Microsoft Vulnerabilities Report 2021

Evolving Threats,
The Dangers of Admin Rights
& How To Address Them

BeyondTrust

TABLE OF CONTENTS

THE BIG PICTURE

Overview

Currently in its 8th year, the Microsoft Vulnerabilities Report has proven to be a valuable asset for many organizations who wish to gain a holistic understanding of the evolving threat landscape. **The report provides a 12-month, consolidated view and analysis of Microsoft Patch Tuesdays**, as well as exclusive insights from some of the world's top cybersecurity experts.

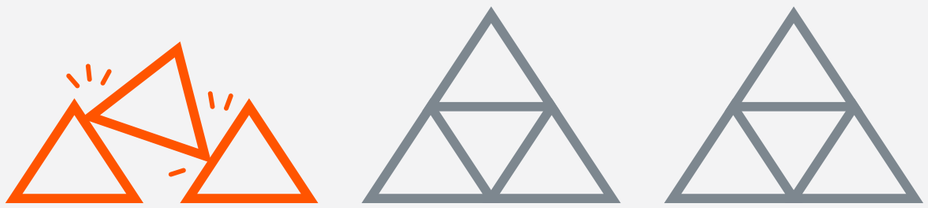
Unpatched vulnerabilities are the cause of 1 in 3 breaches around the world. As a result of unpatched vulnerabilities, organizations can pay the ultimate price.

In 2017, the WannaCry ransomware attack infected over 200,000 computers across 150 countries, causing damages ranging from hundreds of millions to billions of dollars. While Microsoft had released patches to close the exploit, much of WannaCry's spread was from organizations that had not yet applied them.

In 2020, Ryuk Ransomware operators shut down Universal Health Services using the Zerologon privilege-escalation vulnerability to quickly take control of domain controllers. This same vulnerability was also actively used by an Iranian state actor in attacks.

Although many organizations understand the need to install the latest security patches to mitigate vulnerabilities and prevent their corresponding exploits in a timely manner, the volume can be overwhelming. The reality is that many companies, often under-resourced from an IT perspective, struggle with timely patching for every Critical vulnerability released.

Approximately 1.5 billion people use Windows operating systems each day, with various applications for Microsoft's products reaching into homes, businesses, and entertainment venues. **The data in this report provides a crucial barometer of the threat landscape for the Microsoft ecosystem.**



Unpatched vulnerabilities are the cause of 1 in 3 breaches around the world.

What Does the Data Tell Us?

The BeyondTrust Microsoft Vulnerabilities Report analyzes the data from security bulletins issued by Microsoft throughout the previous year. Every Tuesday, Microsoft releases fixes for all vulnerabilities affecting Microsoft products – known as Patch Tuesday. The BeyondTrust report compiles this extensive information into a holistic, consolidated view that highlights key trends from the prior year.

This analysis not only reveals evolving vulnerability trends, but also identifies the Critical vulnerabilities that could be mitigated if admin rights were removed.

We also include an insightful, five-year trend comparison to give you a better understanding of how vulnerabilities have grown over time, along with additional detail by category and product type.

Report Highlights

Vulnerabilities Soared in 2020

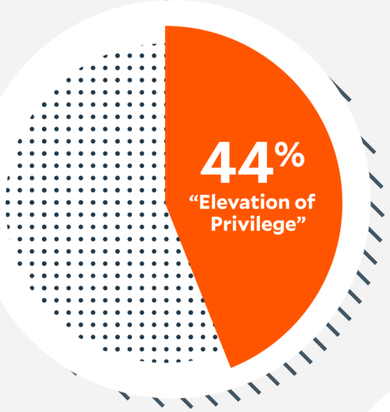
The threat landscape continues to **evolve and expand**, accelerated by the mass shift to **remote working**.

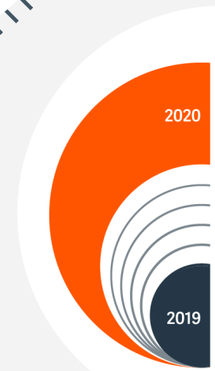
1,268 vulnerabilities a record **HIGH**

48% compared to 2019

"Elevation of Privilege" was the #1 Category of Vulnerabilities

Attackers gain access to accounts and **increase the level of privileges** to compromise other IT assets.



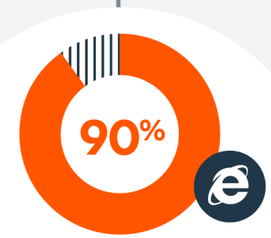


3x as many compared to the previous year

Controlling Admin Rights Mitigates the Risk

Enforcing least privilege is the **fastest & most effective measure** to address this problem.

of all Microsoft Critical Vulnerabilities could have been mitigated by **removing admin rights**

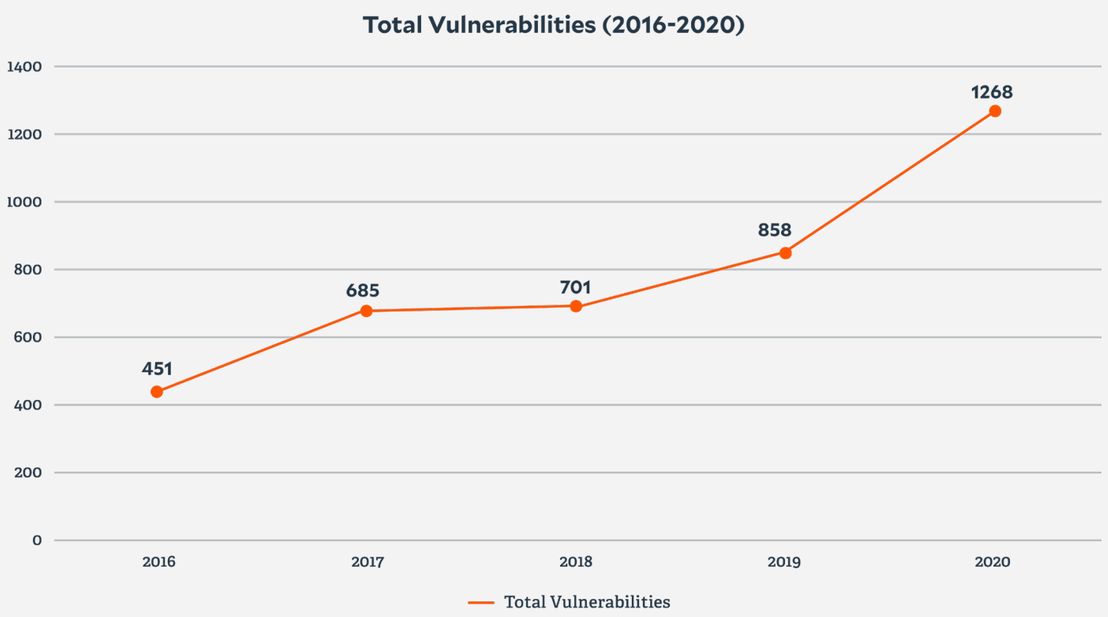


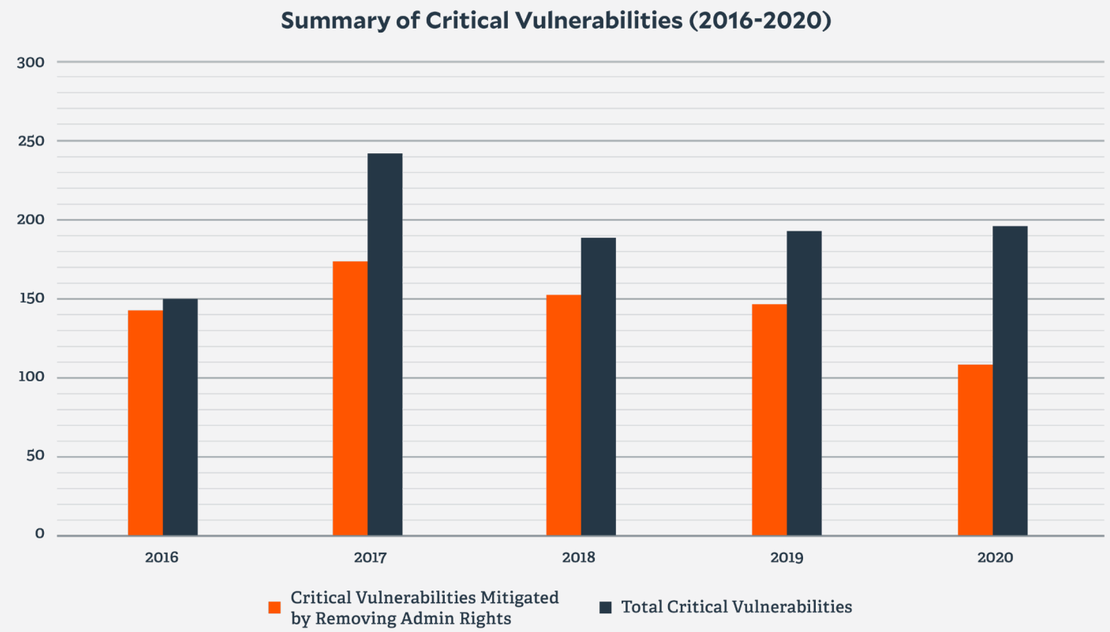
of Critical Vulnerabilities in Internet Explorer would have been mitigated by **removing admin rights**

Five Year View

Over the last five years, the total number of vulnerabilities in Microsoft products has skyrocketed, with a colossal 181% increase since 2016. **The past year marked the single biggest jump – climbing from 858 vulnerabilities in 2019 to 1,268 in 2020 (48% increase YoY).** As the volume of vulnerabilities surges, attackers have access to an ever-growing "catalog of exploits," meaning the attack surface is exponentially increasing year over year.

In the past, a ransomware attack would have targeted one vulnerability; now, a single strain can target a dozen or more. Once attackers gain access to your network via a phishing email, they can seek and target endpoints you haven't yet patched.



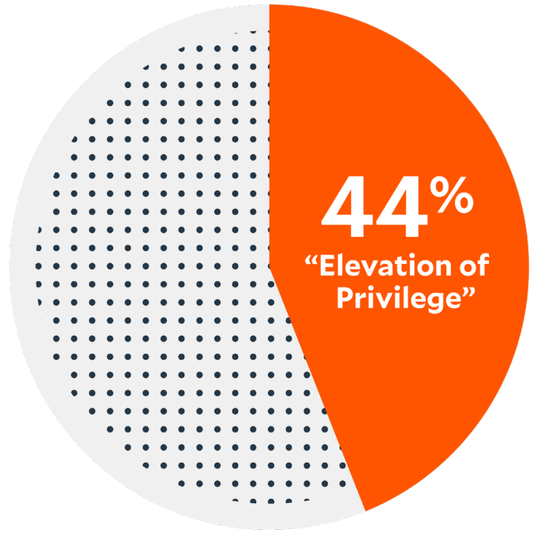


For the previous three years, Critical vulnerabilities have plateaued, but the volume has not materially declined. Critical vulnerabilities carry the highest risk and, if exploited, could significantly impact organizations. **In 2020, 56% of Critical vulnerabilities would have been mitigated by removing admin rights.**

VULNERABILITIES BY CATEGORY

Vulnerabilities by Category (2016-2020)

	2020	2019	2018	2017	2016
Remote Coded Execution	345 (27%)	323	292	301	269
Elevation of Privilege	559 (44%)	198	145	90	114
Information Discloure	179 (14%)	177	153	193	102
Denial of Service	46 (4%)	52	29	43	0
Spoofing	104 (8%)	63	20	16	12
Tampering	7 (0.5%)	8	8	1	0
Security Feature Bypass	30 (2.5%)	38	20	41	26



How Microsoft Groups Vulnerabilities

Each Microsoft Security Bulletin is comprised of one or more vulnerability categories, applying to one or more Microsoft products. These categories, organized by impact type, include Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing and Tampering. These are reflected in the MITRE ATT&CK framework, which documents common tactics, techniques, and procedures that advanced persistent threats use against Windows enterprise networks. Execution and escalation are where most of an attacker’s energy is focused, resulting in these categories experiencing the most reported vulnerabilities.

Elevation of Privilege is the #1 Category

For the first time, Elevation of Privilege accounted for the largest proportion of total Microsoft vulnerabilities (44%), almost tripling in number YoY (from 198 in 2019 to 559 in 2020). This might reflect a decreasing availability of easily compromised admin accounts, driving threat actors to utilize different attack vectors in cyberbreaches.

VULNERABILITIES BY PRODUCT

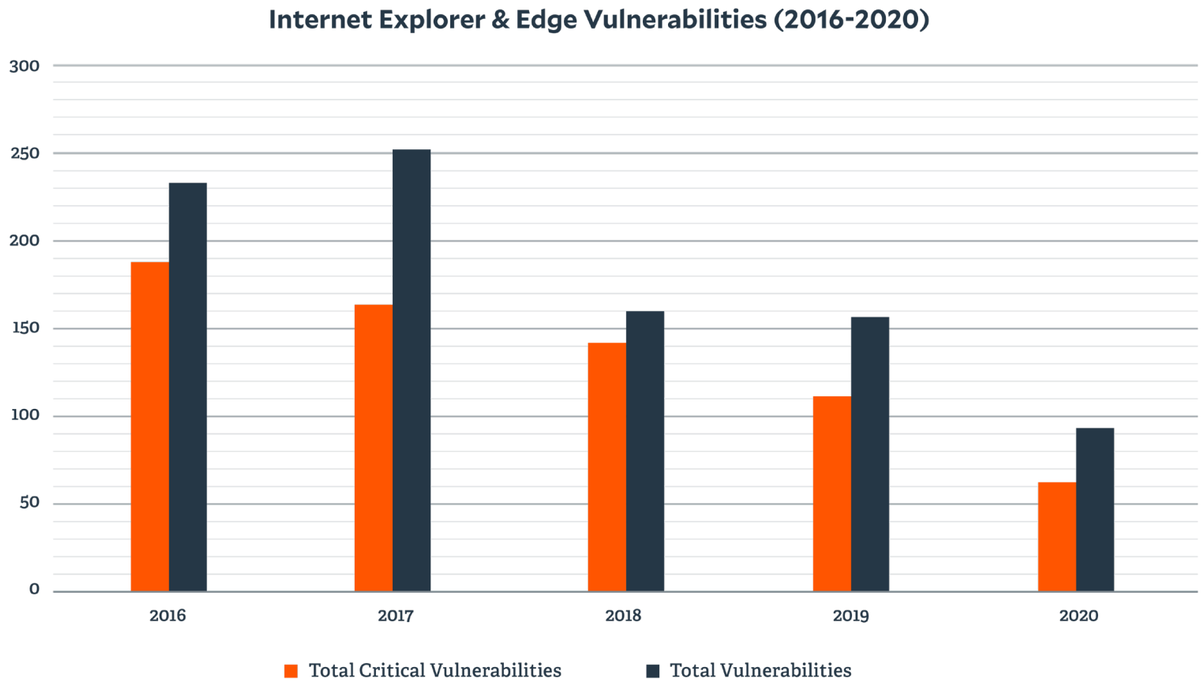
Internet Explorer & Edge Vulnerabilities

Despite the dominance of Google Chrome and Firefox, Microsoft Internet Explorer (IE) is still a popular browser. Yet, since January 2016, Microsoft only supports and patches the most current version of IE available for a supported operating system, and Internet Explorer 10 reached end-of-support on January 31, 2020. From that point forward, IE 11 became the only supported version of Internet Explorer on Windows Server 2012 and Windows Embedded 8 Standard. Additionally, Microsoft will no longer support IE11 in O365, OneDrive and Outlook web as of August 2021 as they try to push users to the more feature-rich and secure Edge.

There were 27 Critical vulnerabilities discovered across Internet Explorer 8, 9, 10, and 11 during 2020. **Removing admin rights could have mitigated 24 of them, eliminating 89% of the risk.**

Critical vulnerabilities in Microsoft Edge decreased last year, from 86 to 34. Of those 34, removing admin rights could have mitigated 29 of them (85%).

On January 15, 2020, Edge moved to a Chromium-based engine, meaning that both Google Chrome and Edge could have the same flaws at the same time, leaving no “safe” mainstream browser to use as a mitigation strategy to Edge vulnerabilities.



Critical Vulnerabilities
61

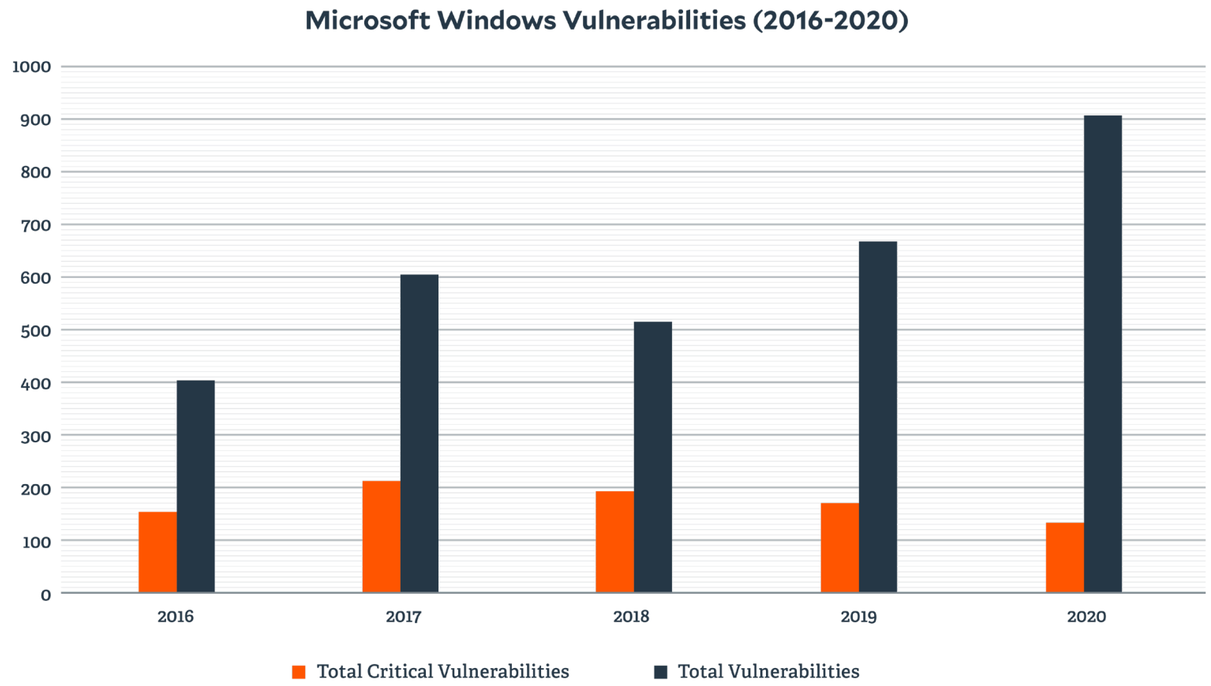
87%
Critical Vulnerabilities Mitigated by Removing Admin Rights

Total Vulnerabilities
92

Windows Vulnerabilities

In 2020, a record high 907 vulnerabilities were reported across Windows 7, Windows RT, Windows 8/8.1, and Windows 10 operating systems. **Windows 10 was touted as the "most secure Windows OS" to date when it was released, yet it still experienced 132 Critical vulnerabilities last year.** Of all the Windows vulnerabilities discovered in 2020, 132 were considered Critical.

Removing admin rights could have mitigated 70% of these Critical vulnerabilities.



Critical Vulnerabilities
132

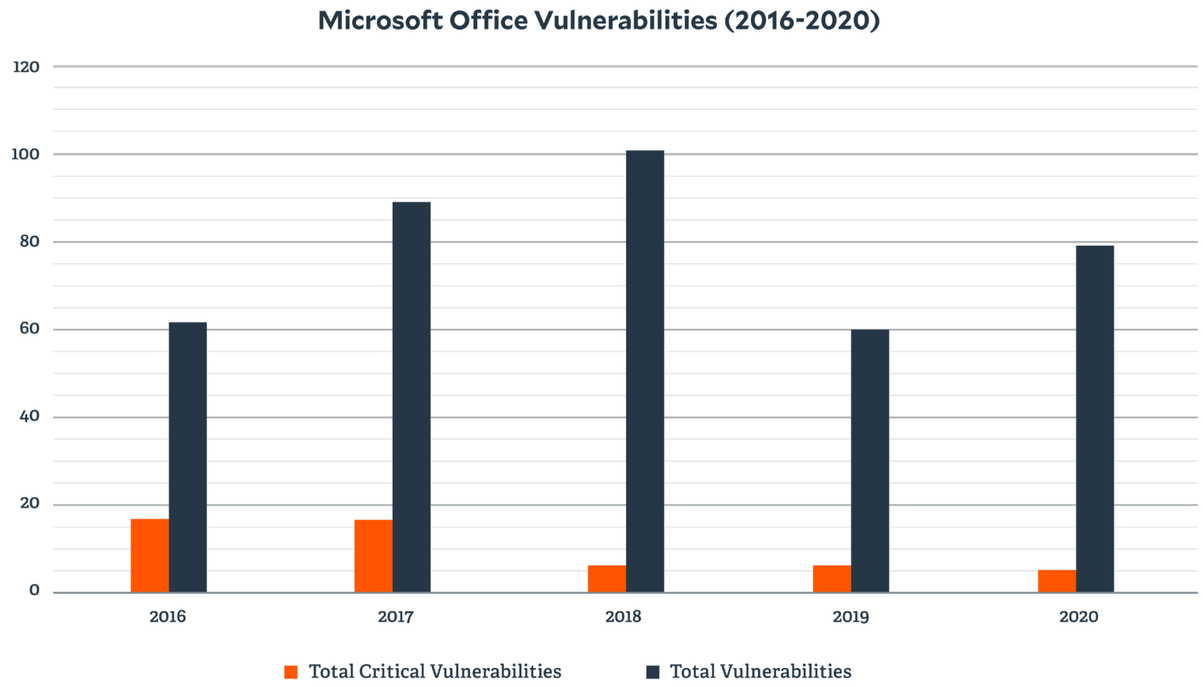
70%
Critical Vulnerabilities Mitigated by Removing Admin Rights

Total Vulnerabilities
907

Microsoft Office Vulnerabilities

Microsoft Office vulnerabilities rose from 60 to 79 in 2020. Of the 79, only 5 were considered Critical and removing admin rights would have mitigated 4 of them (80%) in all Office products (Excel, Word, PowerPoint, Visio, Publisher, and others).

The prevalence of malicious documents used in malware attacks highlights the importance of removing admin rights. Features like Trusted Application Protection further protect against these vulnerabilities — even if your end users inadvertently load malware-laced documents via email or the web — the malicious payloads are instantly blocked from launching.



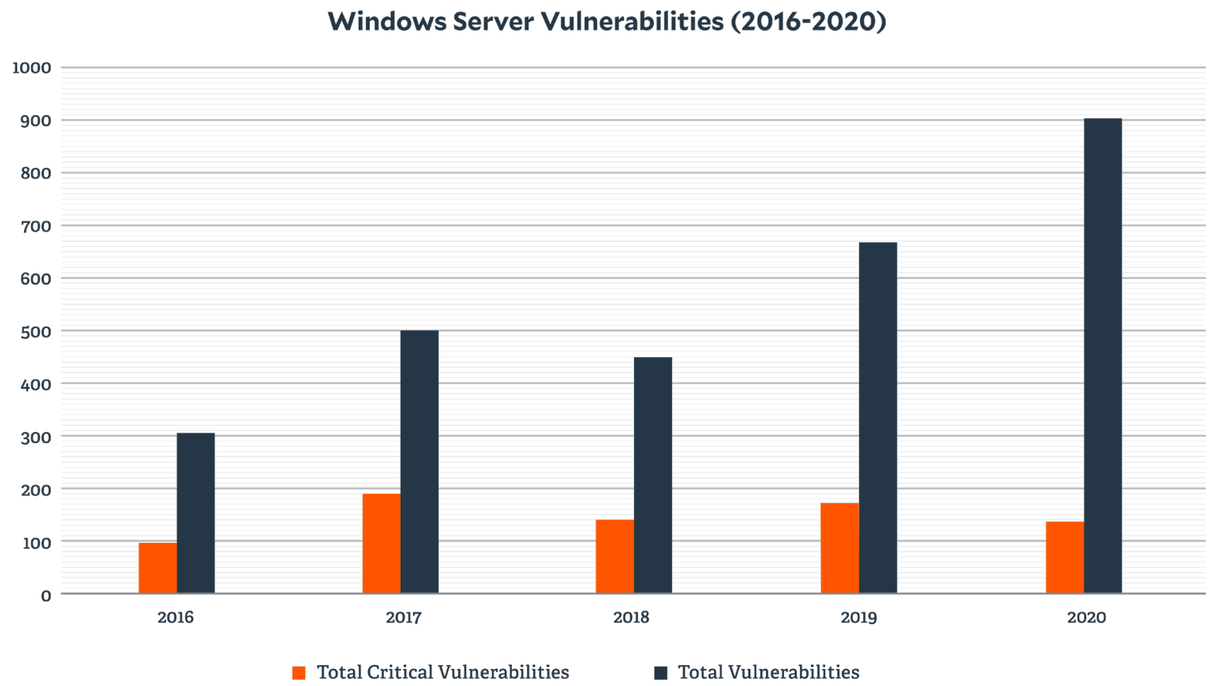
Critical Vulnerabilities
5

80%
Critical Vulnerabilities Mitigated by Removing Admin Rights

Total Vulnerabilities
79

Windows Server Vulnerabilities

A total of 902 vulnerabilities were reported in Microsoft Security Bulletins affecting Microsoft Windows Servers in 2020 — a 35% increase over the previous year. Of the 138 vulnerabilities with a Critical rating, 66% could be mitigated by the removal of admin rights.



Critical Vulnerabilities
138

66%
Critical Vulnerabilities Mitigated by Removing Admin Rights

Total Vulnerabilities
902

EXPERT COMMENTARIES

Chuck Brooks

Cybersecurity Expert

A majority of those remote work-related breaches emanated from a lack of visibility by administrators over employee access policies and vulnerable endpoints.

"Working from outside the office has certainly changed the paradigm of cybersecurity, as newly remote employees have evolved into individual offices. As a result of a greatly expanded digital attack surface, phishing attacks are up 600%, including Covid-19-themed phishing attacks aimed at workers mixing personal and work devices over non-secure Wi-Fi networks. A majority of those remote work-related breaches emanated from a lack of visibility by administrators over employee access policies and vulnerable endpoints.

To adjust to the new work-from-home realities, companies need to better manage the proliferation of desktop and mobile devices, including applying patches and security updates. Controlling user privileges and employing stronger endpoint management under a zero trust framework are prudent initiatives for companies to follow as digital connectivity grows.

In a remote work ecosystem, it can be a significant challenge to validate the security configurations, controls, and patches that are used by employees - it is difficult to protect what you cannot see. However, this gap can be mitigated by removing employee administration rights by assuming they are at risk. In simple terms, zero trust for anything outside the CISO's team or administrator's direct control.

Companies are now looking at zero trust models, whether remote or on-premises, that are anchored by a solid Identity and Access Management (IAM) program that encompasses strong administrative policies and controls for authentication, authorization, and auditing of the identity lifecycle. Hackers usually take the easiest path to a breach, and privileged access rights have traditionally been a point of exploitation.

Controlling and verifying who has access and the proper credentials to data (wherever it resides) is fundamental to cybersecurity in our rapidly evolving digital work era. Software and platforms will inevitably have vulnerabilities - not necessarily from flawed code, but from human administrative error. Along with controlling administrative rights, fortified endpoints layered with strong passwords and data encryption need to be an integral part of the work-from-home business model."

Chuck is on the Faculty of Georgetown University, where he teaches in the Graduate Applied Intelligence and Cybersecurity Programs. Chuck has been a featured speaker at numerous cybersecurity events, including presenting before the G20 country meeting on energy cybersecurity. He is also a Visiting Editor at Homeland Security Today, and a Contributor to Forbes.

“This report is something I can’t wait to get my hands on every year! If we look at the numbers, we can see the trend of growing vulnerabilities in a year — getting even worse than ever before. The huge jump in the number of vulnerabilities tells me that more and more security researchers are actively helping companies to protect themselves, but sadly also that the bad guys are doing the same to actively search for the vulnerabilities. There were numerous zero-day vulnerabilities in multiple different products last year and that means that proactive measures are even more important than ever before.

Block-listing is an active protection - I believe that’s a job for your anti-malware - but allow-listing is the most recommended proactive protection for every company out there. With allow-listing, you can just add maybe one rule a month to the “Good Application or Locations” list, while deny-listing needs to add more than a million lines to the list every day!

The problem with allow-listing is that it is insanely difficult if you don’t have the Principle of Least Privilege in place. The Windows security subsystem was not built to withstand the use of admin rights. Allow-list will let you run things from your C:\Windows-folder, but an admin can put anything in there. So, to make this work for admins, you would need to create thousands of rules instead of one.

The removal of admin rights is a great proactive protection, as you can see from the numbers in this report. We need to protect the components that execute malicious payloads, so our most important apps to protect are things that browse the web or read email. The numbers in this report tell you the great results removing admin rights will give you in protection for Outlook, Office, IE, and Edge!”

The Windows security subsystem was not built to withstand the use of admin rights.

Sami Laiho

Microsoft MVP & Ethical Hacker

Sami Laiho is one of the world’s leading professionals in Windows OS and Security. Sami has been working with and teaching OS troubleshooting, management, and security since 1996. At Ignite 2017, the world’s biggest Microsoft event, Sami was evaluated as the Best External Speaker.

If end users do not operate with local administrative privileges, the vast majority of Critical vulnerabilities can be mitigated until security updates are applied.

Morey Haber

CTO & CISO BeyondTrust

Morey J. Haber is Chief Technology Officer and Chief Information Security Officer at BeyondTrust. He has more than 25 years of IT industry experience and has authored three Apress books: Privileged Attack Vectors, Asset Attack Vectors, and Identity Attack Vectors.

"There was a day when information and security professionals scrambled to install the latest security patches to mitigate published vulnerabilities and prevent their corresponding exploits. Sadly, some organizations still scramble for every Critical vulnerability released due to service level agreements, archaic policies, and compliance requirements.

Don't get me wrong, Critical vulnerabilities should be patched in a timely manner, but there are other mitigating controls that can be incorporated into daily processes to create a defense-in-depth strategy by layering on multiple proactive controls to reduce the risk. As a result, modern controls, like least privilege, can buy time for an organization to patch on schedule, versus "panic patching".

Every year, BeyondTrust authors the Microsoft Vulnerabilities Report. In 2021, "Elevation of Privilege" was the #1 vulnerability for the first time. The concept of least privilege, which includes the removal and management of administrative rights for end users, has a profound effect in mitigating security risks associated with Critical vulnerabilities.

A simple, powerful fact is that, if end users do not operate with local administrative privileges, the vast majority of Critical vulnerabilities can be mitigated until security updates are applied. This least-privilege approach also saves IT teams from squandering valuable resources that may otherwise be hastily re-allocated to "panic patching".

The simple fact that patching must always occur is a fundamental cyber security hygiene practice. However, deflecting an attack with good cyber security policies like the removal of administrative rights ultimately makes the environment (and home-based workers) even more secure. And, most importantly, enabling least privilege can buy your organization time to patch when Critical vulnerabilities are published."

As the permitter dissolves, the attack surface expands along with even more sophisticated assaults.

Jane Frankland

Executive, Influencer, Author & Founder of the IN Security Movement

"The COVID-19 pandemic has created a perfect storm for all threat actors. Catching businesses unprepared at the start, this past year has seen digital transformation advance in two months what was due in two years. More people are working remotely, there's more interconnectedness than ever, more tools to use, and as the permitter dissolves, the attack surface expands along with even more sophisticated assaults.

Even with a move to the cloud, which can be considered a more secure solution when implemented correctly, BeyondTrust's report clearly illustrates the relevance of cyber hygiene basics, like privileged account management, and baking security in at the start of any IT transformation journey.

BeyondTrust's report once again highlights how many vulnerabilities can be reduced or, better still, eliminated when administrator rights are removed. Understanding this and limiting the number of users with full administrative privileges is essential for any organization that seeks a competitive advantage. Those in charge must get this. They must understand that operating in an environment of 'least privilege' does not mean tardiness and inefficiency. Quite the contrary. It equates to a stronger security posture, without limiting operational agility.

Security measures can be balanced while allowing employees the freedom to work efficiently. Administrator rights can reduce the attack surface for malicious individuals while maintaining the ability of personnel to be productive in their role. However, it is only when administrator rights and endpoint privilege management are fully understood."

Jane sits on the board of Black Hat Exec, SC Magazine, and judges 15 awards around the world – from teens in tech, to business, to literature, to cybersecurity – and she works with some of the world's most forward-thinking companies. During the past 5 years, Jane has won (or been shortlisted) for 25 awards.

MITIGATING THE RISKS

BeyondTrust Privileged Access Management

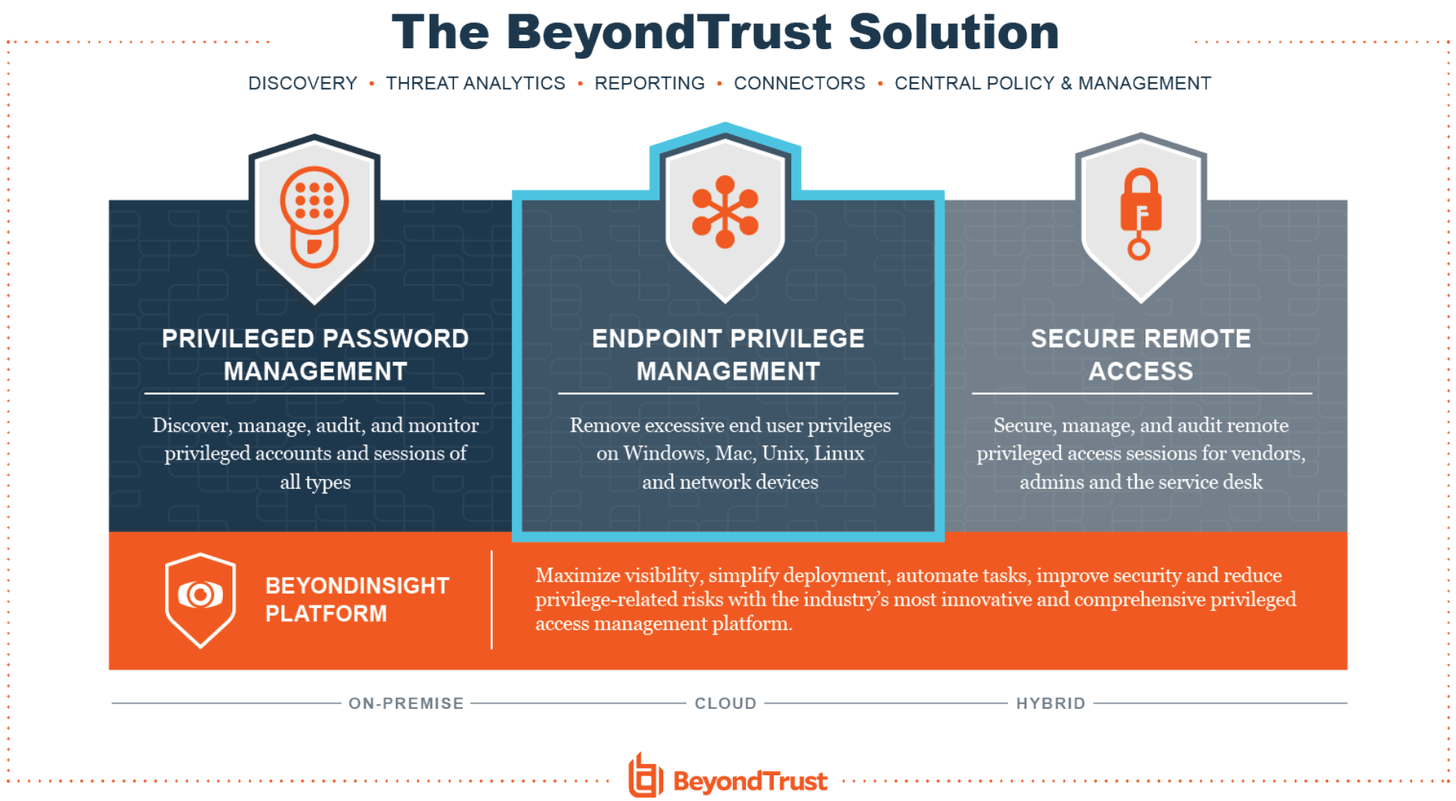
The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Garnter Magic Quadrant for Privileged Access Management[1], BeyondTrust is named a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.

Endpoint Privilege Management is a core solution of the BeyondTrust PAM portfolio, enabling comprehensive privilege and application control for desktops and servers.

[1] Gartner, Magic Quadrant for Privileged Access Management, Felix Gaehtgens, Abhyuday Data, Michael Kelley, August 4, 2020



BeyondTrust Endpoint Privilege Management

With a fast-evolving threat landscape, ensuring the endpoints in your organization are secured and protected is more critical than ever. The findings of this report show that many risks can be easily mitigated if administration rights are removed, a practice also widely recommended by industry experts.

Barriers Preventing Organizations from Addressing the Risk

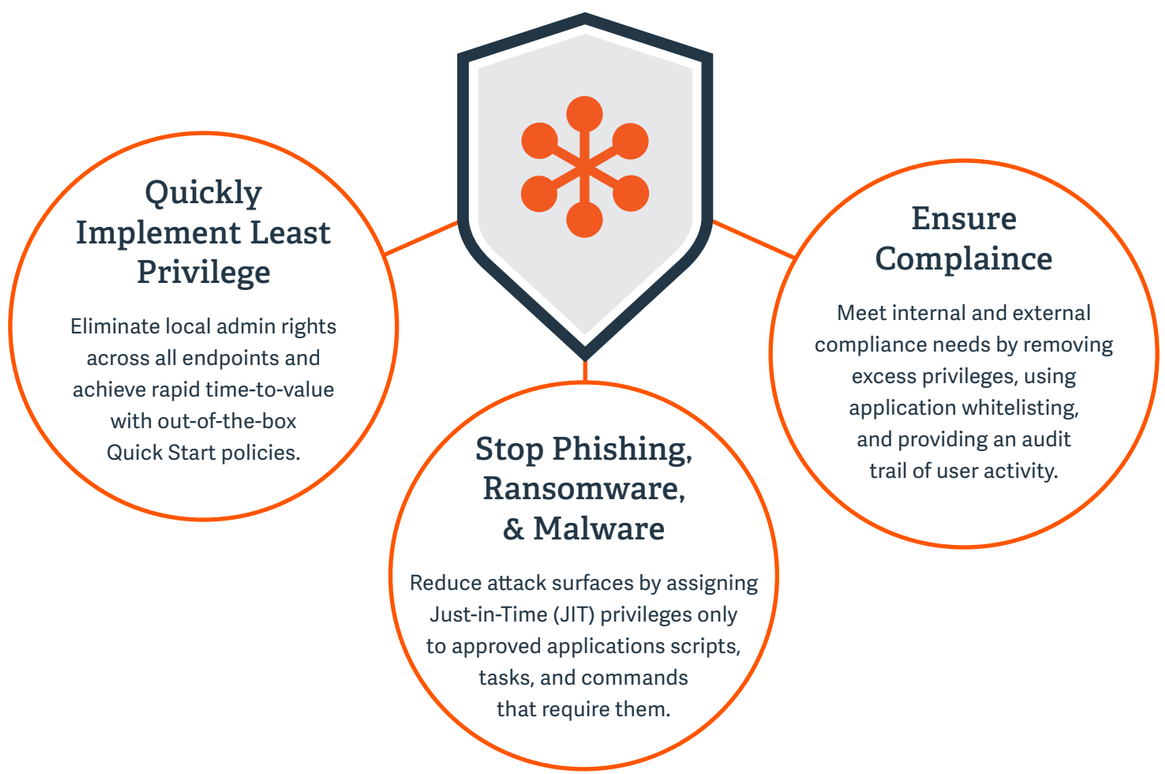
Perceptions that deploying a privilege management solution is a difficult process

Concerns that end-user productivity will be negatively impacted

The right endpoint security solution can enable organizations to achieve least privilege quickly, while also managing the right balance between security and productivity.

With BeyondTrust Endpoint Privilege Management, you can rapidly remove excessive end-user privileges on Windows, Mac, Unix, Linux, and network devices, and achieve immediate risk reduction without impacting user productivity.

Key Benefits



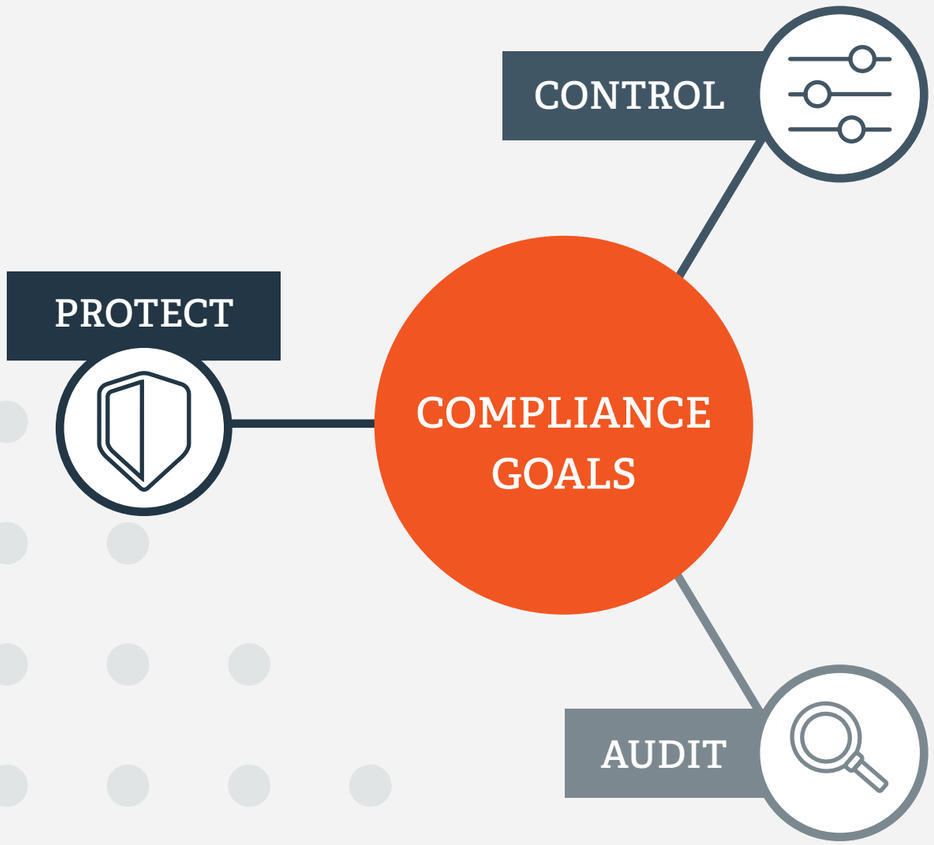
BeyondTrust Endpoint Privilege Management for Windows can be deployed either on-premises or in the Cloud and is scalable to the needs of organizations of any size, delivering a solution that both significantly increases security, improves productivity, and enables rapid time-to-value.

Removing admin rights is one of the most basic, yet powerful and protective, measures an organization can take.

Jane Frankland, Executive, Influencer, Author &
Founder of the IN Security Movement

Achieving Compliance

Implementing the principle of least privilege and removing administrator rights is a key requirement for many compliance mandates around the world. Compliance requirements can be banded into **three primary purposes** with the use of IT resources and the sensitive data they contain.



Deploying a comprehensive endpoint privilege management solution as part of your wider security strategy **enables organizations to meet the following requirements**:

IMPLEMENT only one primary function per server and **ENABLE** only necessary service, protocols, daemons, etc. as required for the function of the system. *(PCI, CIS)*

TRACK, CONTROL, PREVENT, and **CORRECT** the use, assignment, and configuration of administrative privileges on computers, networks, and applications. *(CIS, PCI, NIST, HIPAA, GDPR)*

COLLECT, MANAGE, and **ANALYZE** audit logs of events that could help detect, understand, or recover from an attack; audit logs should specify user identification, type of event, date, and time. *(CIS, PCI, NIST, HIPAA, GDPR)*

For more details on how BeyondTrust can help your organization achieve compliance, visit beyondtrust.com/solutions/compliance.

ADDITIONAL RESOURCES

A Guide to Endpoint Privilege Management

The 5 Critical Steps in your Endpoint Security Strategy

A Zero Trust Approach to Windows & macOS Endpoint Security

KuppingerCole Executive Review - BeyondTrust Endpoint Privilege Management

Video Case Study: How the University of Derby Secures Their Endpoints with BeyondTrust

METHODOLOGY

The BeyondTrust Microsoft Vulnerabilities Report, produced annually, analyzes the data from security bulletins issued by Microsoft throughout the previous year. Every Tuesday, Microsoft release fixes for any vulnerabilities affecting Microsoft products, and this report compiles these releases into a year-long overview, creating a holistic view of trends related to vulnerabilities and, more importantly, how many Microsoft vulnerabilities could be mitigated if admin rights were removed from organizations.

Each bulletin issued by Microsoft contains an Executive Summary with general information. For this report, a vulnerability is classified as one that could be mitigated by removing admin rights if it meets the following criteria stated by Microsoft in the vulnerability bulletin:

- Customers/users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights
- If the current user is logged on with administrative user rights, an attacker could take control of an affected system

As of 2020, Microsoft introduced a new layout to parts of their portal, which more succinctly outlined whether privileges were required to exploit the vulnerability. In these instances, where the tab, 'privileges required', was marked 'high', the vulnerability was counted. If the tab was marked 'low', we further investigated the summary to understand more context.

How Microsoft Classifies Vulnerabilities

Each vulnerability can apply to one or more Microsoft products. This is shown as a matrix on each vulnerability page. Each vulnerability is assigned a type from one of seven categories; Remote Code Execution, Elevation of Privilege, Information Disclosure, Denial of Service, Security Feature Bypass, Spoofing, Tampering– which occasionally vary depending on the individual piece software or combination of software affected.

A vulnerability of each type often applies to a combination of different versions of a product or products, and sometimes all versions – e.g. all versions of Windows clients. Often, a vulnerability will only apply to a combination of products – e.g. Internet Explorer 11 on Windows 7.

Each vulnerability is also assigned an aggregate severity rating by Microsoft – Critical, Important, Moderate – which also varies depending on each individual piece of software, or combination of software affected. The Common Vulnerability Scoring System (CVSS is a published standard used by organizations worldwide and provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Certain vulnerabilities have occurred multiple times throughout 2020, usually affecting different software. In these cases, the vulnerability itself is only counted once, with all affected software types attributed to that one entry.

Accuracy of Vulnerability Data

A number of generalizations have been made for each vulnerability as follows:

- Each vulnerability was classified with the highest severity rating of all instances of that vulnerability where it appeared multiple times
- Each vulnerability was classified with the most prevalent type for all instances of that vulnerability
- Product versions were not taken into account
- Product combinations were not taken into account
- Vulnerabilities were counted for both the software and version where appropriate (for example, a vulnerability for Internet Explorer 11 on Windows 10 is taken as a vulnerability for both Internet Explorer 11 and Windows

BeyondTrust

About Endpoint Privilege Management

BeyondTrust Endpoint Privilege Management combines privilege management and application control to efficiently manage admin rights on Windows, Mac, Unix, Linux, and network devices, without hindering productivity. Enforce least privilege and eliminate local admin rights with fine-grained control that scales to secure your expanding universe of privileges, while creating a frictionless user experience.

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. We are trusted by 20,000 customers, including 75 percent of the Fortune 100, and a global partner network.

Learn more at beyondtrust.com