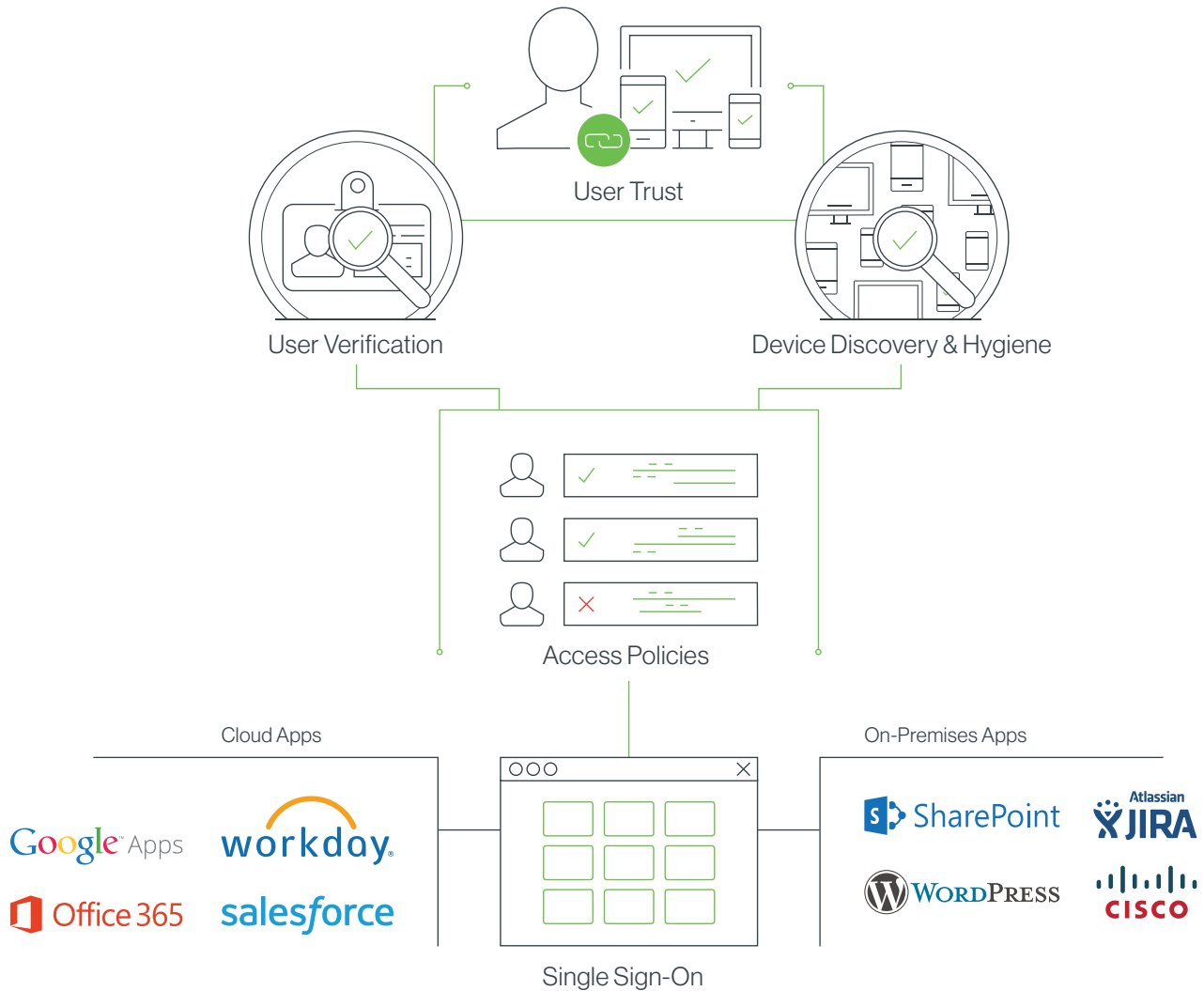
The zero-trust model is a huge step forward: we're moving from mostly static criteria like usernames and passwords to dynamic security scenarios based on the trustworthiness of users and devices. Businesses are safer when they can ask users "Are you the right person, using the right device, under the right circumstances?" and users are safer knowing they're required to do their part by keeping their devices healthy.





# Duo Beyond

Trusted Users. Trusted Devices. Every Application.



**Duo Beyond** secures access to all applications, for any user, from any device, and from anywhere. Cloud-first organizations and those looking for a secure, rapid transition to the cloud use Duo Beyond to protect their on-premises and hosted applications, while securing their mobile workforce and their chosen devices.

Duo Beyond delivers a zero-trust security platform that enables organizations to base application access decisions on the trust established in user identities and the trustworthiness of their devices, instead of the networks from where access originates. Duo delivers this capability from the cloud and without reliance on outdated, cumbersome, and costly technologies.

Learn more about **Duo Beyond** and start your free 30-day trial at [duo.com/beyond](https://duo.com/beyond)



