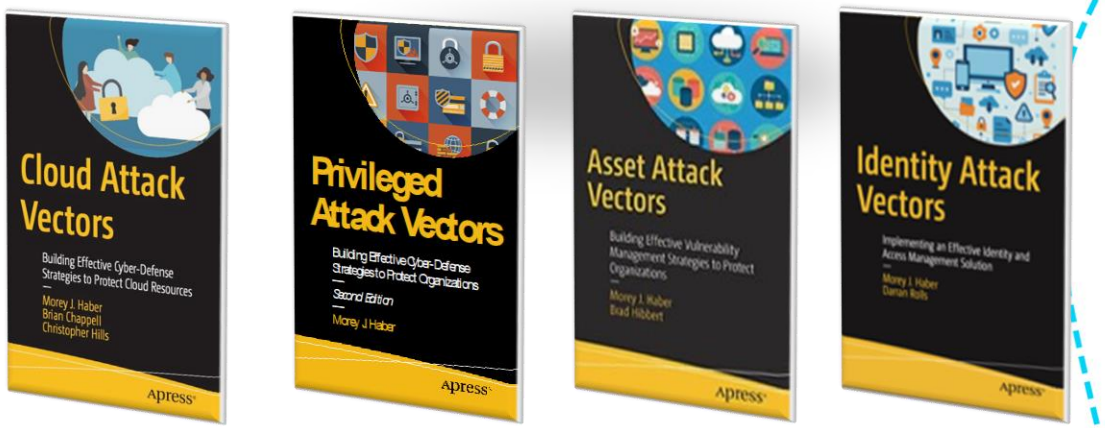
The 2023 Microsoft Vulnerabilities Report – Dissected

AGENDA

- Introductions
- The 2023 Microsoft Vulnerabilities Report
- Data Highlights, Trends, & Key Findings
- The Vulnerability Snowball Effect
- A Peek Ahead: The Evolving Microsoft Vulnerabilities Landscape
- Insights from Cybersecurity Experts
- How to Proactively Mitigate Microsoft-Based Vulnerability Risks
- Blended Threat Protection from BeyondTrust

Morey Haber, CSO, BeyondTrust

- 20+ years security experience
- Founding member of the industry group Transparency in Cyber
- Elected in 2020 to the Identity Defined Security Alliance (IDSA) Executive Advisory Board
- Articles on Forbes, Secure World, CSO Online, Dark Reading, and more
- Author of 4 Cybersecurity Attack Vector Books from Apress Media
- Contributing Author to the *Great Power Competition* on Cyber Risks to Critical Infrastructure



What's Inside?

- A **12-month consolidated view and analysis** of the vulnerabilities within Microsoft's platforms and products
- A **10-year review** of key shifts in vulnerability trends
- A **crucial barometer of the threat landscape** for the Microsoft ecosystem
- An **undeniable business case** for the importance of patching and enforcement of least privilege (removing admin rights, etc.) to reduce risk.

Microsoft Patch Tuesday

What Is It?

Patch Tuesday is the unofficial name of Microsoft's scheduled release of the newest security fixes for its Windows operating system and related software applications, as detailed in the Windows Security Updates Guide. It occurs on the second Tuesday of each month.

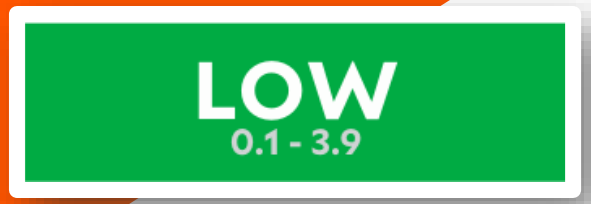
Why Do We Analyze This Data?

The annual Microsoft Vulnerabilities Report, compiled by BeyondTrust, provides a more holistic view of the Microsoft vulnerabilities landscape and best practices for threat reduction and mitigation.

#identiverse

The Common Vulnerability Scoring System (CVSS)

The industry-standard for identifying a vulnerability's severity level



A vulnerability whose **exploitation is extremely difficult**, or has minimal impact

Exploitability is **mitigated to a significant degree** by factors such as default configuration, auditing, or difficulty of exploitation

A vulnerability whose **exploitation could result in compromise** of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources

A vulnerability whose **exploitation could allow propagation of an internet worm without user action, and possibly without even a prompt**

Analysis Methodology

How vulnerabilities were classified:

- 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 or 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 10)

identiverse

The Impact Is Global

1.4 billion monthly active devices are running Windows 10 or 11.[1]

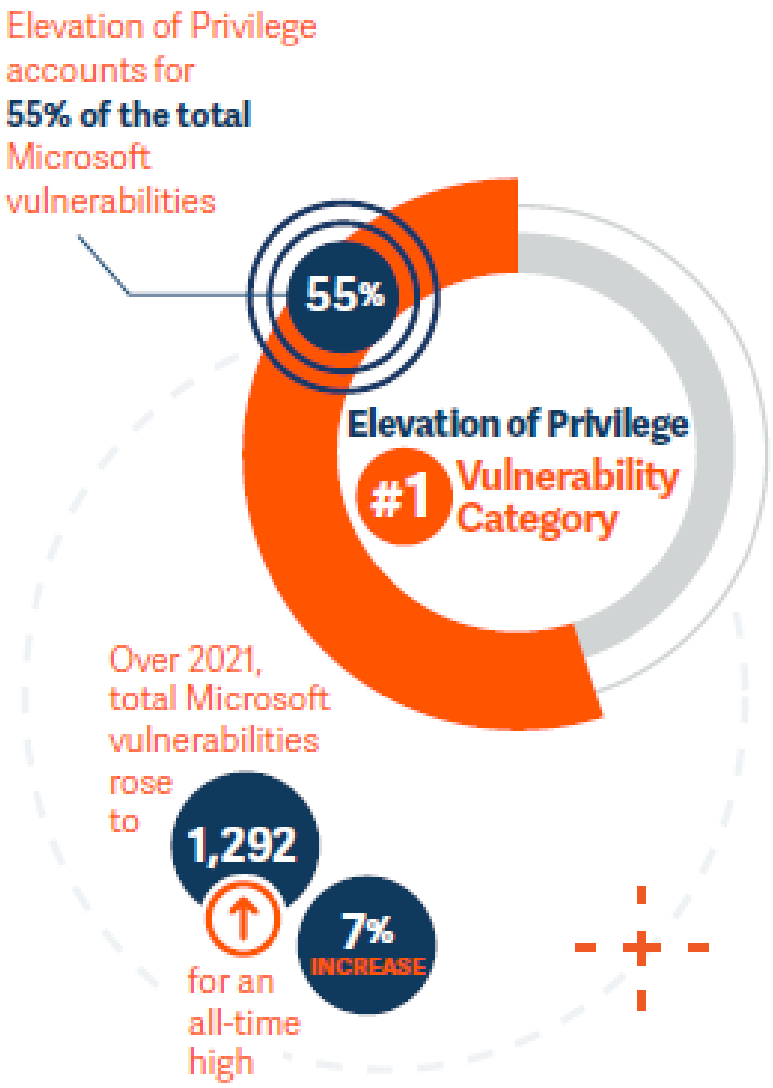
In addition to the 60 million Microsoft 365 consumer subscriptions; 25 million monthly active users on Power Platform; 270 million monthly active users on Teams.

identiverse

Microsoft Vulnerabilities Report 2023

Highlights & Key Findings

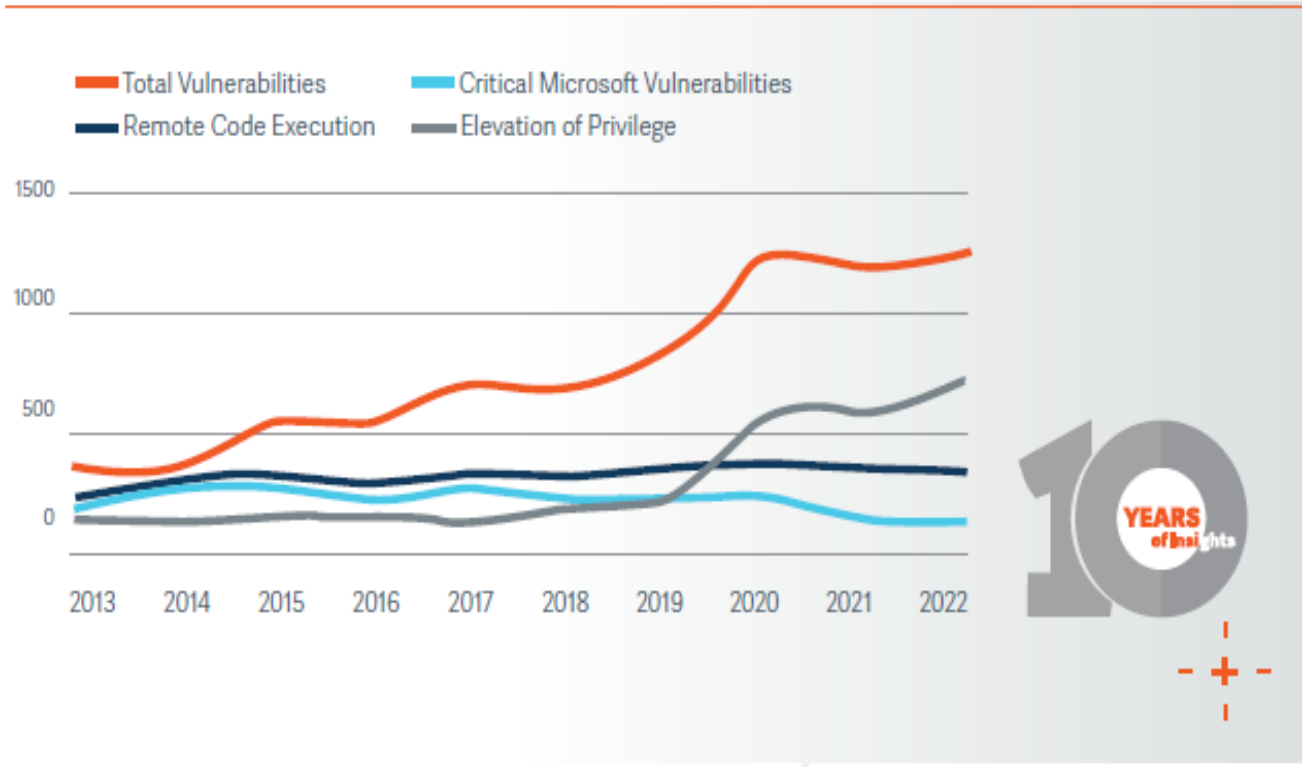
#identiverse



- Total Microsoft **vulnerabilities rose to 1,292, hitting an all-time high** since the report began 10 years ago.
- The **Elevation of Privilege category** dominates the Microsoft vulnerability landscape for the third year in a row and continues its rise.
- Microsoft Azure and Dynamics 365 are not only generating the biggest financial gains for Microsoft; they are also **propelling the biggest gains in number of vulnerabilities.**

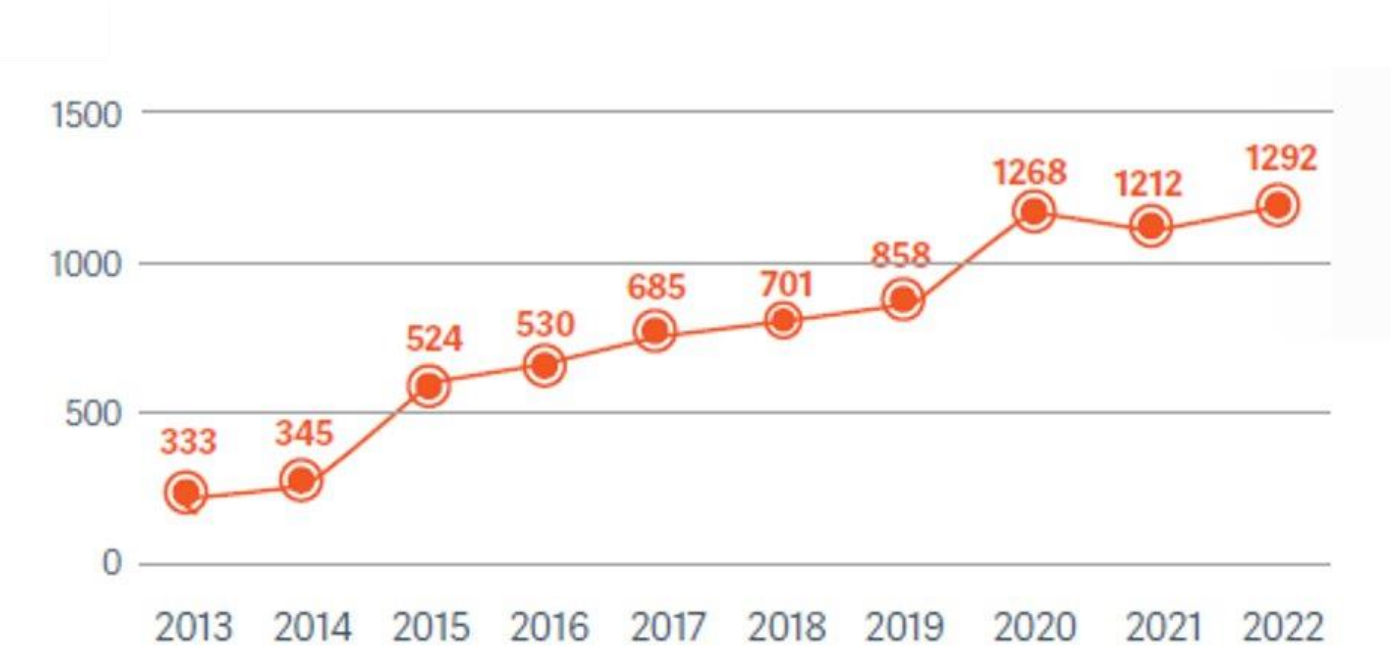
identiverse

A Snapshot of Microsoft Vulnerabilities Across a Decade *(2013 – 2022)*



#identiverse

Microsoft Total Vulnerabilities (2013 - 2022)



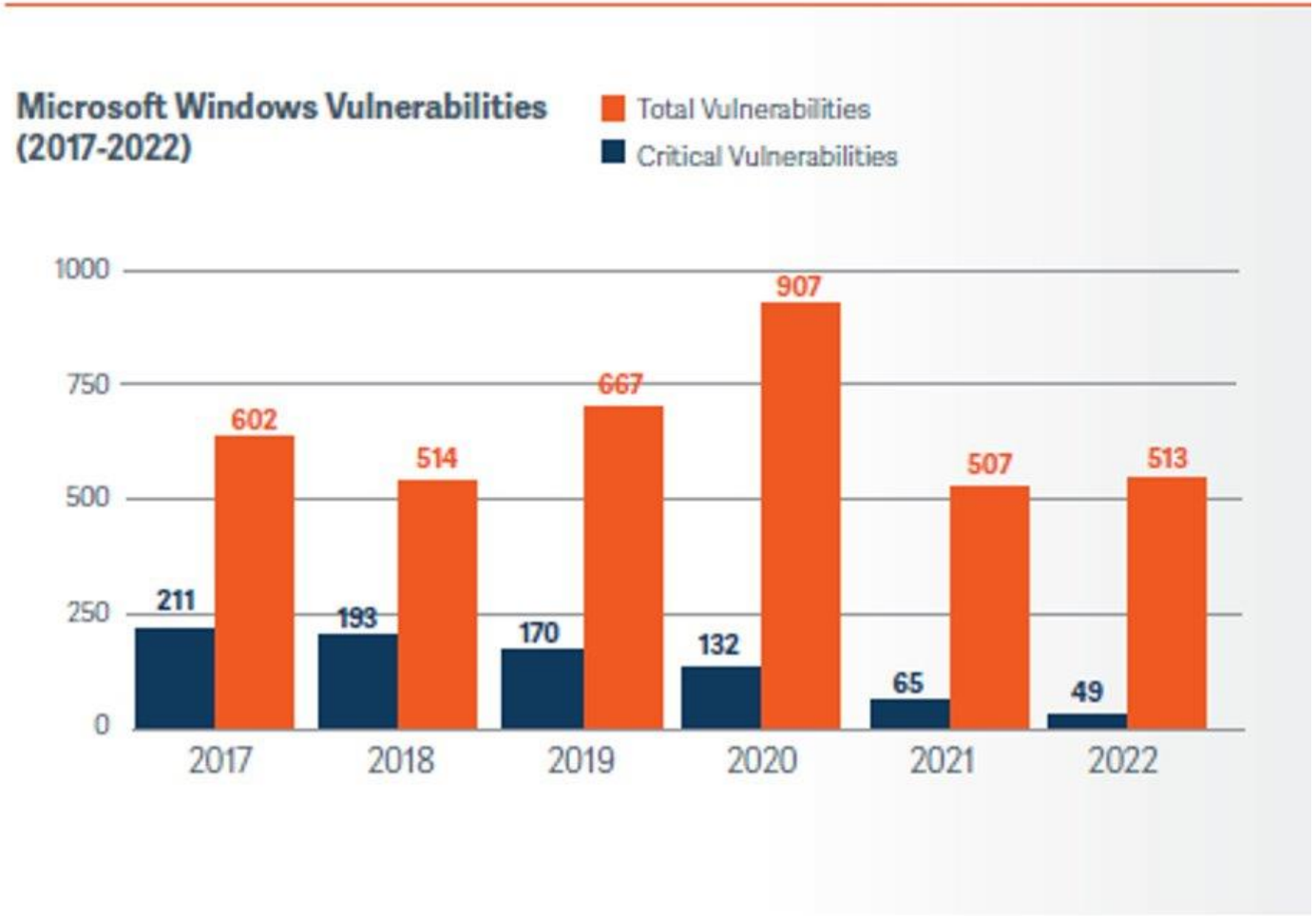
Total Microsoft vuln erabilities hit an all-time high

identiverse

*2017-2021 includes Internet Explorer, which was discontinued last year. 2022 figures are for Edge only.

identiverse

Microsoft Edge experienced 311 vulnerabilities last year, but none were critical.



There were 513 Windows vulnera bilities in 2022, 49 of which were critical.

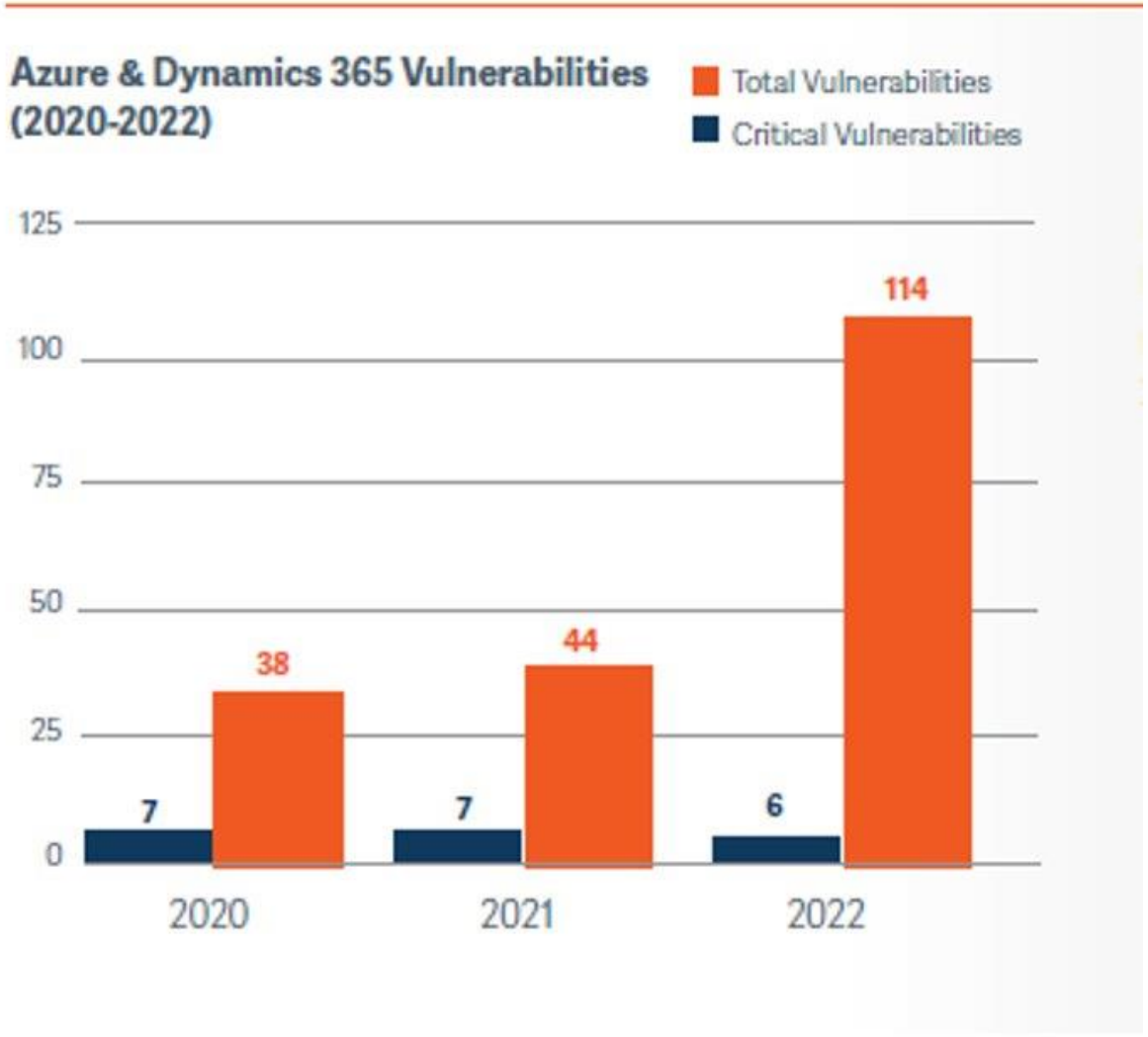
identiverse

Microsoft Office experienced a five-year low of 36 vulnerabilities in 2022.

identiverse

Windows Server vulnerabilities rose slightly to 552 in 2022, but critical vulnerabilities continued their decrease.

identiverse



Azure & Dynamics 356 vulnerabilities skyrocketed by 159%, from 44 in 2021 to 114 in 2022.

identiverse

Key Takeaway?

Vulnerabilities Spotlight

What can we learn?

The importance of proactively recognizing and mitigating vulnerabilities.

THANK YOU!

Available to chat at the BeyondTrust booth #1209

Morey Haber, CSO, BeyondTrust
mhaber@beyondtrust.com