The 2016 Duo
Trusted Access Report: Microsoft Edition

The Current State of Device Security Health

Duo Security is
now part of Cisco.

AUTHOR
THU T. PHAM

RESEARCHER
KYLE LADY

DESIGNER
CHELSEA LEWIS

PRODUCER
PETER BAKER

"In the past, we built security for networks and systems. But now, **we have to build security for people.**"

Dug Song
CEO & Co-Founder, Duo Security

Securing Against Device and User-Targeted Attacks

The traditional security perimeter no longer exists – data and applications are stored in the cloud, and users are bringing their own devices to work, making it difficult for administrators to maintain insight and control.

"*The status quo isn't working – unfortunately, users' devices aren't safe. In addition to unsafe devices, credentials are still king for gaining access to systems with sensitive company data. We're failing at the fundamentals in an age of access, as we increasingly see our data spanning not only infrastructure we own, but a lot that we don't. We don't know who's accessing what, and how.*

In the past, we built security for networks and systems. But now, we have to build security for people."

Dug Song
CEO & Co-Founder, Duo Security

HOW SECURE ARE THE DEVICES ACCESSING YOUR APPLICATIONS?

It takes just one out-of-date device to compromise your entire organization – attackers will target devices with exploitable, older versions of software in order to steal your data.

IN AN ANALYSIS OF DUO'S DATASET, WE FOUND THAT:

- Sixty-five percent of all Windows devices are running an old version of the Microsoft operating system, Windows 7.

- We also found that nearly 62 percent of devices running the Internet Explorer browser have an out-of-date version of Flash installed.

That leaves the majority of users on Microsoft operating systems and browsers open to vulnerabilities and a potential malware infection, which can be passed onto your environment if they log into your applications with risky devices.

The disclosure of high-severity vulnerabilities has increased 42% across the industry in 2015, according to Microsoft's Security Intelligence Report (SIR) report.[1] The chances of malware infection and compromise is greater among devices with out-of-date software, like operating systems, browsers and plugins like Flash and Java.

Additionally, user-centric attacks like phishing and other password theft attempts, as well as attacks against their devices have proved successful time and time again. Microsoft reported that they detected more than 10 million daily attacks, including millions of attacks in which the attacker had valid credentials.

Attackers can exploit many different vulnerabilities in multiple vectors. In a single attack, attackers may both steal credentials and exploit outdated software to gain access to your data. Traditional security solutions are designed to address separate, siloed attacks, making these solutions ineffective against modern threats.

What is Trusted Access?

Protecting your users, devices and access to applications requires a modern, holistic security approach that can give you insight, prevention and remediation in all three areas to effectively prevent a breach.

"More than ever before, employees are working from devices and locations that are not corporate-owned or managed. This shift, enabled by the adoption of cloud and mobile, must be embraced by organizations to enable productivity while maintaining security. The era of the network perimeter and network-centric security controls is over, and it's time to rethink traditional security controls. After all, you can't drop a firewall in front of Salesforce!

In this new world, the most critical aspect of an organization's security program is securing access. This requires a security model where your users are strongly authenticated, their devices are secure and trustworthy, and you can protect access to all of your corporate applications, whether they're cloud-based, on-premises or hybrid. At Duo, we call this new security model Trusted Access, and it's how many of the most progressive organizations are re-architecting and modernizing their security programs."

Jon Oberheide
CTO & Co-Founder, Duo Security

Duo's Trusted Access platform brings a holistic approach to security in order to ensure the trust of your users, devices and applications by verifying the identity of your users and the security health of their devices before they connect to the applications you want them to access.

Duo's Trusted Access platform can be used to protect every application in a hybrid environment – both Microsoft on-premises and cloud-based services during the migration.

With the data collected by our service, we can inform administrators on how to enforce more granular access controls and policies to limit access based on user identity verification and device security health.

"The era of the network perimeter and network-centric security controls is over, and **it's time to rethink traditional security controls.**"

Jon Oberheide
CTO & Co-Founder, Duo Security

Key Findings

OPERATING SYSTEMS

Of all Windows devices analyzed, 65% are running Windows 7, released in 2009.

More than half of all devices analyzed are running Windows OS (63%) – but most are running Windows 7, meaning that most Windows-based laptops, PCs and tablets used to access work applications are missing important security features only available on Windows 10.

BROWSERS

20% of devices running IE are running unsupported versions 8, 9 and 10.

IE versions 8 – 10 have reached end-of-life status without the ability to receive security patches, leaving them susceptible to old exploits. Of the devices running IE in our dataset (29%), 80% are using IE 11 and only 3% are using the latest Windows browser, Edge.

FLASH

Nearly 62% of devices running IE have an old version of Flash installed.

Only 38% of devices running the Internet Explorer browser had the latest version of Adobe Flash Player, compared to 89% of devices running Chrome and 67% on Edge. But that still leaves many IE users open to numerous critical Flash security flaws that could lead to data leaks.

JAVA

98% of devices running IE have Java installed.

In July, the most critical updates released by Oracle was for Java.[2] One flaw, CVE-2016-0636 can be triggered remotely without authentication – an attacker merely has to set up a malicious web page, then trick the user into visiting the page in order to compromise their device.[3]

MICROSOFT APPLICATIONS

The most popular Microsoft remote access services include RDP, OWA and RD Gateway.

Of all of the Microsoft services integrated with Duo's two-factor solution, we found that 62% were Remote Desktop Protocol, 15% Outlook Web Access and 10% Remote Desktop Gateway. By industry, we found that the highest number of authentications into Microsoft services were found in Shipping (98%), Communications (91%) and Nonprofit (89%), according to our customer dataset.

Methodology

HOW DID DUO PREPARE THIS REPORT?

To analyze the current state of device security health among our customers, Duo Security dove deep into our dataset of more than two million devices, 63% of which are running Microsoft operating systems. We also analyzed 18,000 Microsoft integrations in our dataset and millions of endpoints.

63%

Of Duo Endpoints Run Microsoft Operating Systems
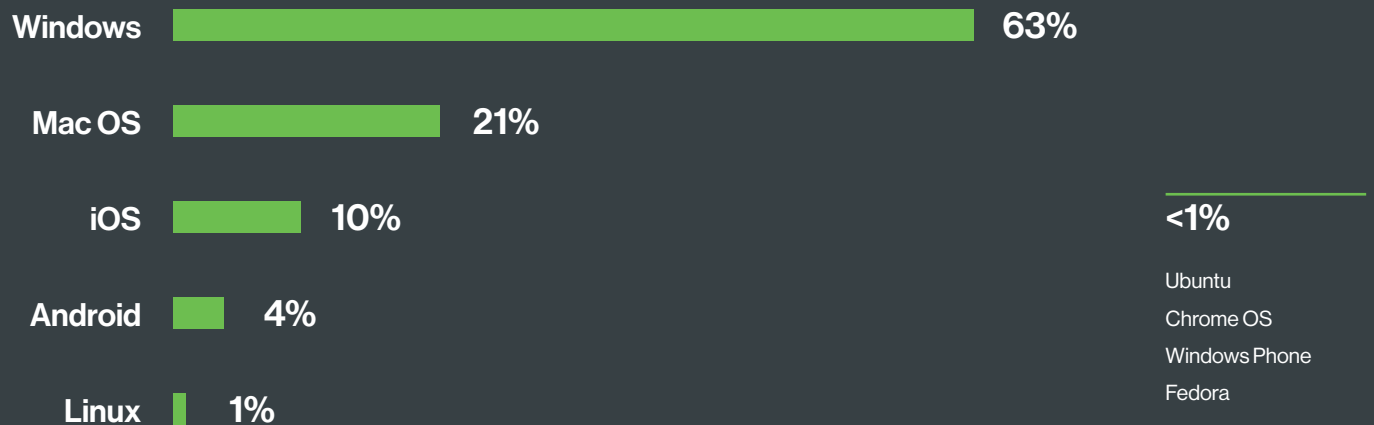
18,000

Microsoft Integrations Analyzed
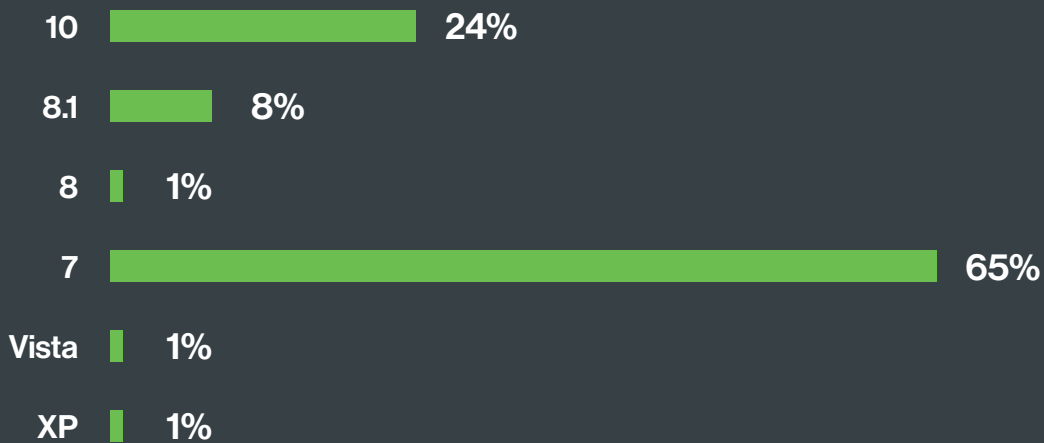
01 Operating Systems

Of all Windows devices analyzed, 65 percent are running Windows 7, released in 2009.

The majority of all devices analyzed are running Windows OS (63%), compared to Mac OS X (21%) and iOS (10%). But most of those Windows devices are running the older OS version, Windows 7. While Windows 7 is receiving extended support and new security patches, it will reach an end very soon.

OPERATING SYSTEMS

Windows	63%
Mac OS	21%
iOS	10%
Android	4%
Linux	1%

<1%

Ubuntu
Chrome OS
Windows Phone
Fedora

WINDOWS VERSIONS

10	24%
8.1	8%
8	1%
7	65%
Vista	1%
XP	1%

That means the majority of Windows-based laptops, PCs and tablets used to access work applications lack some of the advanced security features available on newer Windows client versions, leaving them more susceptible to a potential exploit. With nearly 600 total vulnerabilities affecting Windows 7, these devices have a greater chance of getting compromised.[4]

Some of the features in the latest version, Windows 10, include virtualization-based security (VBS) that vastly reduces the attack surface area, secure booting, better sandboxing and more.[5] Updating to the latest OS can better protect users and their devices against the latest threats.

600
vulnerabilities
affect Windows 7.

WHY ARE WE
OUT-OF-DATE?

THERE ARE MANY REASONS:

- Companies are running older applications that rely on older versions of Windows operating systems

- It can be time-consuming to update user devices and desktop operating systems

- Older hardware may not be compatible with newer operating systems

THERE ARE MANY SECURITY IMPLICATIONS:

- Nearly 600 known Windows 7 vulnerabilities affecting unpatched devices

- On older Windows versions, there is no default disk encryption to protect data on lost devices

- And no file-level encryption to protect data as it leaves the corporate network

- Plus no malware protection, as offered in Windows 10 through VBS, Device Guard, Microsoft Edge and more

Windows XP Lives On
(15 Years Later)

We also found that tens of thousands of endpoints we analyzed are still running Windows XP and the browser IE 7 & 8, which no longer receive security updates. Released in 2001, Windows XP has over 700 reported vulnerabilities, with over 200 rated as high-to-critical severity, using the Common Vulnerability Scoring System (CVSS) industry standard for scoring vulnerabilities.[6]

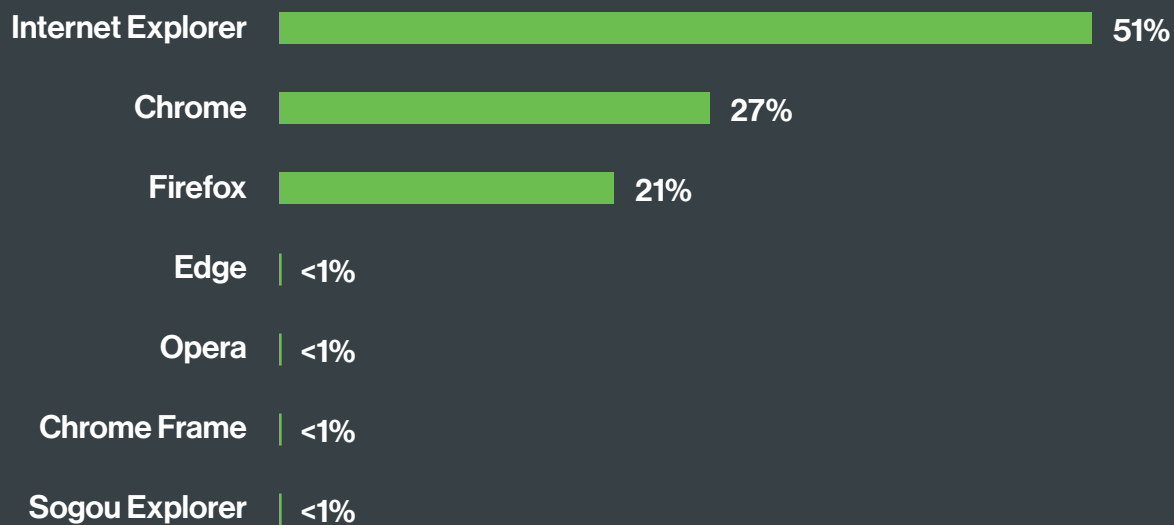According to Microsoft's support article, *Windows XP Support Has Ended*:

If you continue to use Windows XP now that support has ended, your computer will still work but it might become more vulnerable to security risks and viruses. Internet Explorer 8 is also no longer supported, so if your Windows XP PC is connected to the Internet and you use

Internet Explorer 8 to surf the web, you might be exposing your PC to additional threats. Also, as more software and hardware manufacturers continue to optimize for more recent versions of Windows, you can expect to encounter more apps and devices that do not work with Windows XP.[7]

— Microsoft

Finally, a very small sample of our mobile devices are Windows Phones. Sixty-three percent of those endpoints are running version 8.1 (Windows Phone versions mirror desktop versions), and therefore are out of date. When it comes to phones that have the **Duo Mobile** app installed for **two-factor authentication,** we found that 42% of those Windows Phone users are on the latest OS version 10.0.

WINDOWS XP BROWSERS

Browser	Percentage
Internet Explorer	51%
Chrome	27%
Firefox	21%
Edge	<1%
Opera	<1%
Chrome Frame	<1%
Sogou Explorer	<1%

Windows XP has over
700
vulnerabilities, with over
200
rated as high-to-critical.

BREACHED DUE TO
WINDOWS XP EXPLOIT

Some accredit the massive Target breach to a decade-old exploit in Windows XP Embedded, used in their point-of-sale systems, which was also used by many other large franchisors and retailers to power their POS systems.[8]

Specific malware for embedded XP systems used a RAM (random-access memory) scraping technique to steal customer data from retailers, attacking XP's weak memory access protection.

For large retailers, it would take months if not years to deploy and test new POS systems at thousands of stores.

Browsers

Twenty percent of devices running IE are running unsupported versions 8, 9 and 10.

We found that 29% of all devices in our dataset are running Internet Explorer (IE). Of those devices, 80% are using IE 11, and only 3% are using Edge, showing slow adoption of the newest Windows browser.

BROWSER FAMILIES

Browser	Percentage
Chrome	36%
Internet Explorer	29%
Firefox	12%
Safari	7%
Edge	3%
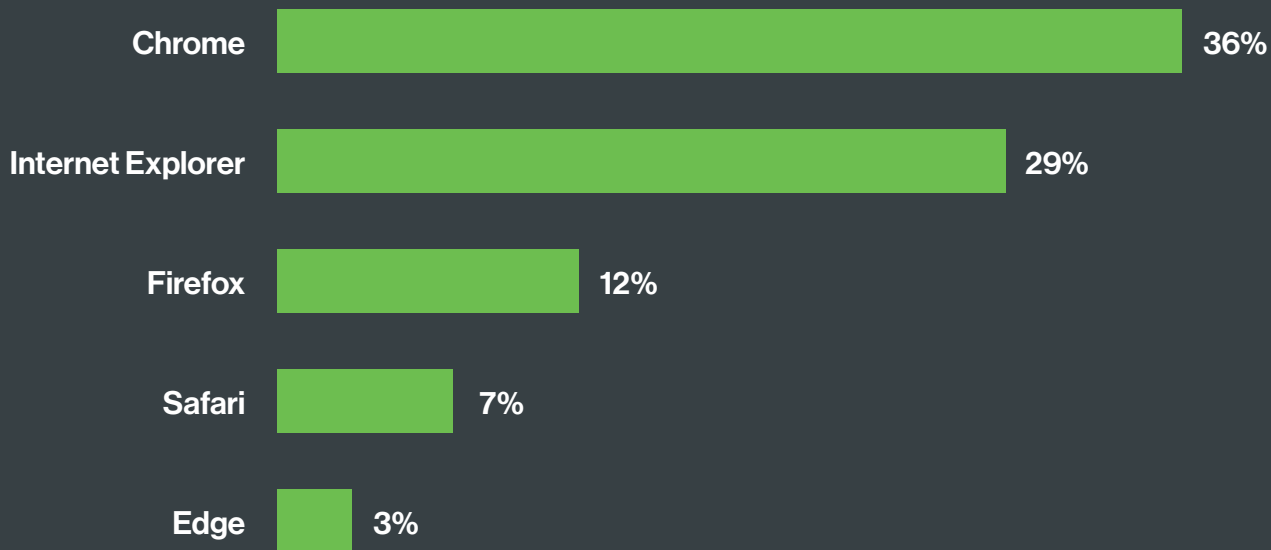
The dominant browser platform is Chrome (36%), followed by Firefox (12%). Google's Chrome checks regularly to ensure it's always kept up to date on your devices, and updates itself with the latest security features without any user interaction required, aside from restarting the browser.[9]

Edge is running on only 3% of Microsoft endpoints.

INTERNET EXPLORER VERSIONS

| Version		
11.0	████████████████	80%
10.0	█	5%
9.11	▏	2%
9.0	██	9%
8.0	█	4%
7.0	▏	<1%
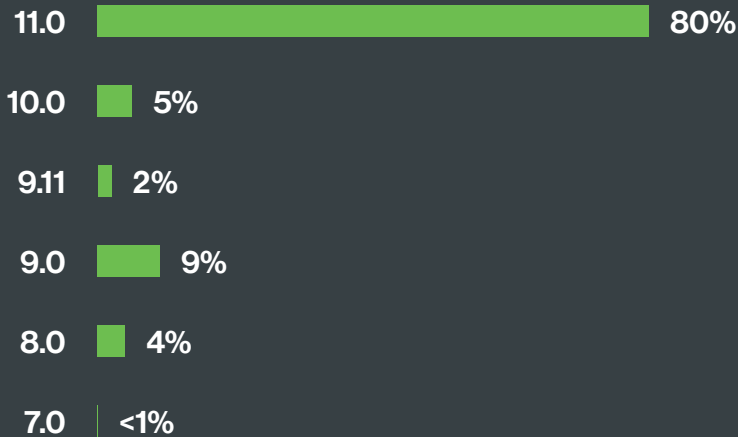
20% of IE devices are running a version that has reached end-of-life status, unable to receive security patches – most IE users are running very old and outdated versions. This has, however, improved since January 2016 – back then, our data showed that 44% of Microsoft browser users were running IE 8, 9, or 10.[10]

WHAT'S THE IMPACT
OF IE VULNERABILITIES?

Many of the vulnerabilities that affect older versions of IE include remote code execution, elevation of privilege, information disclosure and security feature bypass – all of which could put your users machines at risk of a data breach or compromise.

In a security bulletin published in August, Microsoft stated that the most severe of the vulnerabilities listed could allow an attacker to execute code and gain the same rights as the current user, including administrative rights – allowing them to view, change or delete data, or create new accounts.

INTERNET EXPLORER VERSIONS ON WINDOWS XP

Version		
11.0	█	1%
10.0	▏	<1%
9.11	▏	<1%
9.0	▏	<1%
8.0	█████████████████	88%
7.0	██	10%
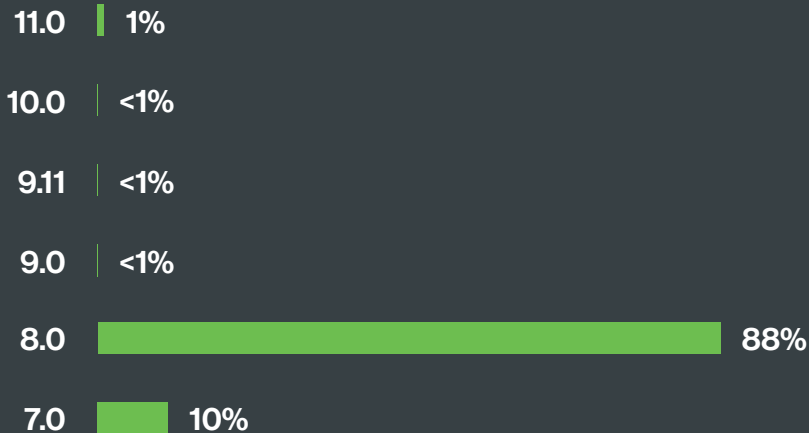
Of the 1% of our endpoints that are still running Windows XP, 88% of them are running IE 8, while another 10% are running IE 7. Both of these browsers have reached end of life and no longer receive security updates from Microsoft, leaving them open to new threats.

Internet Explorer 7 & 8
# no longer receive security updates.

03 Flash

Nearly 62 percent of devices running IE have an old version of Flash installed.

Only 38% of devices running the IE browser had the latest version of Adobe Flash Player, compared to 89% of devices running Chrome.

On the latest Microsoft browser, Edge, Flash was up to date on 67% of browsers.

UP-TO-DATE FLASH ACROSS BROWSERS ON WINDOWS

Browser	Percentage
Chrome	89%
Safari	68%
Firefox	68%
Internet Explorer	38%
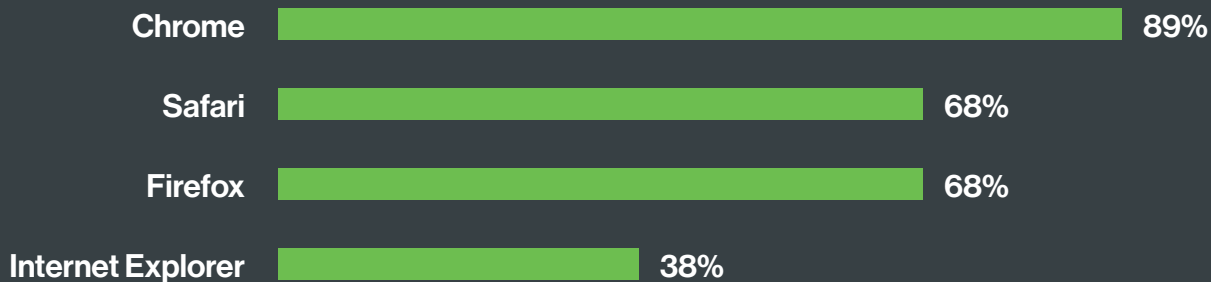
Earlier this year, Adobe released emergency patches to close zero-day vulnerabilities which enabled criminal hackers to spread ransomware.[12] In July, Adobe released one of the biggest security updates to Flash this year, patching for a total of 52 vulnerabilities.[13] These critical security flaws could lead to data leaks and remote code execution, allowing an attacker to take control of an affected system.

Attackers also often quickly integrate the newest Flash software vulnerabilities into their exploit kits, sometimes within weeks or days of being disclosed publicly. In June, just ten days after a patch was released for a Flash zero-day, researchers noticed that it had been added to three different additional exploit kits.[14] These exploit kits are designed to execute payloads and install malware on users' devices.

With over half of IE browsers running unpatched, out-of-date versions, they may be susceptible to a compromise by an exploit kit containing code for the latest Flash vulnerability.

In July, Adobe released one of the biggest security updates to Flash, patching 52 vulnerabilities.

WHAT'S A
ZERO-DAY VULNERABILITY?

A zero-day vulnerability is a previously undisclosed software bug that is unknown to the vendor or public. It can be used by malicious attackers to gain access to systems, control of user devices, and to steal data. Zero-day vulnerabilities are especially difficult for organizations to combat, as vendors have not yet released security updates to fix them.

CRITICAL FLASH VULNERABILITY
AFFECTS INTERNET EXPLORER

Last year, the spyware company Hacking Team was compromised. Two serious vulnerabilities were discovered, affecting Adobe Flash Player and Microsoft's Windows operating system.

The critical Flash vulnerability (CVE-2015-5119) can be used against browsers like IE, Firefox, Chrome and Safari. It allows attackers to execute code on a victim's machine. The Flash vulnerability was used in a series of attacks in Korea – the user received spear-phishing emails with attached documents, containing a URI to a site hosting a Flash exploit.[16]

The Windows OS vulnerability affects an Adobe font driver, and affects Windows XP through Windows 8.1. It allows attackers to elevate privileges on a machine to administrator level – when paired with the Flash exploit, it's a successful way to compromise a machine.

Java

Ninety-eight percent of devices running IE have Java installed.

In July, the most critical security update released by Oracle was for Java.[17] One flaw can be triggered remotely without authentication – an attacker merely has to set up a malicious web page, then trick the user into visiting the page in order to compromise their device.[18]

In 2015, Oracle released four critical patch updates with 83 total security fixes for Java; this year, the company released three critical patches with 30 fixes for Java.[19]

In May 2016, the Department of Homeland Security (DHS) warned of a Java vulnerability from 2010 that led to the breach of three dozen global enterprises, despite being patched six years ago.[20] The flaw was actively exploited to gain full administrative access, leveraging both unpatched and misconfigured SAP systems – taking advantage of the fact that many companies fail to keep up with applying new security patches.

Many businesses have legacy and custom applications that rely on Java, which, if not updated regularly, will leave them with widespread vulnerabilities. Java is still a top target of attackers. If you don't need it, uninstall it – or update it.

An attacker merely has to set up a malicious web page, then trick the user into visiting the page in order to compromise their device. If you don't need Java, uninstall it – or update it.

Just this year, Oracle has released three critical patches with 30 fixes for Java.

NEED JAVA?
STAY SECURE

For organizations that must still use Java, our security recommendations are as follows:

- Use automatic updates with notifications for Java to keep it as up to date as possible

- Use Duo's Trusted Access solution to block out-of-date Java plugins from accessing sensitive data and services

- Duo's solution also gives users actionable feedback on how to update their devices themselves
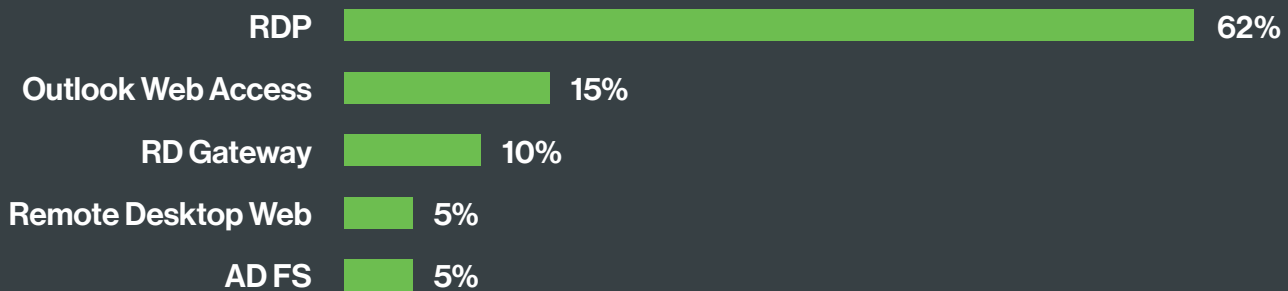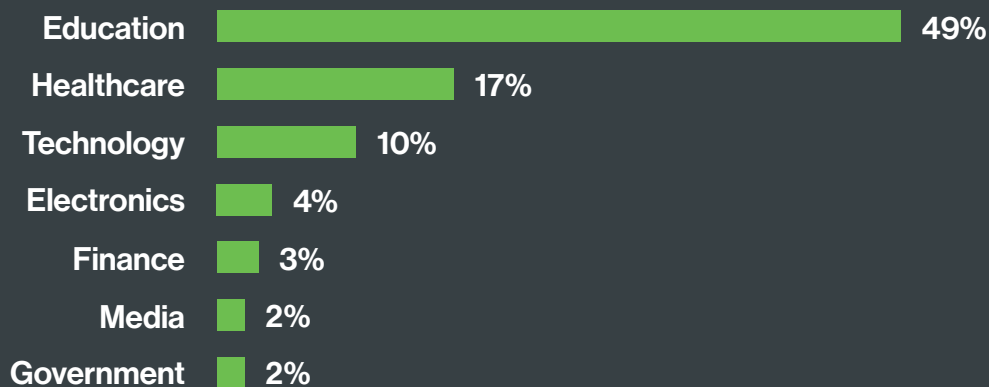
Microsoft Applications

The most popular Microsoft remote access services include RDP, OWA and RD Gateway.

About 42% of Duo's customers integrate our access solution with a Microsoft service. Among them, we found that 62% were Remote Desktop Protocol, 15% Outlook Web Access and 10% Remote Desktop Gateway.
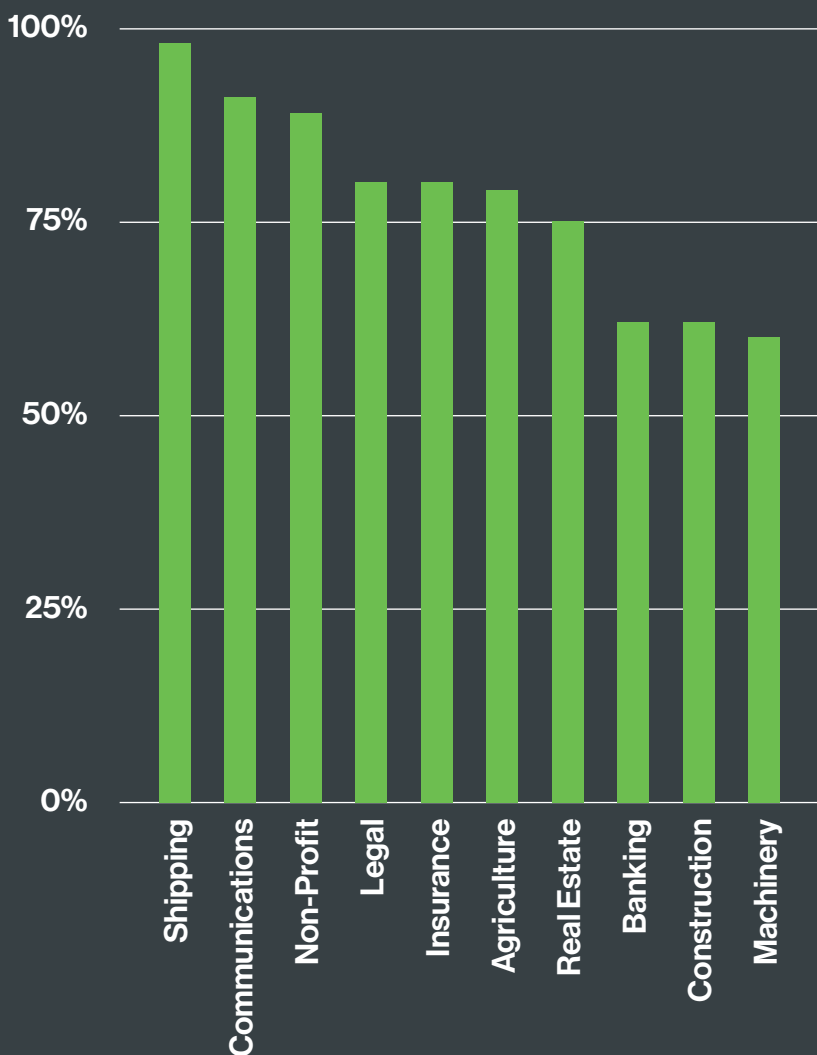
MICROSOFT SERVICES

RDP	62%
Outlook Web Access	15%
RD Gateway	10%
Remote Desktop Web	5%
AD FS	5%

WINDOWS ENDPOINTS BY INDUSTRY

Education	49%
Healthcare	17%
Technology	10%
Electronics	4%
Finance	3%
Media	2%
Government	2%

Our verticals with the largest number of Windows endpoints include Education (49% of their endpoints are Windows), and Healthcare (17% of their endpoints are Windows).

When it comes to adoption of Windows 10, the healthcare industry is even more behind than the average Duo customer. We found that 78% of the Windows endpoints in healthcare are running on the Windows 7 OS, while only 14% are running the latest version, Windows 10.

WINDOWS ENDPOINTS BY INDUSTRY (TOP 10)

By industry, we found that the highest number of authentications into Microsoft services were found in Shipping (98%), Communications (91%) and Nonprofit (89%). Other industries that were also mostly Microsoft-driven include Legal, Insurance, Agriculture, Real Estate, and Banking.

SAFE MIGRATION
TO THE CLOUD

As part of the upgrade to newer applications, many large Microsoft customers are also migrating their services to the public cloud, switching from Exchange servers and local Microsoft Office software in favor of Office 365 in the cloud.

Duo's Trusted Access platform can be used to protect every application in a hybrid environment – both Microsoft on-premises and cloud-based services during the migration. **Learn more about Duo for Microsoft**.

WINDOWS
IN HEALTHCARE

Additionally, the healthcare industry has twice as many Windows endpoints running XP than our average customers. Early this year, one of Melbourne's largest hospital networks was disrupted by a virus that affected machines running Windows XP (which is no longer supported by Microsoft).[21]

Part of the reason for a higher occurrence of out-of-date versions of Windows within the healthcare industry may be due to the fact that medical devices often run on legacy software and operating systems, and can be difficult to update. Additionally, Epic is one of the most widely used electronic health record (EHR) systems that requires Windows, which may account for the high occurrence of Windows use within the healthcare industry.

There are Health Insurance Portability and Accountability Act (HIPAA) compliance consequences for running unpatched and unsupported software. In 2014, an Alaskan health services organization was found in violation of the HIPAA Security Rule when they experienced malware and a data breach that was the direct result of the failure to upgrade their IT systems with available patches, as well as running outdated software.[22]

06 Conclusion

Our findings reveal over half of devices are running a seven-year-old Microsoft operating system, which is missing many security features of the latest Microsoft OS, Windows 10. Additionally, almost a quarter are running unsupported versions of Microsoft's Internet Explorer web browser, and more than half of devices running the IE browser have an old version of Flash installed.

That means many Windows devices we've observed may have a significantly lower security posture, as out-of-date software can leave devices open to known vulnerabilities that can be exploited by an attacker, leading to a data breach.

Ensuring trusted and healthy devices requires insight into your complete device inventory, including managed and unmanaged devices, for devices that log into all of your applications, both on-premises and cloud. When paired with the ability to create policies around your device security posture, this data can allow you to block or remediate out-of-date devices.

That way, you can both prevent any risky devices from accessing your applications while collecting the data you need to address outdated software.

Duo's Trusted Access platform can be used to protect every application in a hybrid environment – both Microsoft on-premises and cloud-based services during the migration.

Reduce the risk of a data breach by enforcing strong access control policies to ensure up-to-date devices and systems in your organization.

We also recommend:

Disable Java and prevent Flash from running automatically on corporate and user-owned devices through endpoint access policies and controls.

Prepare for Bring Your Own Device (BYOD), instead of rejecting it. Give your IT administrators data on device ownership and health to inform risk-based access control decisions.

Use browser platforms that update more frequently and automatically, like Google Chrome.

Establish and communicate good security hygiene practices, such as:

Run regular security updates as well as emergency patches.

Use device encryption, passcodes and fingerprint ID.

Implement an additional authentication solution to protect systems and data.

Enable automatic updates for as much software as possible to make it easier for your users.

07 Duo's Trusted Access Solution

To protect your environment from multiple attack vectors, Duo has taken a holistic approach to security.

Our **Trusted Access** solution verifies your users' identities and the security health of their devices before granting them access to specific applications.

We've combined the most effective defenses into one solution that our customers use to securely log into services every day. It's comprised of **Trusted Users** and **Trusted Devices** for secure access to **Every Application**. Duo's Trusted Access platform can be used to protect every application in a hybrid environment – both Microsoft on-premises and cloud-based services during the migration.

Trusted Users

Make sure everybody really is who they say they are.

Two-factor authentication provides an additional layer of security to your users' logins, eliminating the threat of a compromise due to phishing or other password-stealing attack by requiring a second factor to verify their identities.

Verify your users with our easy-to-use, cloud-based two-factor authentication solution which lets your users get to work quickly with our **mobile authentication application** that allows them to approve **push notification** requests.

Duo also enables your administrators to enforce access policies based on contextual parameters such as user location, IP reputation, etc. Plus, it's fast and easy to deploy with no hardware to buy, install, or manage.

Trusted Users and Trusted Devices for secure access to Every Application.

Trusted Devices

Be sure their devices meet your security standards.

Even a trusted user may still show up with risky mobile devices and computers that have vulnerabilities or out-of-date software. Before users can connect to your company's applications, Duo checks to see if they're using a known device.

Then, our platform **inspects those endpoints** to verify they're running the latest operating systems, browsers, and plugins like Flash and Java. Duo also checks your users' devices to ensure they have important security features enabled, like screen lock, fingerprint identification and a passcode to keep intruders out.

Finally, our endpoint controls allow you to **block any device** that doesn't meet your minimum security requirements or **warn and notify users** to update them, eliminating the risk of spreading malware and unauthorized access.

Every Application

Let them access only the applications you deem appropriate.

Duo integrates to protect **every type of application** – VPNs like Juniper, Cisco, and Palo Alto; cloud applications like Microsoft O365, Salesforce, Google Apps, AWS and Box; on-premises applications and web applications like Epic, SSH, UNIX, and Wordpress; and APIs and client libraries for everything else like Python, .Net, Ruby and more – to help you quickly and easily secure your environment.

Our **single sign-on (SSO)** solution allows users to securely and conveniently access their cloud applications via a portal by logging in only once. Duo checks the security health of your users' devices every time they access an application, without the use of an agent.

Finally, Duo also lets you create custom authentication **policies and controls** per user group or application, to ensure users only access the applications you want them to access.

08 References

[1] *Microsoft Security Intelligence Report Volume 20*; Microsoft; Sept. 13, 2016

[2] *Oracle's Critical Patch Update for July Contains Record Number of Fixes*; SecurityWeek.com; July 20, 2016

[3] *Patch Java Immediately or Attackers Can Hack You*; SecurityAffairs.co; March 24, 2016

[4] *Microsoft: Windows 7 Security Vulnerabilities*; CVE Details; Sept. 13, 2016

[5] *The Best New Security Features of Windows 10*; InfoWorld.com; March 15, 2016

[6] *Microsoft: Windows XP: Security Vulnerabilities*; CVE Details; Sept. 22, 2016

[7] *Windows XP Support Has Ended*; Microsoft; Sept. 1, 2016

[8] *Home Depot, Target Breaches Exploited Windows XP Flaw, Report Says*; NetworkWorld; Sept. 18, 2014

[9] *Explore the Chrome Browser*; Google; Sept. 13, 2016

[10] *Microsoft Drops Support for Internet Explorer: Just How Big of Deal is This?*; Duo Security; Jan. 7, 2016

[11] *Microsoft Security Bulletin MS16-095 – Critical*; Microsoft; August 9, 2016

[12] *Latest Flash Zero Day Being Used to Push Ransomware*; Threatpost.com; April 7, 2016

[13] *Adobe Deploys Security Update to Fix 52 Vulnerabilities in Flash*; ZDNet.com; July 13, 2016

[14] *Flash Zero-Day Exploited in Targeted Attacks*; SecurityWeek; June 14, 2016

[15] *Major Adobe Flash Security Flaw Discovered in Hacking Team Leak*; The Verge; July 8, 2015

[16] *Hacking Team Flash Zero-Day Tied To Attacks In Korea and Japan… on July 1*; Trend Micro; July 8, 2015

[17] *Oracle's Critical Patch Update for July Contains Record Number of Fixes*; SecurityWeek.com; July 20, 2016

[18] *Patch Java Immediately or Attackers Can Hack You*; SecurityAffairs.co; March 24, 2016

[19] *Critical Patch Updates, Security Alerts and Third Party Bulletin*; Oracle.com; August 22, 2016

[20] *DHS Warns on Actively Exploited SAP Java Vulnerability*; SearchSecurity; May 13, 2016

[21] *Hack Attack on a Hospital IT System Highlights the Risk of Still Running Windows XP*; Phys.org; Jan. 22, 2016

[22] *Bulletin: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software* (PDF); U.S. Dept. of Health & Human Services; December 2014

Protect all users, all devices and any application with Duo's Unified Access Security (UAS).

Trusted Users

Verify users with advanced two-factor authentication and enforce user access policies to limit access to applications.

Trusted Devices

At login, Duo checks the security health of every device – including employee-owned devices. Customize access policies based on device risk.

Every Application

Protect cloud and on-premises applications, and simplify access with Duo's secure single sign-on (SSO) for both users and admins.

DUO
The Most Loved Company in Security

North America

866.760.4247

Europe, Middle East & Africa

+44 8003 585 309

Contact Us

duo.sc/contactduo