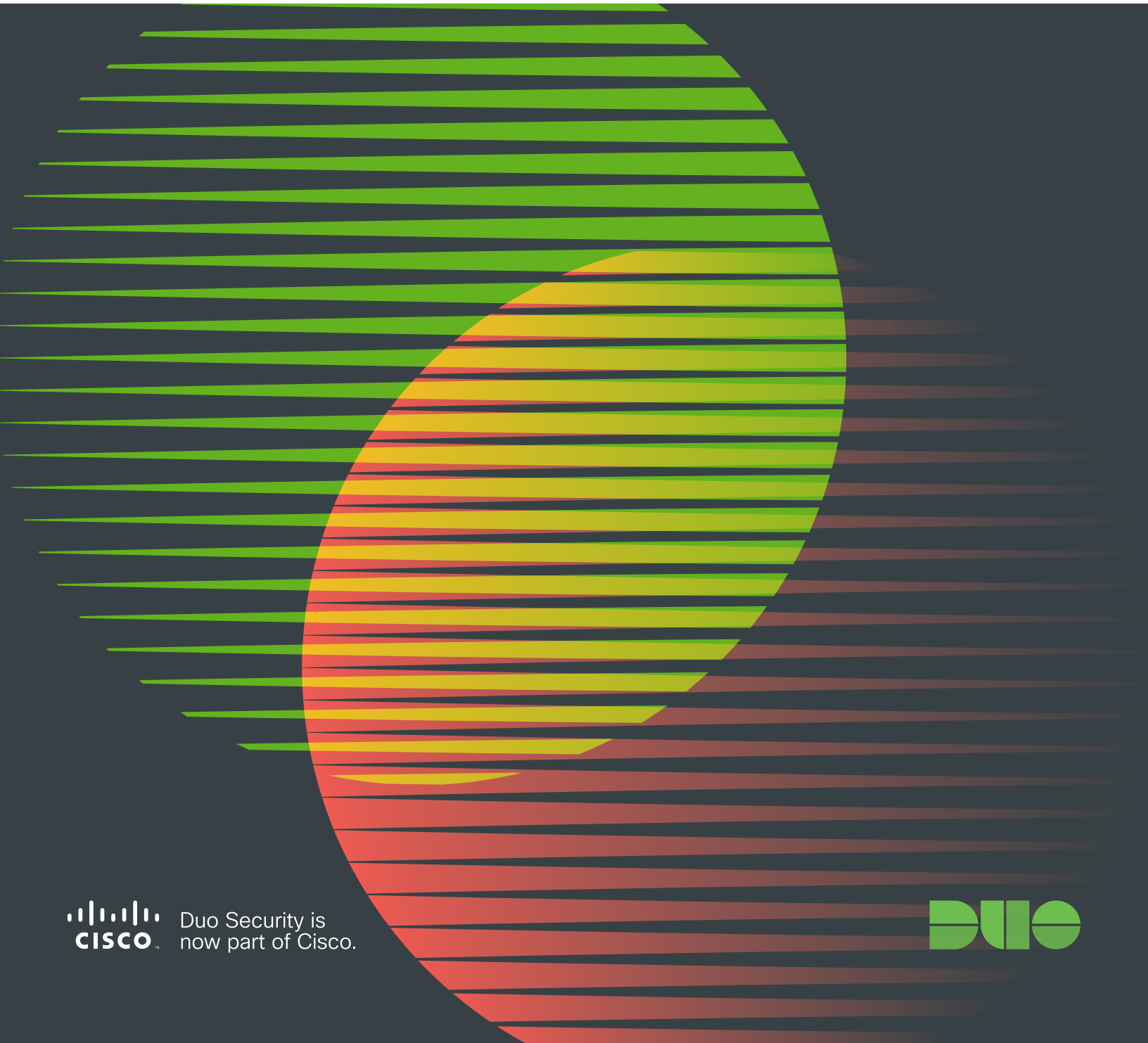
The 2018 Duo

Trusted Access Report

The State of Enterprise Remote Access



Duo Security is now part of Cisco.

The 2018 Duo
Trusted Access Report

The State of Enterprise Remote Access

AUTHOR
THU T. PHAM

RESEARCHERS
OLABODE ANISE
KYLE LADY

DESIGNERS
CHELSEA LEWIS
MARLA JONES

PRODUCER
BRANDON NALBAND

0.0

Securing Enterprise Remote Access

What does work look like today?

The way people interact with technology has irrevocably changed our concept of and relationship with remote access to the enterprise, calling for a major digital transformation.

A digital transformation of the enterprise IT model means:

- Newer businesses are now cloud-centric by design, and older, larger enterprise companies are making the transition from legacy infrastructure to the cloud.
- People (users, consumers and employees) have embraced mobile, often using personal, unmanaged devices to conduct work remotely.

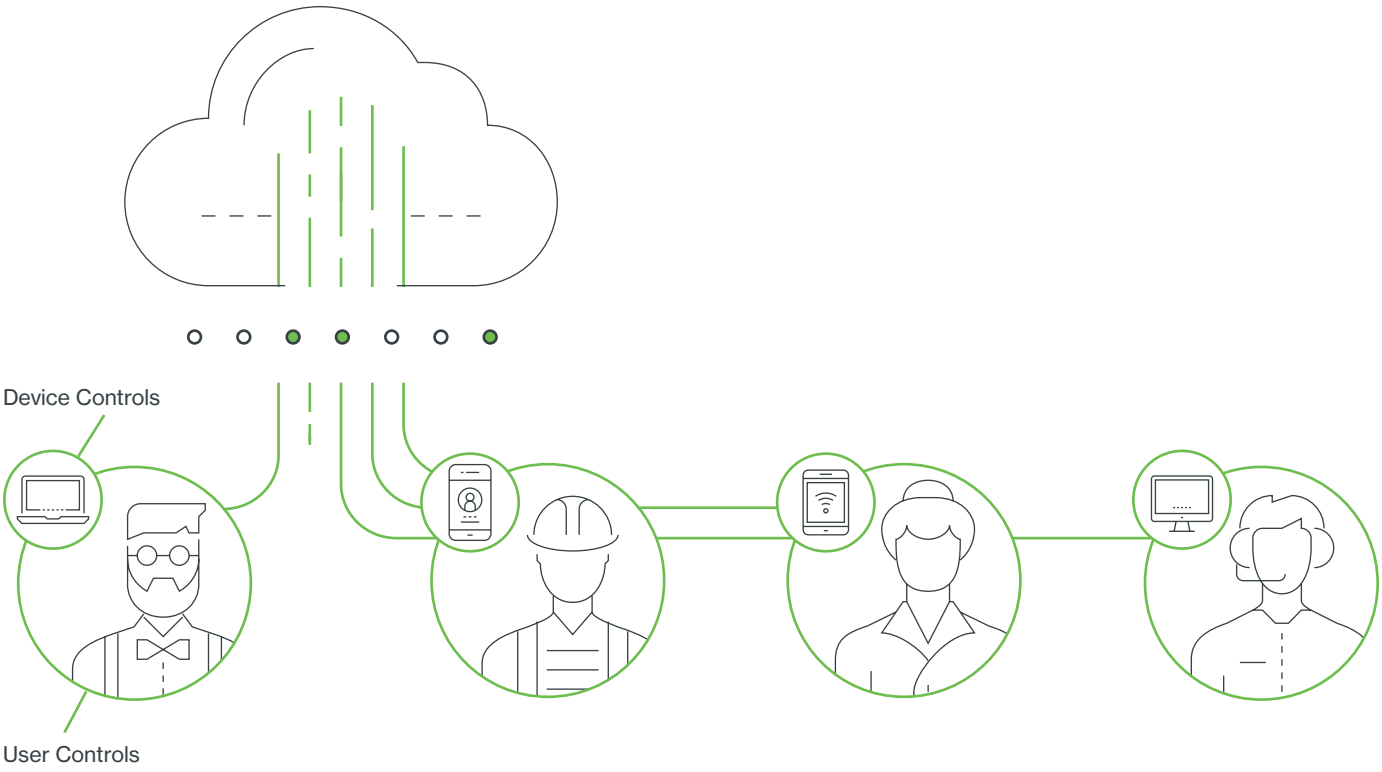
This digital transformation has driven the enablement of remote access to company data, applications and resources.

That can put your users and devices at risk – threats that exploit their **identities** (like social engineering, phishing, stolen or weak passwords, etc.) and their **devices** (malware, vulnerabilities, etc.) mean your company may be at risk, too – as they present entry points into your network.

These threats bypass traditional network-based security controls that focused on protecting against external threats, with no protection on the inside.

As a result, a new enterprise security model must evolve to effectively and strongly secure both users and devices – adding more controls than a traditional perimeter-based security model.

This report takes a closer look at user authentications and how users behave in phishing simulations, as well as shedding light on the security health of users' devices used to log into enterprise applications.



Methodology

In this report, our security research team, **Duo Labs** analyzed Duo's data on over 10.7 million devices and nearly half a billion authentications per month, spanning North America and Western Europe to give you insight into:

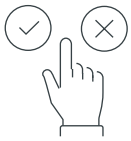
User Behavior

- Where are users authenticating from? Which industries see different trends in remote access?
- In phishing simulations, how many users are opening emails, clicking on links and entering in credentials?
- How many phished users are on devices running out-of-date operating systems or software?

Device Health

- What types of devices are users authenticating into enterprise applications with? What kind of trends are we seeing in mobile usage?
- Which operating systems (OS), browsers and plugins are out of date? Which industries are slow to adopt the latest versions?

Nearly 11 million users securely access over 800,000 applications and services across the world using Duo's trusted access solution.



Nearly

0.5 billion

Authentications per Month

10.7 million

Devices

800,000

Applications and Services

1.0

Key Findings

A high-level overview of the top findings from our data research and analysis.

User Behavior

Trends in how users are accessing enterprise applications, and the results of how they respond to phishing campaign simulations.

Remote Access:
Increasingly Mobile Users

Enterprise organizations are increasingly authenticating into applications from non-office networks (10 percent increase in the average number of unique networks) – and the largest increase can be seen by large enterprise companies (24 percent).

Phishing

Over half (62 percent) of simulated phishing campaigns captured at least one set of user credentials, and even more campaigns (64 percent) had at least one out-of-date device.

Device Health

The current state of enterprise devices, trends in mobile usage and across different industries.

OPERATING SYSTEMS:

Apple Rises in Dominance

The data shows more users on Apple devices, and a slight drop off in Windows users. The data also shows a majority shift toward Windows 10 – a jump from 27 percent in 2017 to 48 percent running the latest Windows OS in 2018.

The computer and electronics industry is the top industry moving to Windows 10, while healthcare is slowest to update.

MOBILE:

Android Devices Lag Behind in Updates

iOS and macOS devices are generally more up to date than Android and Chrome OS devices. In March, only 8 percent of Android phones were on the latest security patch (released 26 days prior).

BROWSERS:

Firefox Mobile Remains Out of Date

At the time of our data collection, Firefox mobile was the most out-of-date browser, and Internet Explorer was most up to date. Compared to 2017, nothing has changed – Firefox mobile and IE were the most out-of-date and up-to-date browsers, respectively.

FLASH:

Extinction Continues

Flash is very quickly disappearing from browsers – jumping from 24 percent of browsers with Flash uninstalled in 2017, to 69 percent in 2018. But of the devices that did have Flash installed, 52 percent were running an out-of-date version.

2.0

User Behavior

How are people using technology today – and how can supporting them working remotely help increase their productivity? We looked at the networks from which people access work applications, as well as how they perform in internal phishing simulations.

Working Remotely

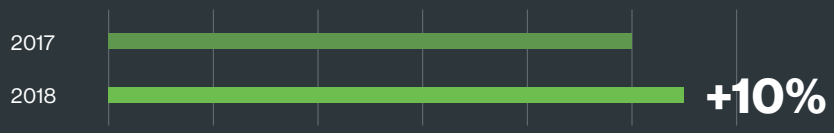
In 2018, 63 percent of employers have remote workers, while more than half of hiring managers today employ freelancers and contractors. This is up from 24 percent in 2017, according to Upwork's ***Future Workforce Report***[1]. Hiring managers also expect up to 38 percent of their full-time staff will be working remotely in the next decade.

People are logging into applications, networks and systems wherever, and whenever as work hours start to flex to fit different lifestyles, time zones and travel. Cloud-based applications and data allow users to access work resources wherever – whether at home, in-flight, in coffee shops, at hotels, etc.

Trends in Authentications From Unique Networks

Likewise, there's an upward trend in enterprise application access from non-office networks. From 2017 to 2018, our data shows a ten percent increase in the average number of unique networks that customers and enterprise organizations are authenticating from.

INCREASE IN UNIQUE NETWORKS PER CUSTOMER



SOURCE: Duo Security

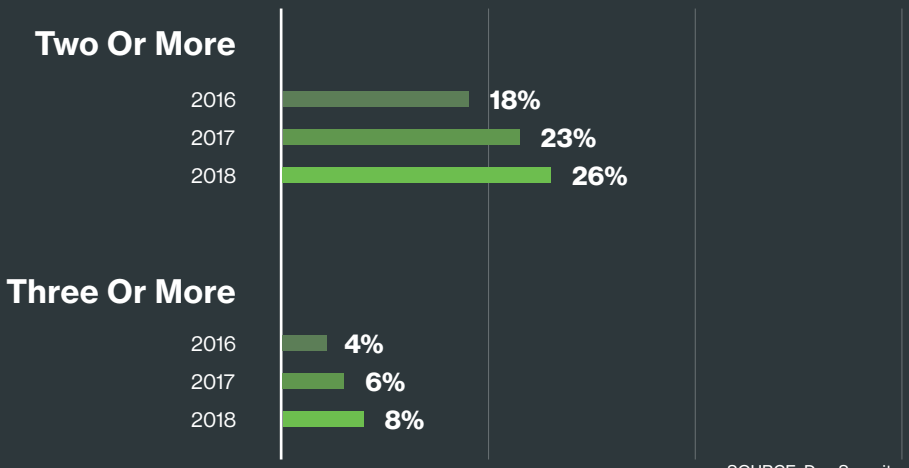
That means more work is being conducted from potentially unsecured Wi-Fi networks – those might include homes, airports, coffee shops or other public spaces. These external, untrusted networks may introduce potential risks to your corporate applications.

Trends by User, Per Week

The percent of users accessing applications from two or more unique networks per week has increased. In 2017, 26 percent of users accessed apps from two or more distinct IP address ranges, an increase from 2016, when it was 18 percent of users.

While a small increase, the percent of users accessing apps from three or more distinct IP address ranges doubled since 2016 – from 4 percent to 8 percent in 2018. This means that users are increasingly logging into work applications from several different networks and locations during the course of a week.

USER ACCESS FROM MULTIPLE UNIQUE NETWORKS



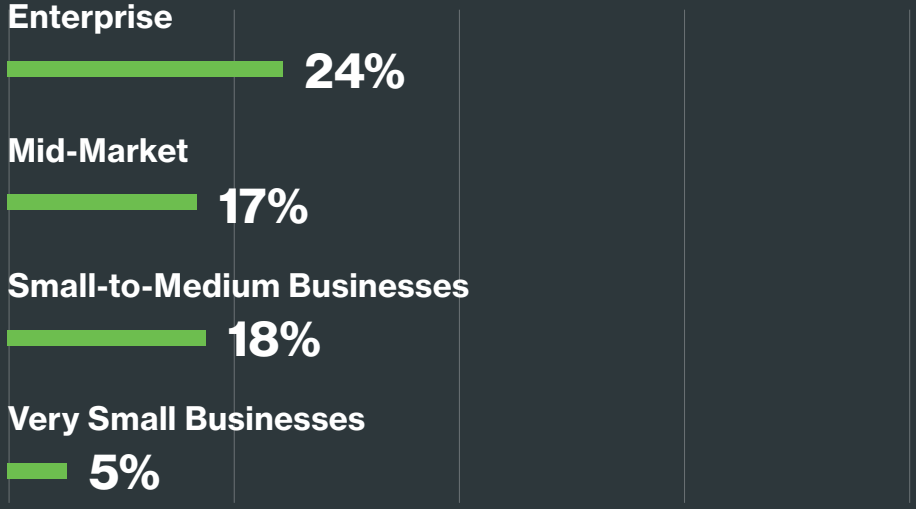
SOURCE: Duo Security

Trends by Market Segment

Our authentication data also shows a 17 percent and 24 percent increase in unique networks per organization, for mid-market and enterprise companies, respectively. Enterprises often have many more and different types of users that may be traveling more often, which could account for the major increase in access from unique networks.

INCREASE IN UNIQUE NETWORKS ACCESSED PER CUSTOMER

From 2017 to 2018

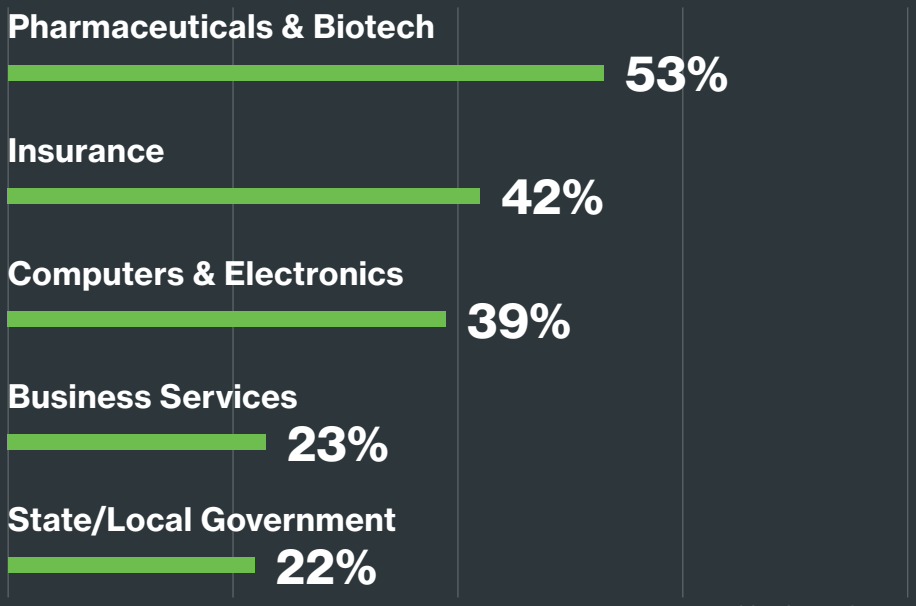


SOURCE: Duo Security

Trends by Industry

The growth in remote network authentications is the greatest in the pharmaceuticals and biotech, insurance, computers and electronics, business services and government (state/local).

REMOTE ACCESS TRENDS BY INDUSTRY



SOURCE: Duo Security

Phishing

How do users respond to internal phishing simulations? Those are campaigns that a security or IT team will set up and send to their users to assess how they react.

Here's what we found after analyzing **7,483 phishing simulation campaigns** conducted from mid 2017 to April 2018 on more than **230,000 recipients** via the Duo Admin Panel and free **Duo Insight tool**.

User Credentials and Devices

Our data shows that more than half of phishing campaigns have captured at least one set of user credentials. It also found that more than half of phishing campaigns involved at least one out-of-date device.

62% of campaigns captured **one set of user credentials**

64% of campaigns involved **one out-of-date device**

This exemplifies the need for stronger user authentication to prevent unauthorized logins by attackers with phished credentials. The most effective way to accomplish this is by requiring a security token or smartphone to verify user identities through *something they have*, not just *something they know* (such as a password, which can be easily phished).

In addition to verifying user trust, confirming device trust is important for avoiding compromises or malware delivered through phishing attempts that exploit known vulnerabilities in out-of-date devices. A major part of determining device trust is having insight into managed, unmanaged and potentially risky devices.

Nearly half of users opened phishing emails, while almost a quarter clicked on links in the emails – others entered their credentials and had out-of-date browsers and operating systems – all user behavior that could potentially lead to a remote access compromise or malware infection.

43%
Opened the email

23%
Clicked the link

12%
Entered credentials

10%
Had out-of-date browsers

15%
Had out-of-date operating systems

SOURCE: Duo Security

3.0

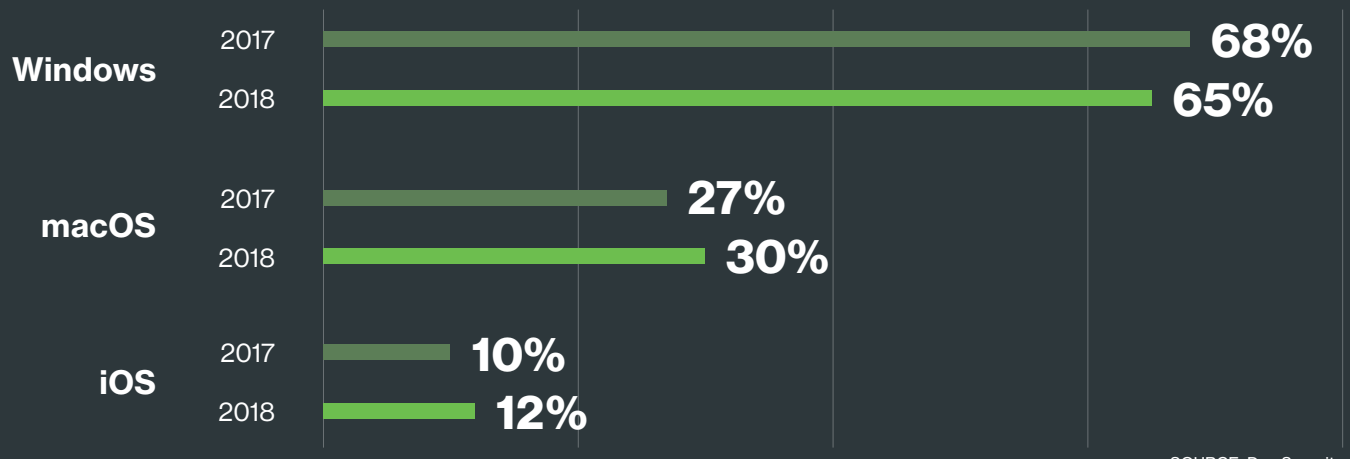
Device Health

Windows vs. Mac

Our data shows a slight drop in Windows users, while there's an uptick in Mac users, including iOS – indicating a slight increase in mobile users on Apple iPhones and iPads.

With more users authenticating into enterprise applications via mobile Apple devices, this shows a trend in the increasingly mobile enterprise user, accessing work applications remotely.

OS ADOPTION



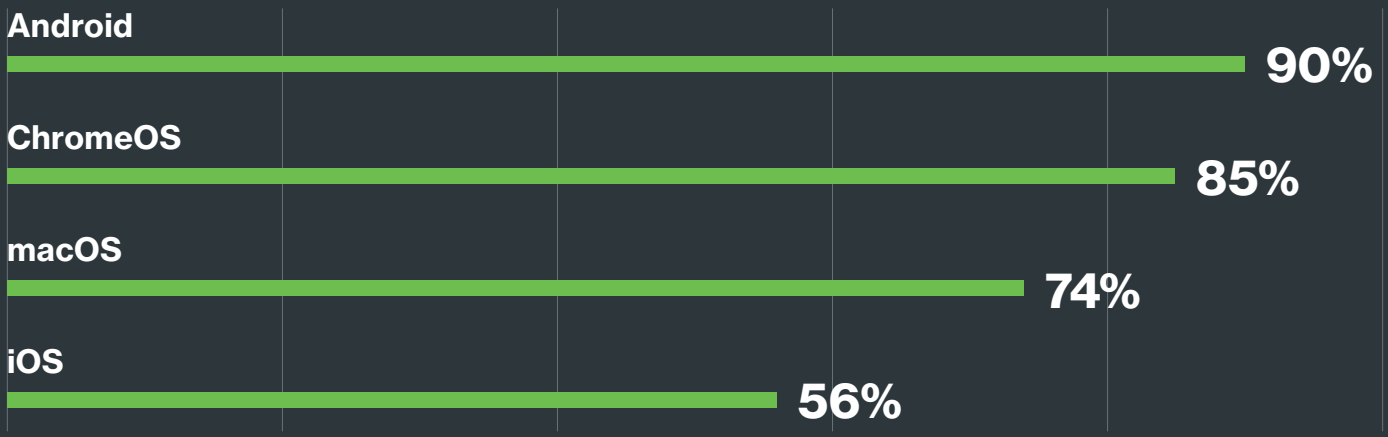
SOURCE: Duo Security

Operating Systems

Most endpoints are not running the latest operating system version, but iOS and macOS devices are generally more up to date than Android and Chrome OS devices.

At the end of March, only 8 percent of Android phones had applied the latest security patch released 26 days prior. Only 13 percent of Android phones were running one of the last three patches released.

OUT-OF-DATE DEVICES



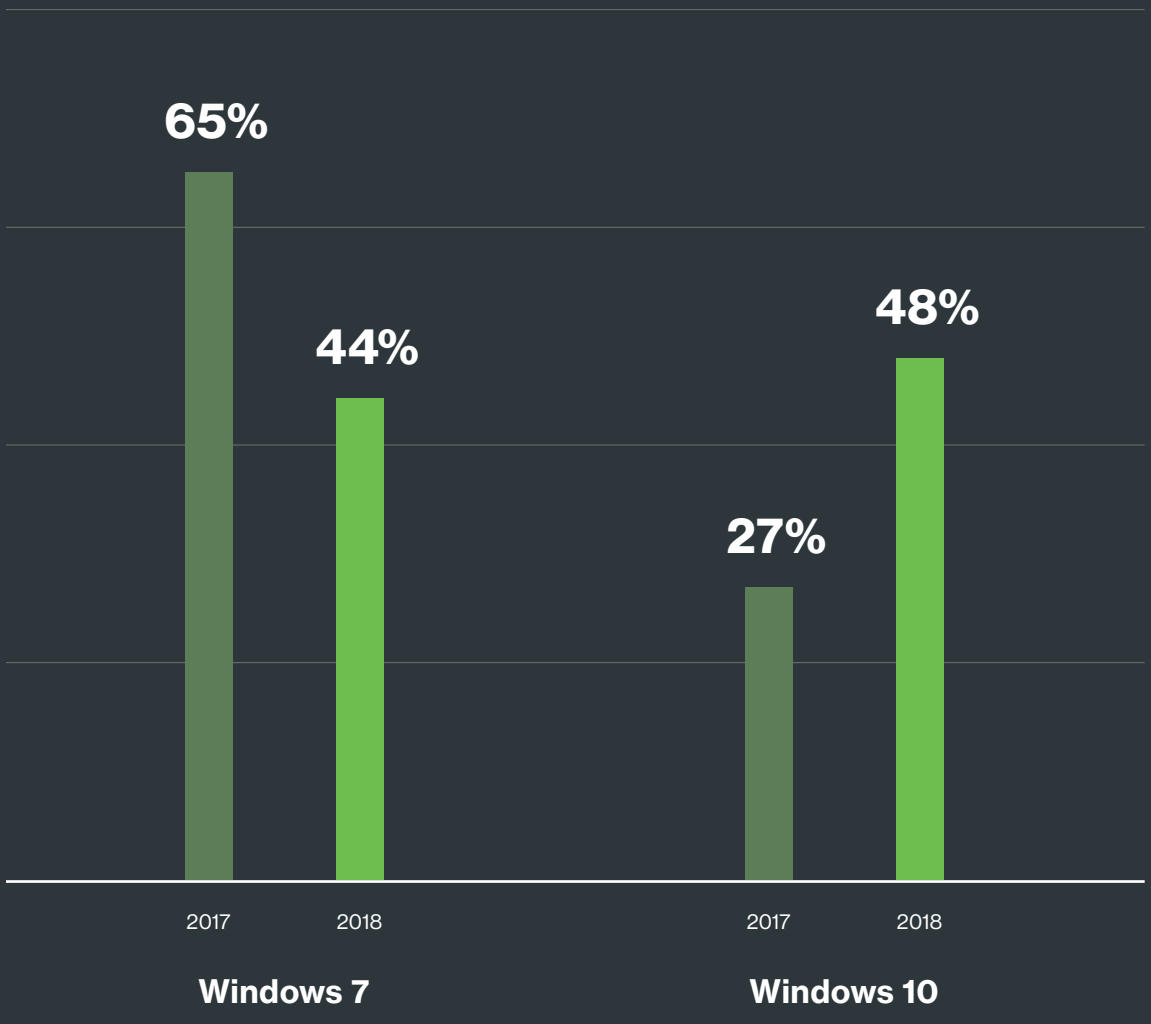
SOURCE: Duo Security

Out-of-date endpoints accessing enterprise applications can introduce risk to your organization if you lack visibility or control over all devices on your network – both managed (corporate-owned and controlled) and unmanaged (personal devices owned by employees).

Windows 10 Trends

At long last, our data shows more Windows endpoints running the latest OS version, Windows 10 – a major increase from 27 percent in 2017 to 48 percent in 2018. There's also a decrease in devices running Windows 7, from 65 percent last year to 44 percent in this year.

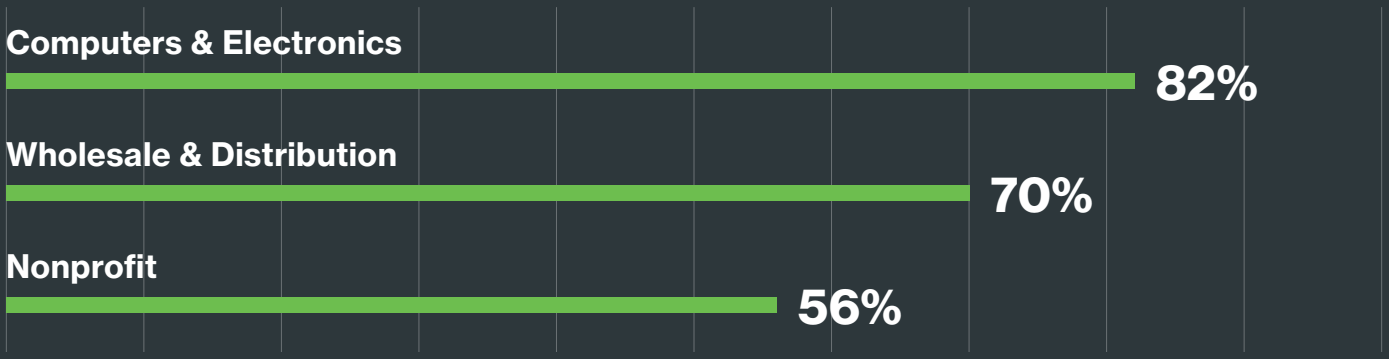
WINDOWS 10 ADOPTION



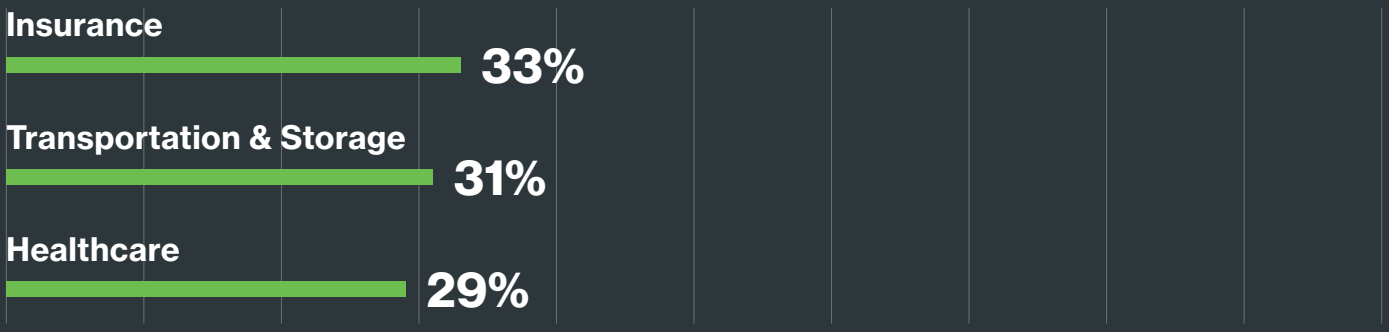
SOURCE: Duo Security

The industries that are slowest to adopt Windows 10 are healthcare, transportation and storage, and insurance. The industries quickest to move to the latest Windows OS are computer and electronics, wholesale and distribution, and nonprofit.

WINDOWS 10 ADOPTION: TOP 3



WINDOWS 10 ADOPTION: BOTTOM 3



SOURCE: Duo Security

Updating operating systems across large enterprises with complex IT models isn't always possible without rendering certain devices inoperable – for example, some internet-connected medical devices and software used in the healthcare industry aren't always designed or updated by vendors to run on the latest Windows OS.

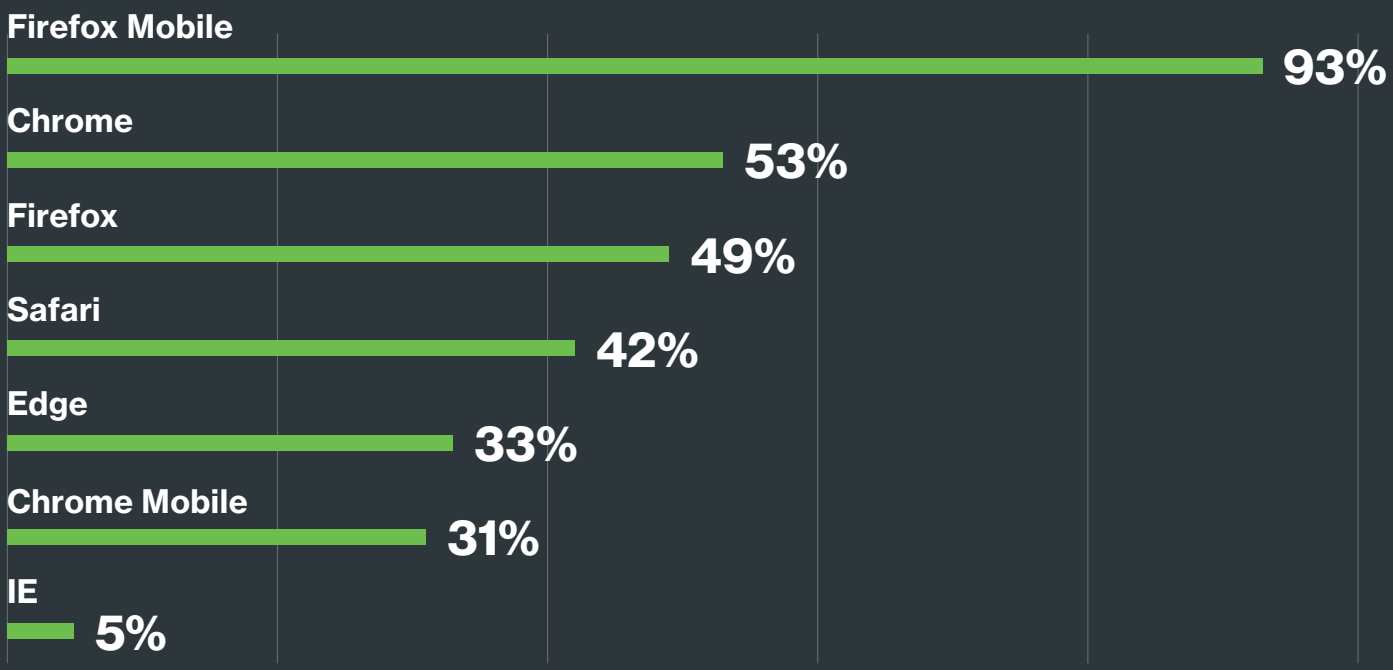
But running an unpatched, older OS can potentially leave your enterprise vulnerable to attack. In 2017, the WannaCry ransomware that infected more than 400,000 devices worldwide exploited a vulnerability designed to work only against unpatched Windows 7 and Windows Server 2008 systems, according to Microsoft.[2] About 98 percent of the computers affected by WannaCry were running some version of Windows 7, according to data from Kaspersky Lab.[3]

Knowing what devices are running what OS version requires insight into both managed and unmanaged devices accessing your corporate applications and data. And through device-based policies, you can control what devices are allowed access to certain applications.

Browser Trends

At the time of our data collection, Firefox mobile was the most out-of-date browser running on enterprise devices, while Internet Explorer was the most up to date, followed by Chrome mobile and Edge.

OUT-OF-DATE BROWSERS



SOURCE: Duo Security

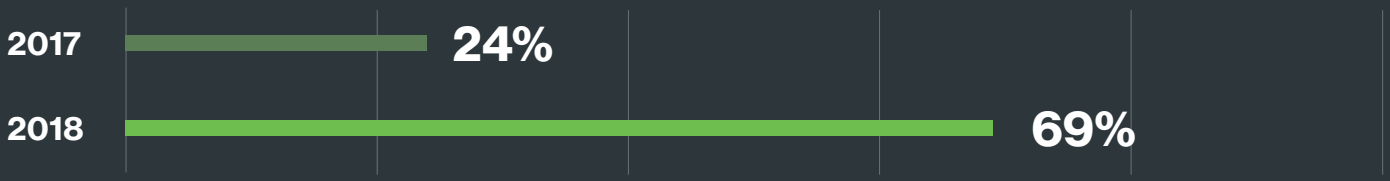
Compared to 2017, Firefox mobile still ranks as the most out-of-date browser, while IE is the most up to date. However, Chrome now ranks second as the most out-of-date browser, taking rank over Safari.

For additional context, IE hasn't released a new version since 2013, while Chrome just released one on March 6, 2018. So, while it appears as though Chrome browsers are more out of date, the browser tends to get updated more frequently by its vendor, Google, than other browsers.

Disappearing Flash

Adobe Flash Player is very quickly disappearing from browsers – jumping from 24 percent of devices with Flash uninstalled in 2017 to 69 percent in 2018.*

BROWSERS WITH UNINSTALLED FLASH



SOURCE: Duo Security

BROWSERS WITH OUT-OF-DATE FLASH

SOURCE: Duo Security

According to Google, the percentage of daily Chrome users loading at least one page of Flash content per day has plummeted from 80 percent in 2014 to 4 percent in early 2018. Flash will cease to be shipped with Chrome by 2020, and Adobe will end-of-life it in that same year.

Flash will cease to be shipped with Chrome by 2020, and Adobe will end-of-life it that same year.

*Note, "uninstalled" includes browsers with Click to Play or other form of Flash blocker implemented. This means browsers won't run arbitrary Flash applications without explicit user opt-in, which can help protect against attacks and cut down on annoying Flash ads.

4.0

Summary

In summary, after analyzing our data on over 10.7 million devices and nearly half a billion authentications per month, we've found that:

- Remote access has increased over the past two years – and the biggest increase was seen in the enterprise.
- Phishing is still as effective as ever – more than half of simulated campaigns captured credentials or out-of-date devices.
- There's a rise in mobile Apple users, and they're more up to date than Android/Chrome OS users.
- Nearly half of Windows endpoints are finally running Windows 10 (although there's another 44 percent still running Windows 7).
- The majority of browsers are finally uninstalling or enabling Click to Play for Adobe Flash Player.

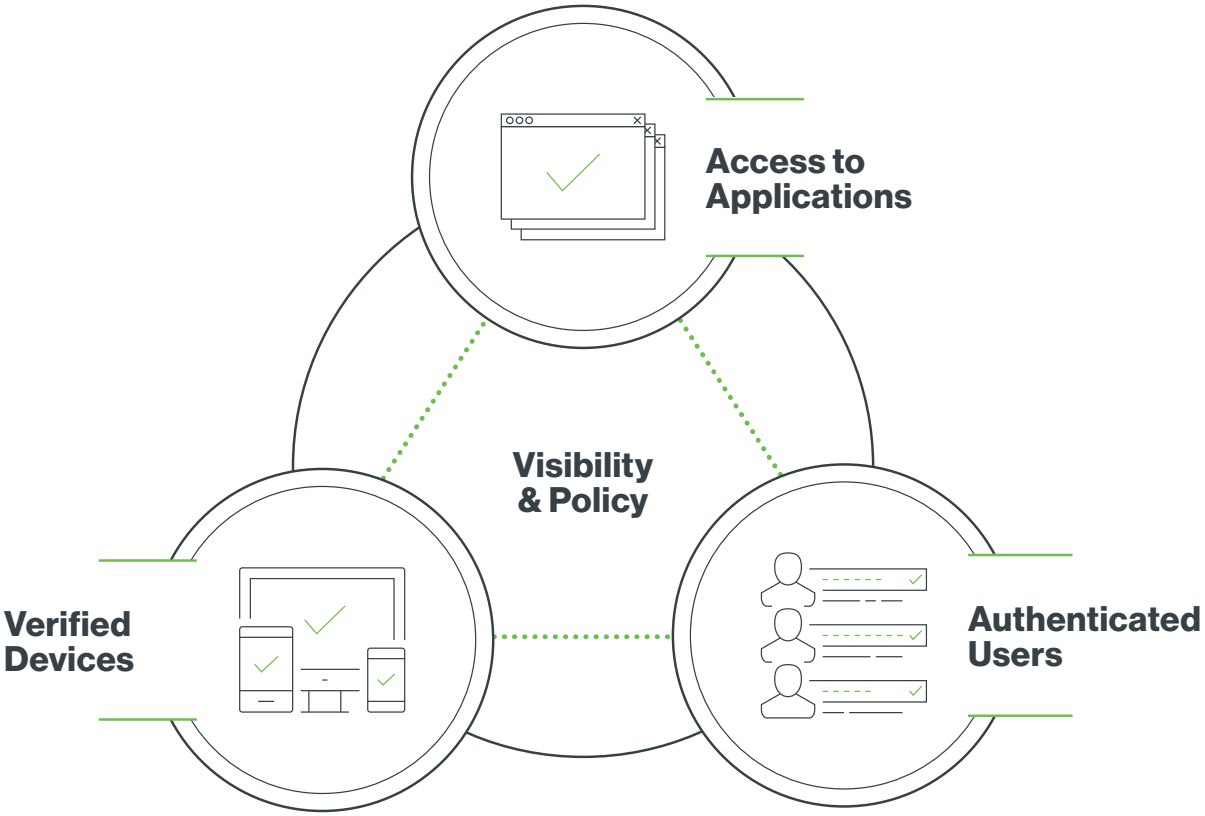
Shifting to a new enterprise security model means refocusing controls based on risk factors related to users and their devices to protect against threats like phishing, stolen credentials and exploits that compromise out-of-date devices and gain access to enterprise applications.

By verifying both the identity of a user and the security health of their device, you can employ a zero-trust security model at your organization that assures no traffic within an enterprise's network is any more trustworthy than traffic coming from outside the network.

5.0

Duo Beyond

A Zero-Trust Approach to Securing Remote Access

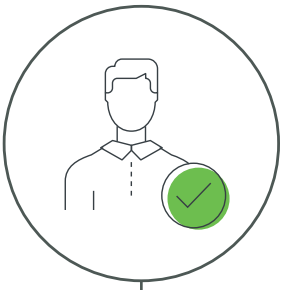


A zero-trust security model can help you secure against remote access threats outlined in this report, such as phishing, stolen credentials and out-of-date devices that may be vulnerable to known exploits and malware.

This security framework gives you visibility into and control over your authenticated users and their verified devices, granting them secure access to your applications only after they meet your specific security policy requirements.

Zero-Trust Maturity Model

Your organization can quickly and securely adopt a zero-trust security model by taking the following steps:



1

Establish Trust in User Identities

Verify the identity of all users with Duo's easy-to-use, strong **two-factor authentication** before granting access to corporate applications and resources.

2

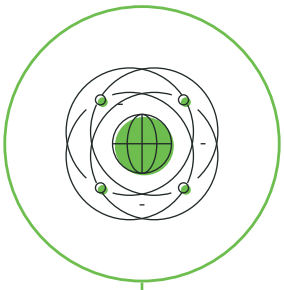
Gain Visibility Into Devices & Activity

Gain visibility into every device used to access corporate applications, whether or not the device is corporate-managed, without onerous device management agents.

3

Ensure Device Trustworthiness

Inspect all devices used to access corporate applications and resources at the time of access to determine their security posture and trustworthiness. Devices that do not meet the minimum security and trust requirements set by your organization are denied access to protected applications.



4

Enforce Adaptive & Risk-Based Policies

Protect every application by defining policies that limit access only to users and devices that meet your organization's risk tolerance levels. Define, with fine granularity, which users and which devices can access what applications under which circumstances.

5

Enable Secure Access to All Apps

Grant users secure access to all protected applications through a frictionless, secure **single sign-on** interface accessible from anywhere, without a VPN. Protect all applications – legacy, on-premises, and cloud-based.

Zero Trust

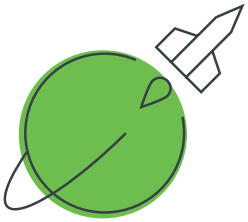
References

[1] ***Future Workforce Report***; Upwork; 2018

[2] ***Ransom:Win32/WannCrypt***; Microsoft; Jan. 10, 2018

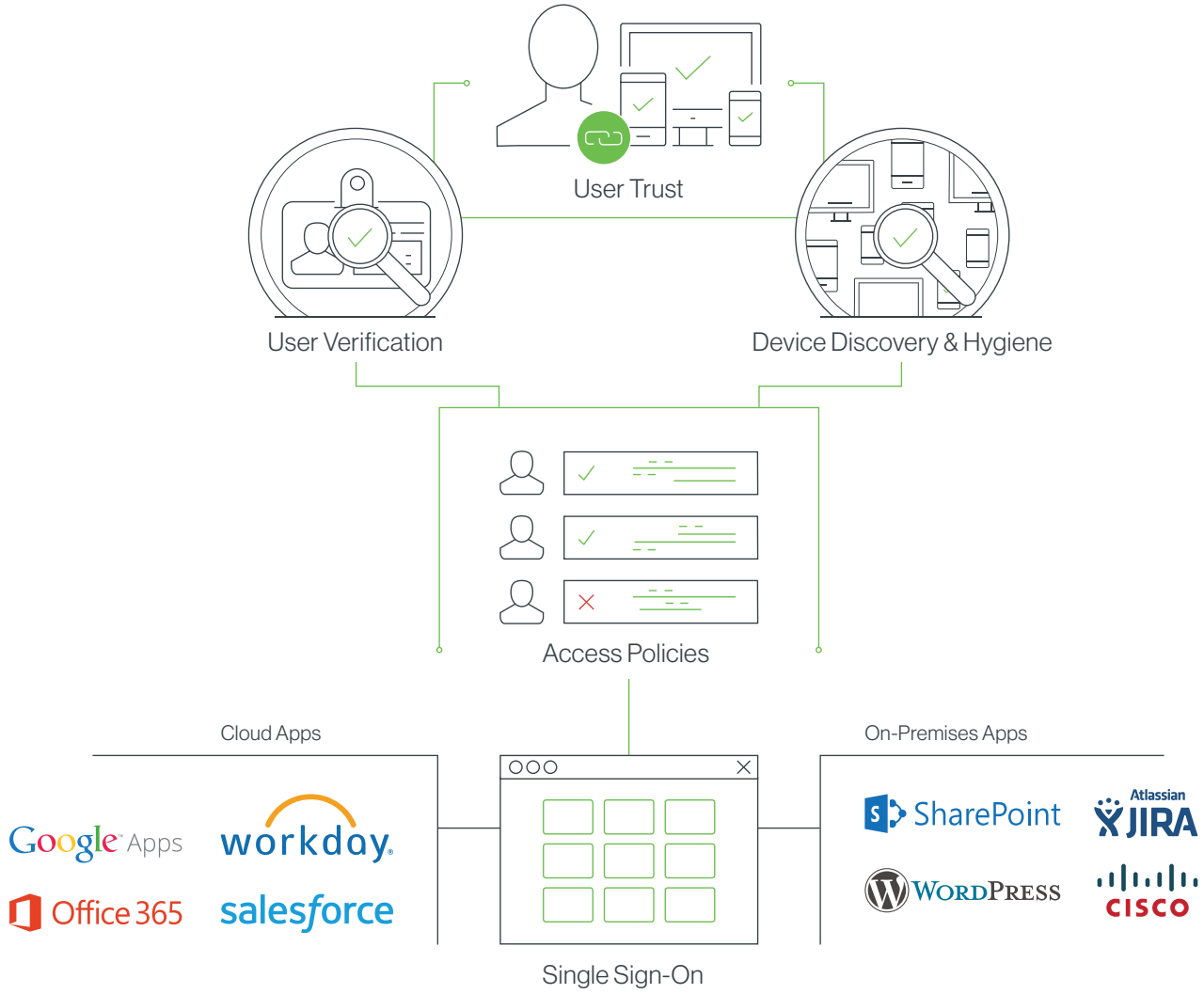
[3] ***Almost All WannaCry Victims Were Running Windows 7***; The Verge; May 19, 2017

[4] ***Google Chrome: Flash Usage Declines from 80% in 2014 to Under 8% Today***; BleepingComputer.com; Feb. 28, 2018



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**