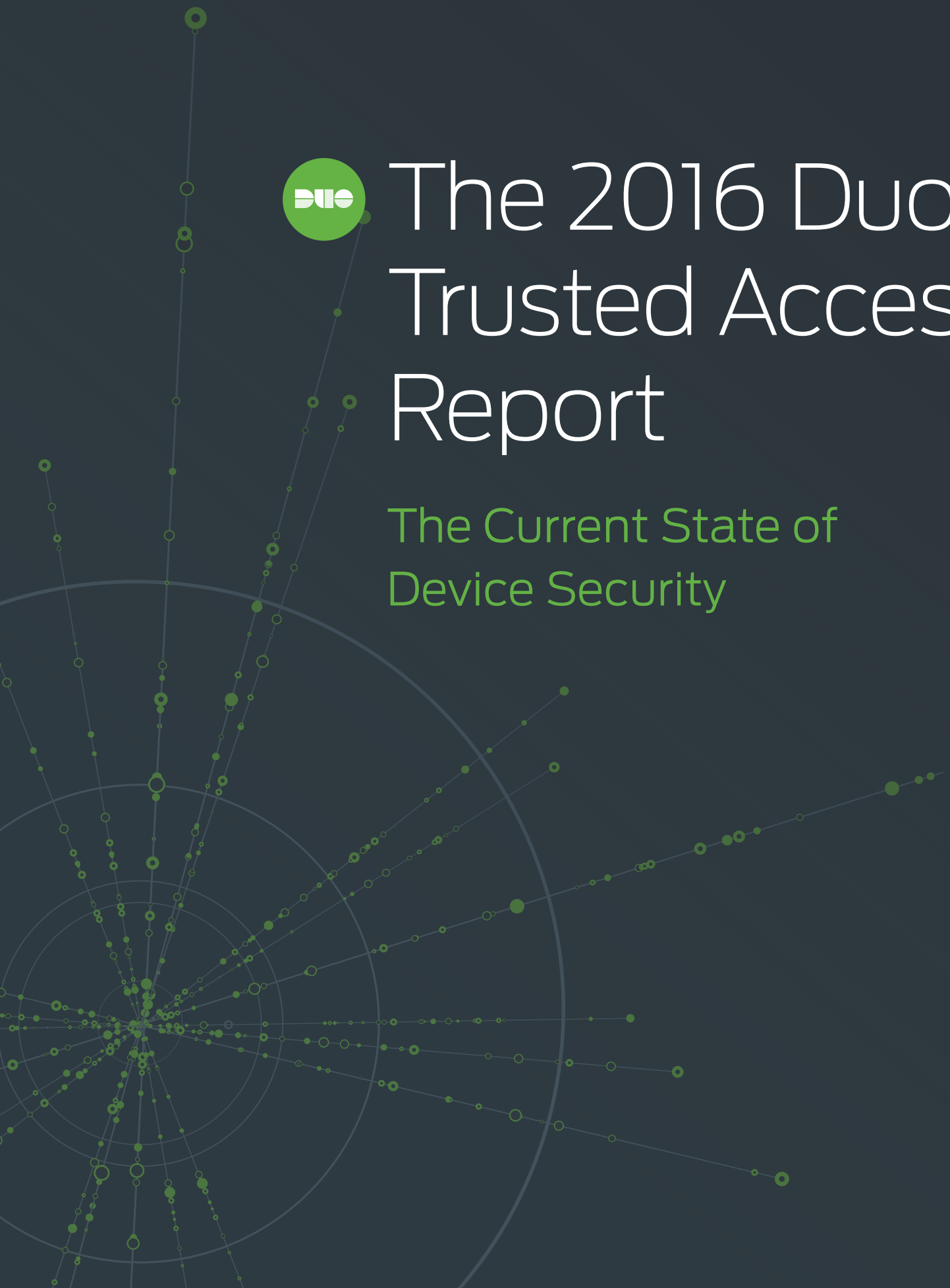
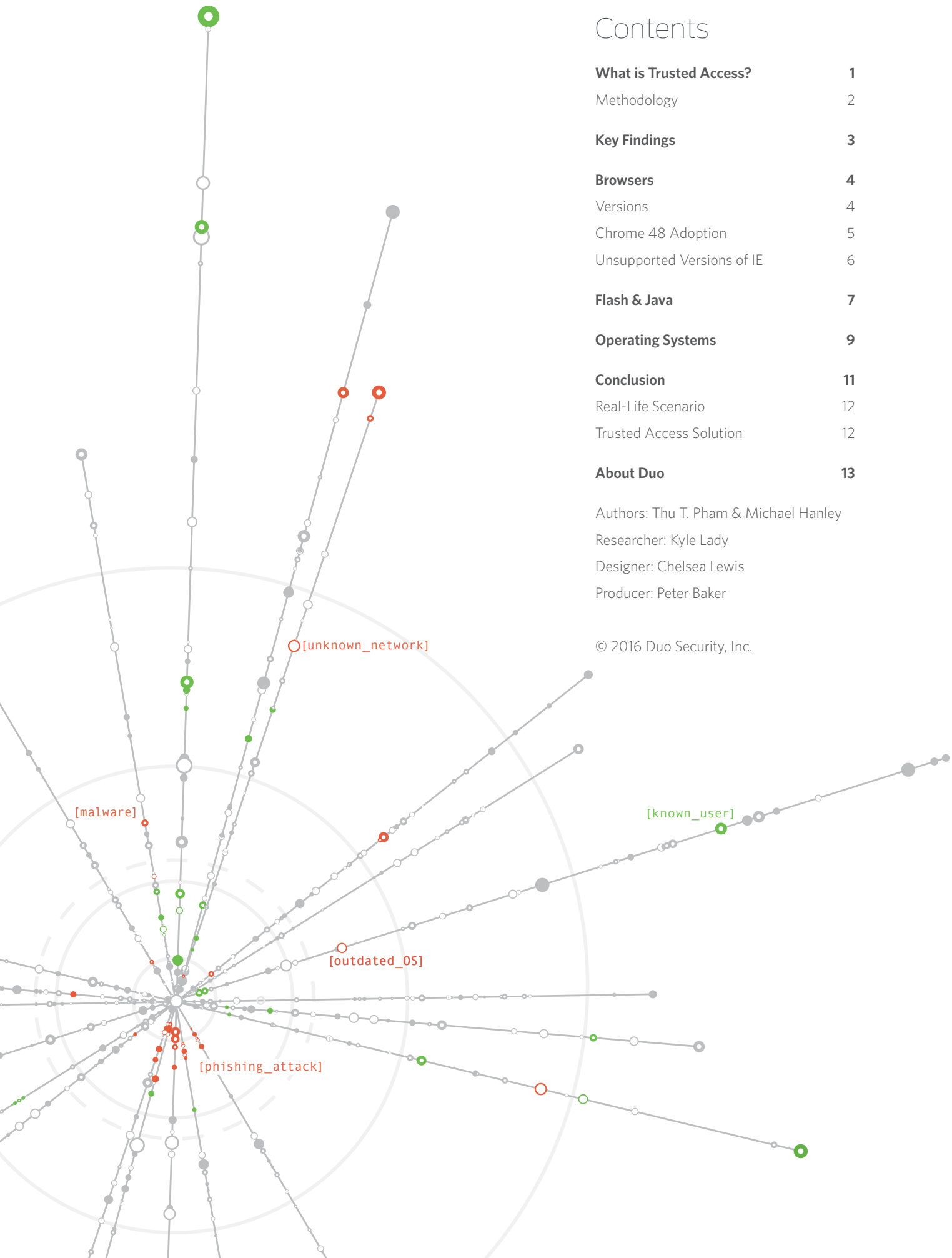


The 2016 Duo Trusted Access Report

The Current State of Device Security



Contents

Authors: Thu T. Pham & Michael Hanley
Researcher: Kyle Lady
Designer: Chelsea Lewis
Producer: Peter Baker

What is Trusted Access?

An in-depth analysis of the security health of millions of devices and what kind of risk they may bring to companies, based on Duo's dataset of 2,000,000 devices worldwide.

Defining the New IT Model

Traditionally, users worked from the office on IT-managed workstations, accessing on-premises applications and systems hosted in data centers. Today, users work from anywhere. Different locations, personal devices, and an increasingly mobile experience all accelerate our adoption of a new IT model where there is simply no defined network perimeter.

At the same time, new threats have evolved to match this model, often relying not on zero-days, but instead on compromising outdated devices with known vulnerabilities, or social engineering user credentials. Attackers are targeting end users and their devices directly. Oftentimes, IT departments don't have visibility into these targeted users' devices at all, making it difficult to protect access to data in the cloud with traditional perimeter-focused security solutions.

Securing the New IT Model

To secure everything in this new IT model, we've developed Trusted Access solutions to verify the trust of both users and devices before granting access to business applications. Instead of gaining complete control over user devices, we believe in helping IT administrators and their users work through establishing device health and trust together by providing both strong authentication and visibility into cloud apps, as well as the ability to create policies to prevent access from outdated devices.

This report uses Duo's dataset of more than 2 million devices used by businesses worldwide. We reviewed device, operating system, browser and plugin usage to offer insight into the current state of Trusted Access, and the security health of devices connecting to business applications.

Methodology

How did Duo Security prepare this report?

Our security research team, Duo Labs, analyzed our dataset of more than 2 million devices used by businesses located worldwide to learn more about the current state of device security health.

This report uses data collected from devices performing over 2 million authentications per day using Duo's two-factor authentication to securely log into thousands of applications and services. Our customers span every industry and size, ranging from small startups to Fortune 500 enterprises.

In addition to providing secure authentication, Duo's endpoint visibility solution includes a Device Insight feature that collects data about devices, including details about OS, browser, Java and Flash versions via our Duo Mobile application and web-based authentication prompt. This report details findings about the security health of our users' devices.

2,000,000

DEVICES

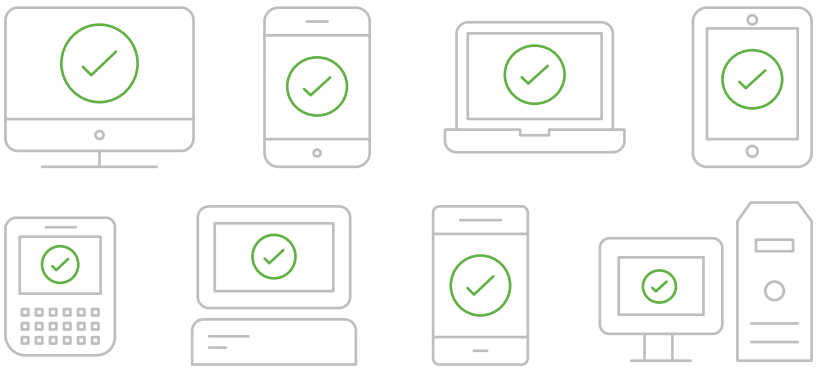
2,000,000

AUTHENTICATIONS DAILY

SMALL STARTUPS TO FORTUNE 500 ENTERPRISES

Devices Analyzed

Any user or IT-owned laptop, PC, mobile phone and tablet authenticating with Duo's two-factor authentication.



Key Findings

A quarter of all Windows devices are running outdated and unsupported versions of IE.

Twenty-five percent of Windows devices are running an outdated and unsupported version of Internet Explorer (IE). Half of all Windows XP devices are running either IE 8 or 7. This may expose unpatched Windows users to more than 700 known vulnerabilities (number includes ones that affect IE 11 and Edge).

Google's Chrome browser is the most up-to-date browser among our sample size.

Eighty-two percent of Chrome users are up to date, compared to 58 percent of Edge and IE 11 users, and 66 percent of Firefox users. Chrome users may be more up to date than other browsers since Google rolls out updates and new versions automatically to Chrome, without required approval from the user.

60% of Flash users and 72% of Java users are running an outdated version.

Flash and Java are notorious targets, used by attackers in exploit kits to gain access to their machines. While critical Flash and Java vulnerabilities often prompt emergency vendor patches, users still run outdated software on the devices used to log into their company applications that can put entire organizations at risk.

Mac users are more up to date than Windows users when it comes to operating systems.

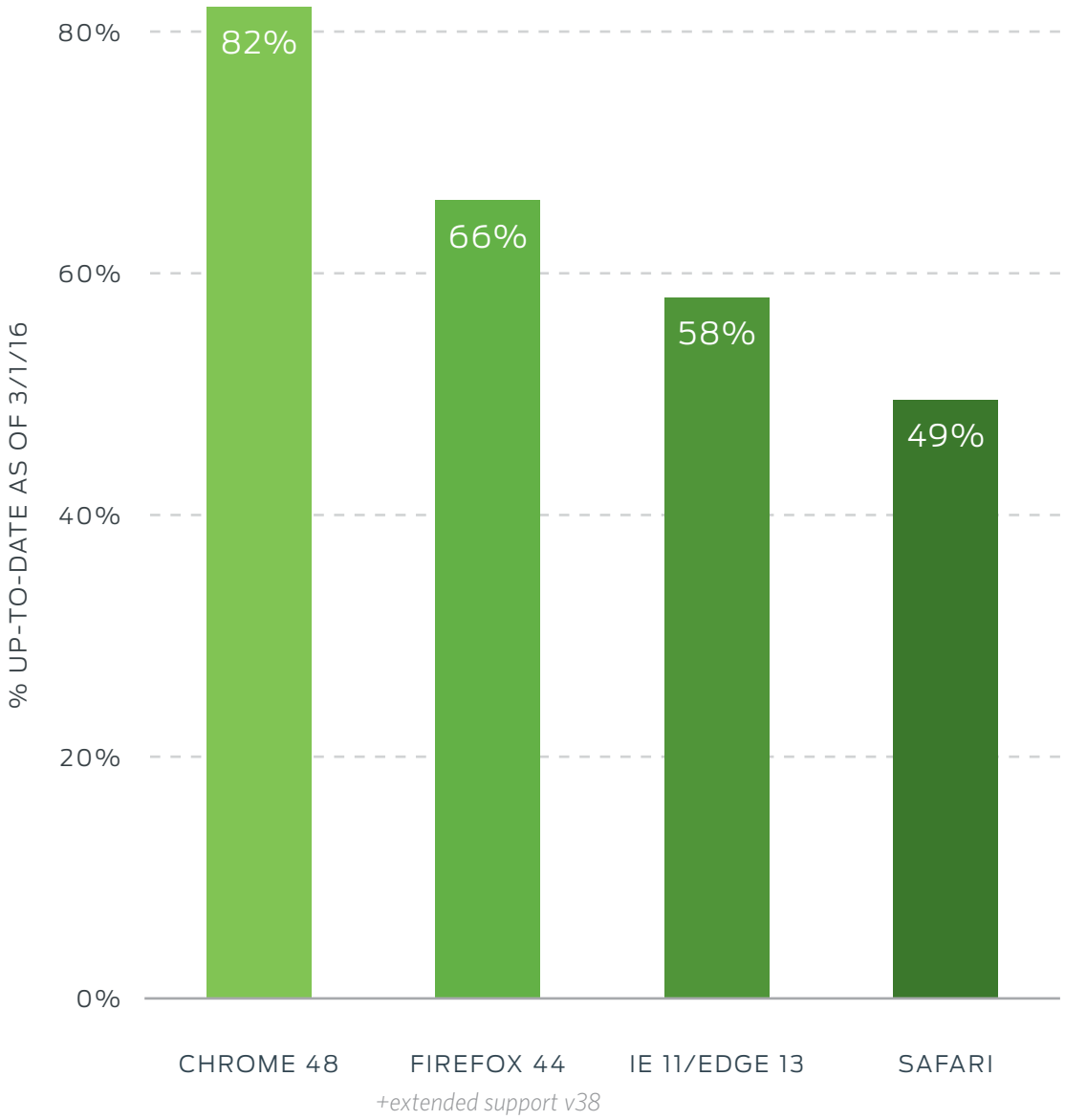
Apple users may be more likely to update their OS because these updates have been known to be more stable than Windows updates; new OS X versions are also free and heavily promoted. Historically, major Windows updates have a reputation for causing major problems — sometimes even the blue screen of death.

Browsers

Chrome Users Are Most Up to Date

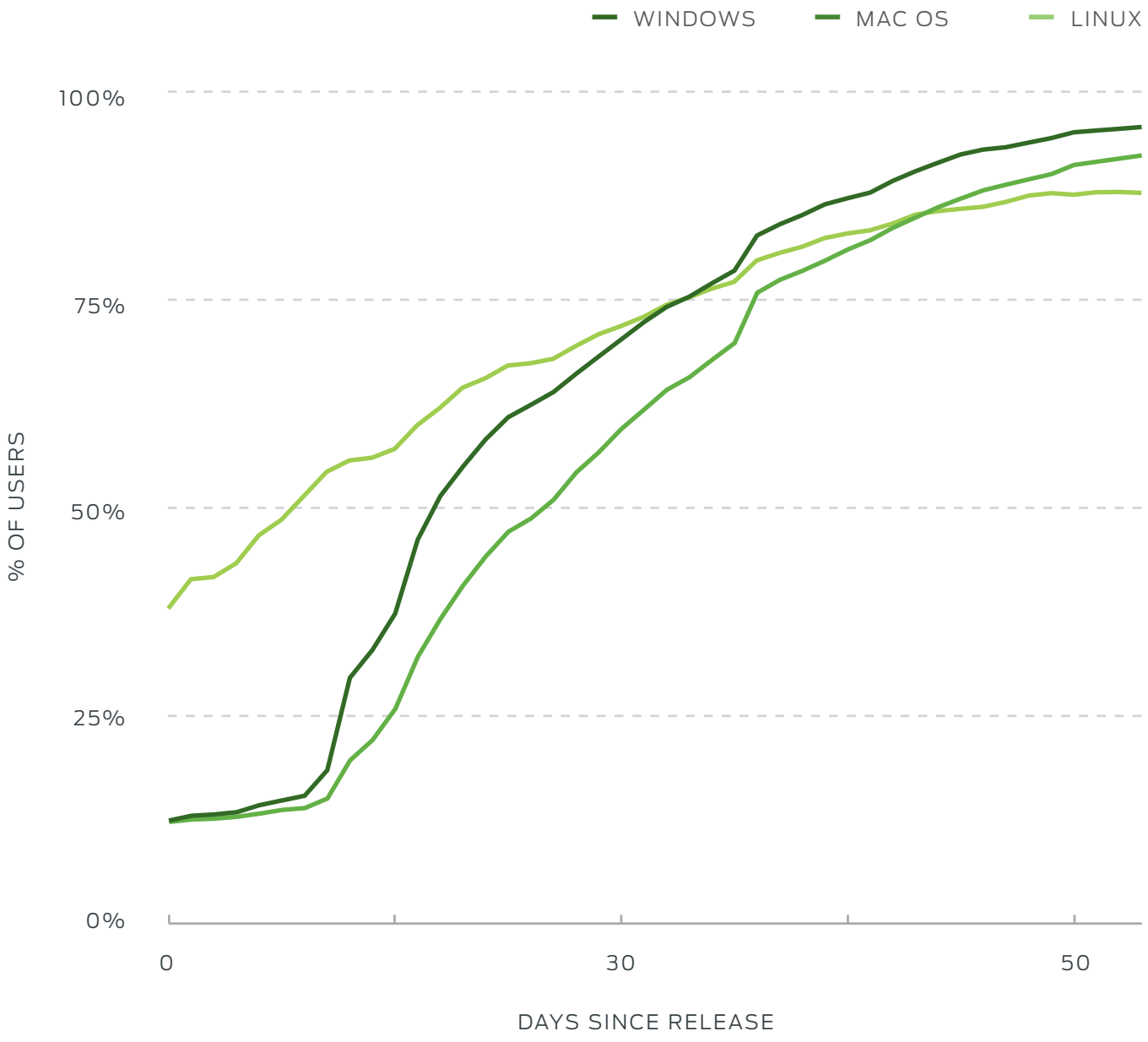
Google's Chrome browser is the most up-to-date browser among our sample size, likely due to automatic, timely updates.

Chrome users bypass Firefox (66 percent), IE 11/Edge (58 percent) and Safari (49 percent) users in the race to update at 82 percent.



Chrome 48 Adoption

When it came to the percent of users across different platforms that updated to the latest version of Chrome after a new version was released, we found that Linux users take longer to update.

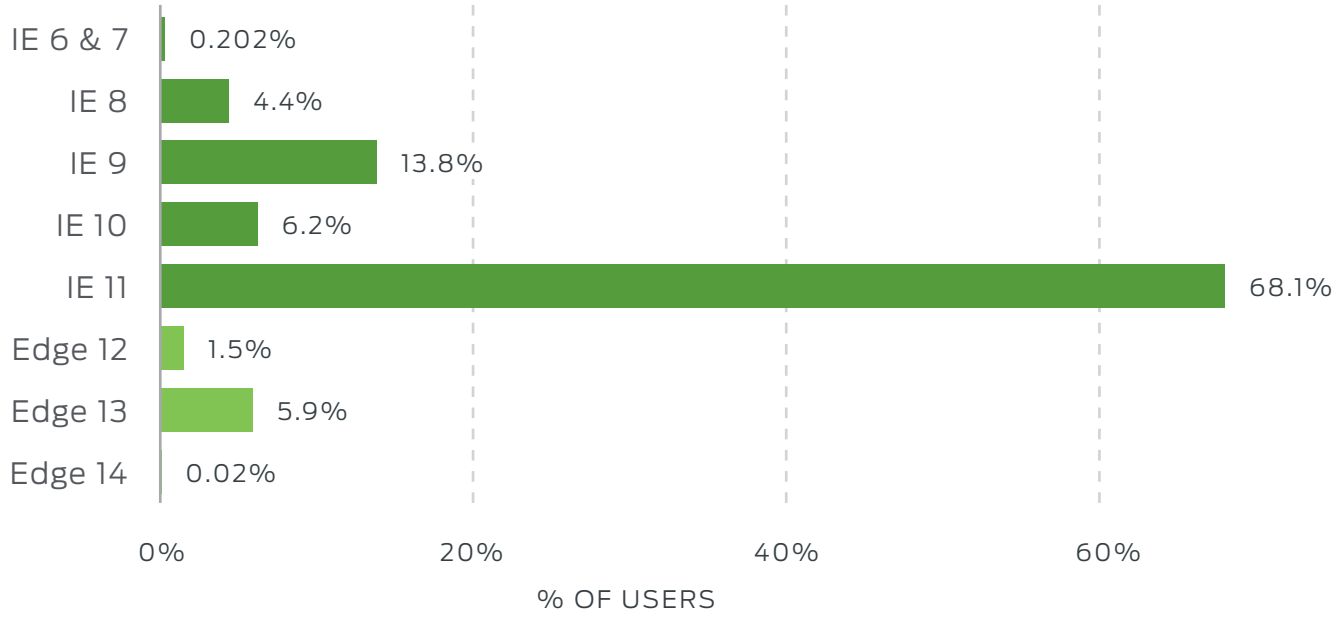


Unsupported Versions of Internet Explorer

However, nearly 40 percent of Windows XP devices are running IE 8, and another 10 percent is running IE 7. This is compared to 68 percent of overall Windows devices that are running the latest version of IE 11 or Edge 12/13. Another 25 percent of all Windows devices are running an outdated version of IE 10 or prior.

WINDOWS XP ONLY

ALL WINDOWS DEVICES



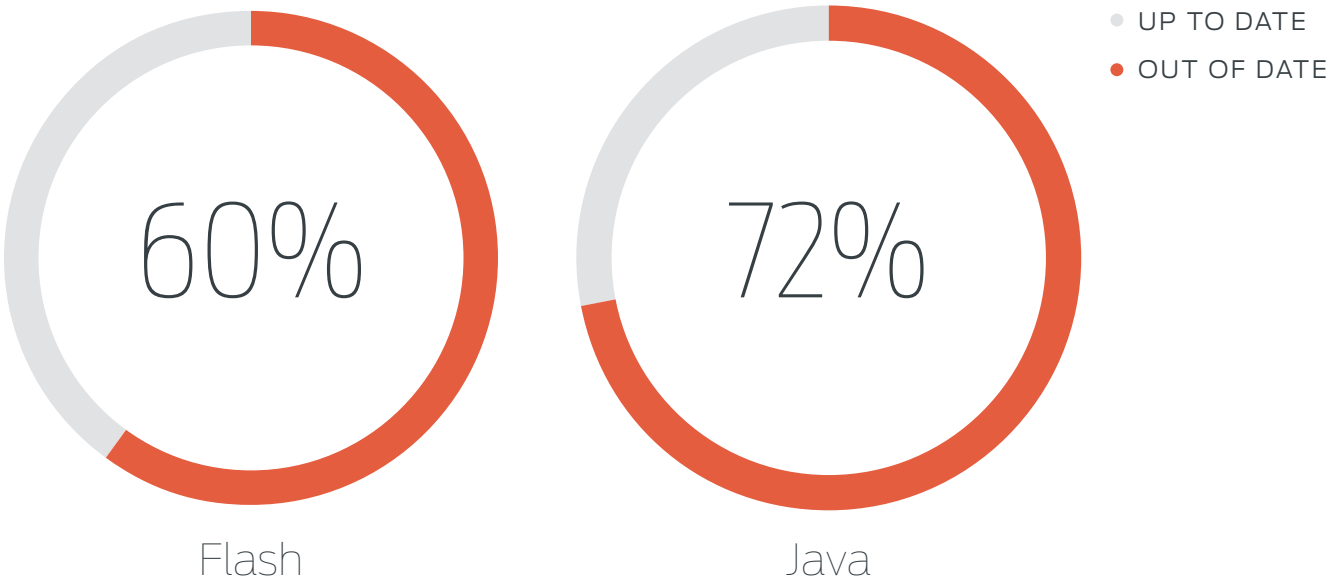
WINDOWS XP VULNERABILITIES LIVE ON

Windows XP is no longer supported by Microsoft, meaning the OS no longer receives security updates. Early this year, Microsoft announced the end of life support for versions IE 10 and prior. That means these browsers aren't protected against new vulnerabilities and exploits, which could put companies at risk if these browsers are used to access work applications.

Google's Chrome browser rolls out updates automatically to their users, making it easier to stay up to date and protected against the latest vulnerabilities. Chrome also blocks Flash advertisements by default, which can reduce the risk of malware infection.

Flash & Java

Most devices running browser plugins are running an out-of-date version, exposing them to hundreds of vulnerabilities.



FLASH: STILL A BIG TARGET

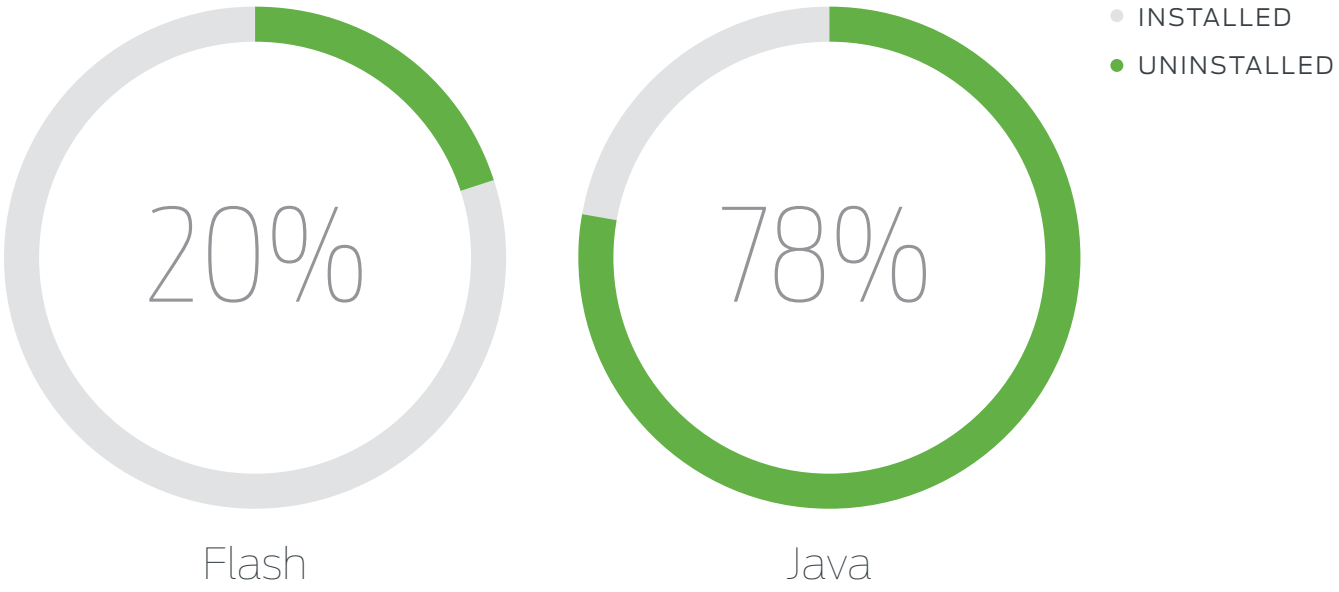
Adobe Flash is notoriously susceptible to many very critical and prolific vulnerabilities — over 300 were reported in 2015 alone. Eight out of the top 10 vulnerabilities employed by exploit kits (software used for malicious hacking) this year targeted Flash.

If just one device on your network is running an outdated version of Flash, they could be exploited to run malware your company's apps and systems, allowing them to steal confidential data from your company.

Flash & Java (cont.)

Uninstall Rates of Java vs. Flash

At 78 percent, most devices have Java uninstalled on their browsers, compared to only 20 percent of devices with Flash uninstalled.



DEPRECATING THE JAVA PLUGIN

The higher percentage of devices with Java uninstalled may be attributed to Oracle's plans to deprecate the plugin in its JDK 9 update. This is in step with many browser vendors that have removed or announced timelines to remove plugin support.

Another contributing factor may be that Java is no longer a default install for browsers, and users can do without Java when using web applications.

Operating Systems

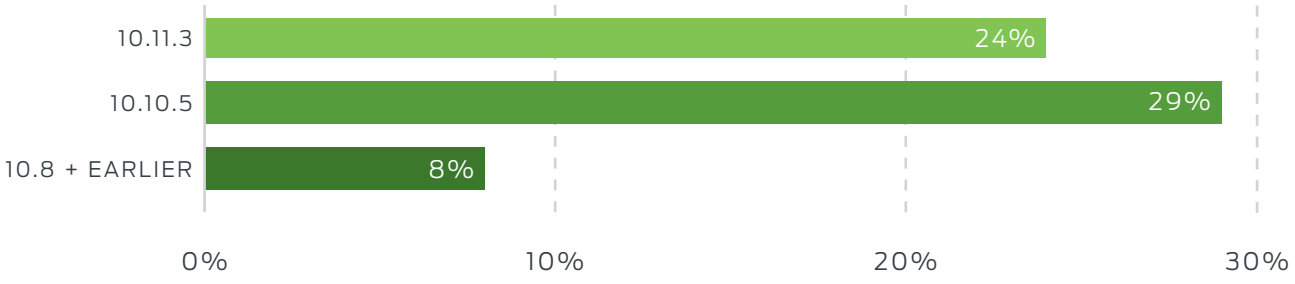
Mac users are more up to date than Windows users when it comes to operating systems.

Mac OS vs. Windows

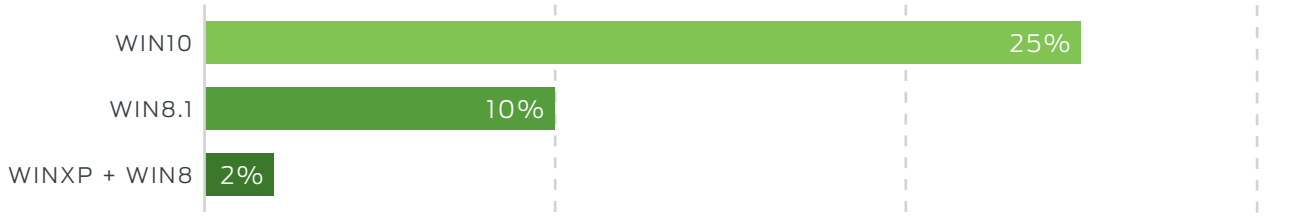
Fifty-three percent of Mac OS users are running either the fully patched, latest version of OS X, or the previous version, compared to 35% of Windows users on Windows 10 and 8.1.

However, 8% of Apple users are running unsupported versions of OS X that cannot receive security updates — 10.8 and earlier. That's compared to 2% of Windows users running unsupported OS versions, including Windows 8 and XP.

MAC OS



WINDOWS



- FULLY-PATCHED, LATEST VERSION
- ONE PREVIOUS VERSION
- UNSUPPORTED VERSIONS/NOT RECEIVING SECURITY UPDATES

VULNERABILITIES AFFECTING OUTDATED OS VERSIONS

Running an outdated and unpatched OS can expose your company to vulnerabilities that target older versions of OS X and Windows.

DYLD_PRINT_TO_FILE is a privilege escalation vulnerability that may allow malware to gain root access to a Mac. It affects OS X Yosemite versions prior to 10.10.5 and has been observed being used actively in the wild. This is just one of over a thousand reported OS X vulnerabilities.

Gaining root access to a managed or unmanaged device allows an attacker to access your data, and potentially your company's data. Updating on a timely basis can reduce this risk.

Conclusion

Duo's security recommendations on how to secure your data and apps, while verifying the trust of your users and devices.

The changing security landscape and rapid adoption of cloud apps necessitates an increased emphasis on security hygiene basics. With any device accessing data from any location, establishing and maintaining the health of these devices is critical, in addition to strongly attesting that the user is who they say they are.

Our data indicates a high rate of out-of-date and vulnerable endpoints that can expose your company's apps and data to malware, credential theft, and a potential data breach. How can your company secure your data and apps in time when the perimeter is disappearing, and verify the trust of users and devices before they connect? We recommend:

- **Don't reject BYOD — be prepared for it.** Give your IT administrators actionable data on device ownership and health that can inform risk-based access control decisions.
- **Encourage safe computing practices and good security hygiene**, such as running regular security updates or using device encryption, passcodes and additional authentication to protect systems and data.
- **Configure systems and deploy policies that enable automatic updates** for as much software as possible to remove some of the friction that users feel when manually installing updates. We found that an overwhelming number of out-of-date browsers and systems don't take basic steps like enabling automatic updates.
- **Switch to browser platforms that update** more frequently and automatically, like Google Chrome.
- **Disable Java and prevent Flash** from running automatically on corporate devices, and enforce this on user-owned devices through endpoint access policies and controls.

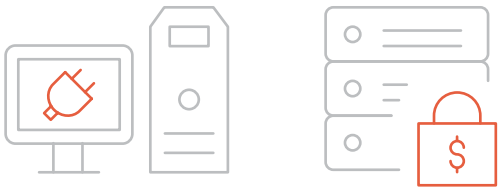
Duo also recommends the use of a Trusted Access solution with both strong authentication and endpoint visibility features to verify both users and devices. Find out why in a real breach scenario below — and how a Trusted Access solution can stop this type of attack.

Real-Life Scenario

Why is Trusted Access important?

Here's an example of a real-world scenario detailing how an outdated device could put your company at risk:

Many hospitals running Windows PCs with out-of-date Flash are getting exploited by ransomware. Attackers are targeting older versions of Flash with known vulnerabilities in order to encrypt all data on the PC (and any local systems networked to the computer).



Some attackers back up the data, delete the original, and then encrypt the backup, holding it for hostage until the hospitals pay ransom. The ransomware is also exploiting known vulnerabilities in outdated browsers like Internet Explorer and operating systems like Windows in order to spread itself to other workstations and servers on the network.

Without access to critical data and systems, these hospitals often must shut down for days in attempts to recover data and remove malware.

Trusted Access Solution

Protecting against a data breach or malware infection due to outdated devices requires a Trusted Access solution that ensures the trust of both the user and their device.

Trust of Users

Employ two-factor authentication that requires two forms of identification verification. One is a username and password, the second requires physical possession of their smartphone.

Ensuring the user is who they say they are is the first step of a Trusted Access solution.

Trust of Devices

Employ endpoint visibility solutions to ensure the security and trust of your users' devices before they connect to your company network.

Invest in endpoint protection that gives you:

- Insight into every mobile, tablet, PC or laptop accessing your company apps
- Ability to notify users when their devices are out of date and provide resources to update
- Ability to create policies to warn and block users from accessing your apps with outdated devices to keep your company data secure

Have questions about Duo's Trusted Access Report? Feel free to contact labs@duosecurity.com, send Duo a message, or tweet @duosec or @duo_labs, #TrustedAccess.

About Duo

Duo Security is a cloud-based trusted access provider protecting the world's fastest-growing companies and thousands of organizations worldwide, including Dresser-Rand Group, Etsy, Facebook, K-Swiss, Paramount Pictures, Random House, SuddenLink, Toyota, Twitter, Yelp, Zillow, and more. Duo Security's innovative and easy-to-use technology can be quickly deployed to protect users, data, and applications from breaches, credential theft and account takeover. Duo Security is backed by Benchmark, Google Ventures, Radar Partners, Redpoint Ventures and True Ventures. Try it for free at duo.com.

866.760.4247

duo.com