FLEXERA™ 2021

State of IT Visibility Report

Hybrid IT infrastructure and vulnerability trends

Flexera

Inform IT. Transform IT.™

Reuse

We encourage the reuse of data, charts and text published in this report under the terms of this **Creative Commons Attribution 4.0 International License**.

You are free to share and make commercial use of this work as long as you attribute the ***Flexera 2021 State of IT Visibility Report*** as stipulated in the terms of the license.

Table of contents

Table of figures

Report highlights

FLEXERA™ 2021

State of IT Visibility Report

FLEXERA™ 2021

State of IT Visibility Report

The IT landscape is rapidly evolving as enterprises digitally transform and respond to major market and societal upheavals

Executive summary

Keeping technology assets secure, well-governed and cost effective is a formidable challenge. IT leaders need comprehensive, clear insights into their technology to fuel the data-driven decision making that leads to better results.

This inaugural *Flexera 2021 State of IT Visibility Report* combines detailed survey respondent information with the industry expertise and data of Flexera's renowned Secunia Research and Technopedia research teams to shed light on what's happening with information technology and the data that supports the vast array of business initiatives around the world.

Visibility into IT data—especially toward adaptability to changing technology—is foundational to organizational success. IT lifecycle and risk management in a sprawling tech landscape is both complex and dynamic, with thousands of applications and services scattered across hundreds of providers. Enterprises need complete, accurate and up-to-date visibility into every technology asset in their estates to effectively manage it all.

This report explores the thinking of more than 300 global technology decision makers and users about IT infrastructure, asset management, vulnerability posture and industry trends. It shares their current and future IT management strategies alongside tactical data regarding software obsolescence and vulnerability mitigation for strategic planning.

Methodology

More than 300 global technology decision makers and users from around the globe and across a broad cross-section of industries participated in the *Flexera 2021 State of IT Visibility Report* survey. Respondents provided insights into their IT infrastructure, asset management, vulnerability posture and industry trends. The survey was conducted in April and May of 2021.

Terminology used throughout the report

End of life (EOL) is the last date that full support for a product is provided by a vendor/manufacturer, captured as it was originally published by the vendor. Partial support may still be available.

End of support (EOS) is the last date on which any support is provided by a vendor/manufacturer. The only support available after this date might be online self-help support.

Vulnerability is an error in software which can be exploited with a security impact and gain.

Exploit is malicious code that takes advantage of vulnerabilities to infect a computer or perform other harmful actions.

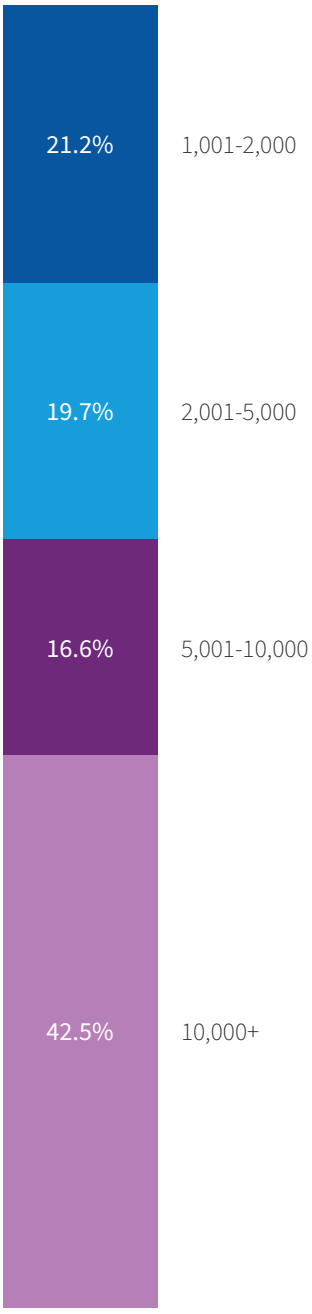
Demographics

Survey respondents included enterprise organizations (public- or private-sector) with 1,000 or more employees across the globe. The majority of these respondents are from organizations with more than 10,000 employees, and the majority of respondents are from the United States, as figures 1 and 2 indicate.

FIGURE 1

The majority of respondents are from large enterprises

How many employees are in your company?



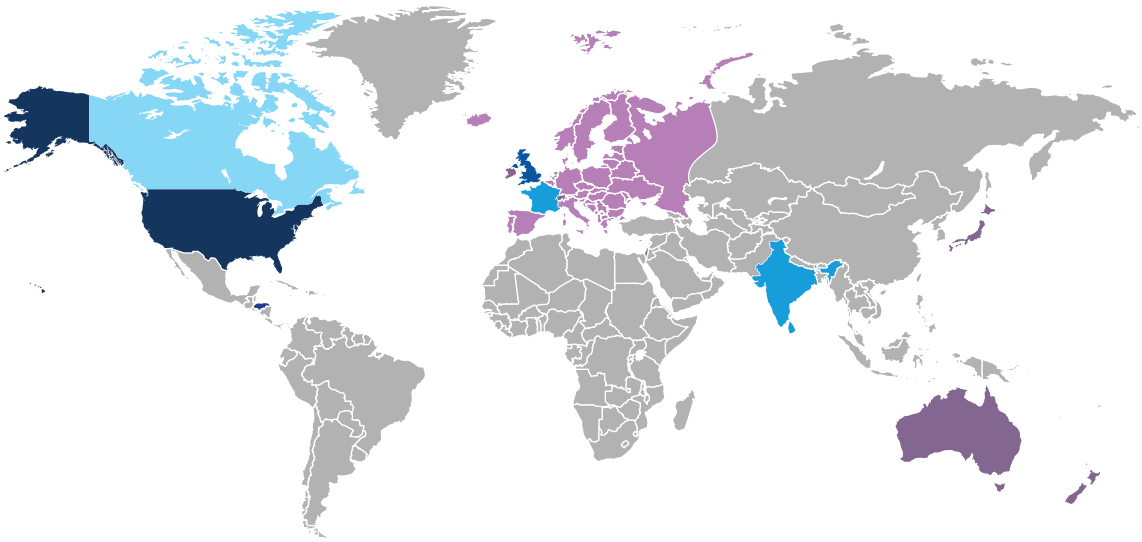
N=325

Source: Flexera 2021 State of IT Visibility Report

FIGURE 2

The majority of respondents are from the United States

In what country is your company headquarters or main office?



United States	85.9%	Denmark	0.6%	Israel	0.3%
United Kingdom	4.6%	Germany	0.6%	Japan	0.3%
France	1.5%	Netherlands	0.6%	New Zealand	0.3%
India	1.5%	Other Europe	0.6%	Switzerland	0.3%
Canada	1.2%	Australia	0.3%		
Other	0.9%	Ireland	0.3%		

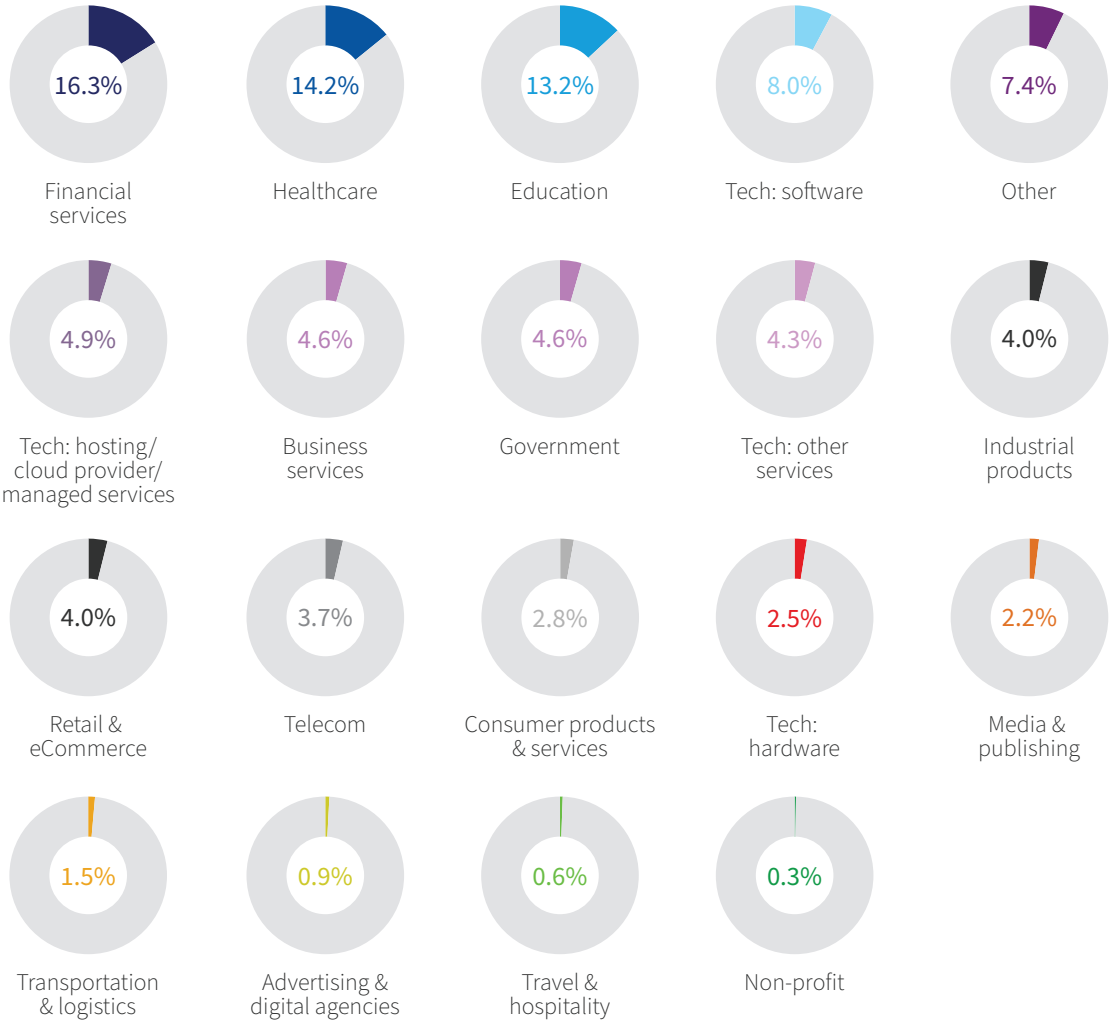
N=325

Source: Flexera 2021 State of IT Visibility Report

FIGURE 3

Financial services and *healthcare* lead respondents' industries

In what industry is your company?



N=325

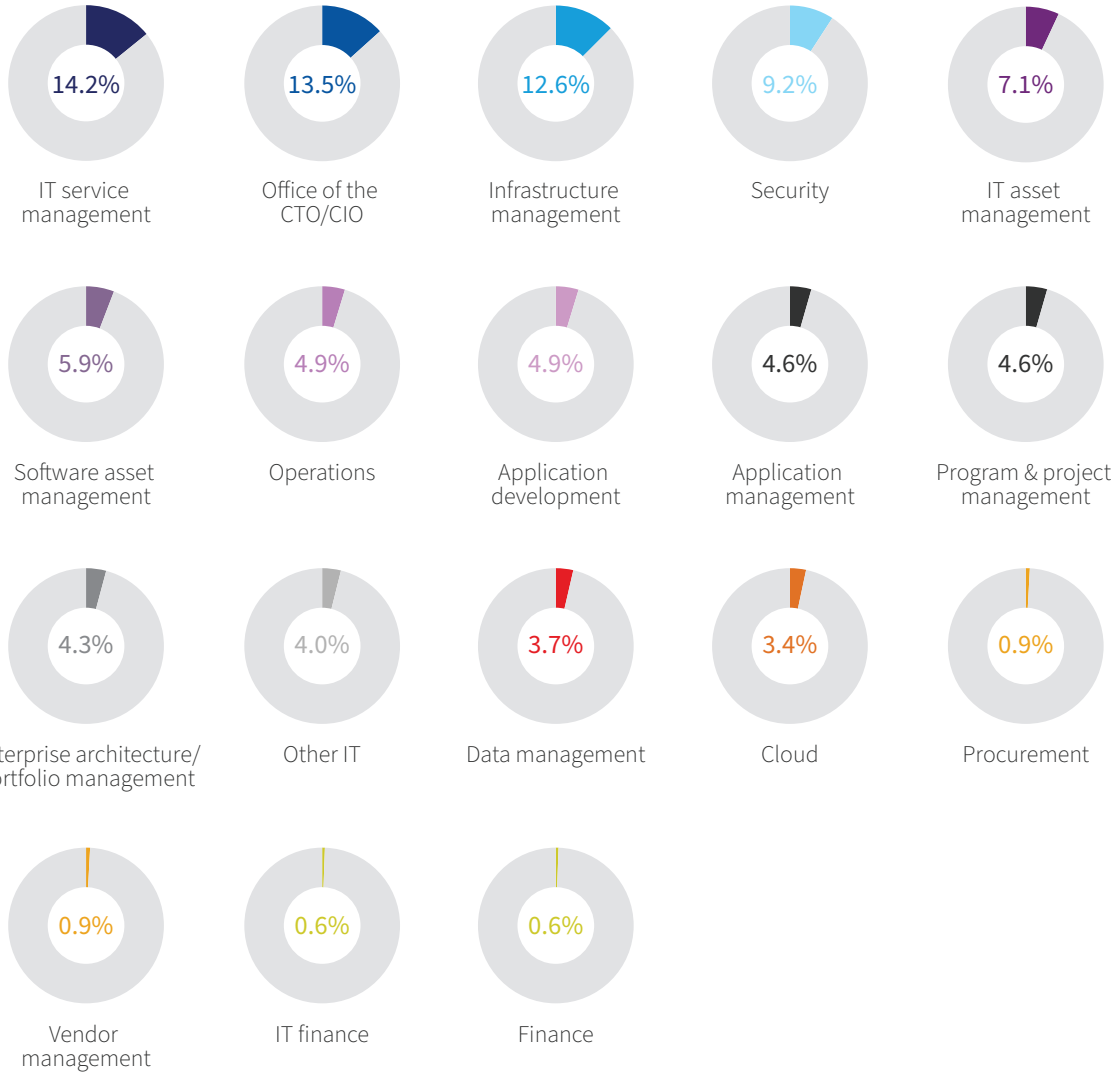
Source: Flexera 2021 State of IT Visibility Report

Technology touches every company in every industry. The insights in this report originate from a range of industries, but the top three represented are *financial services, healthcare* and *education*.

FIGURE 4

Most respondents are in IT management

What best describes the function in which you work?



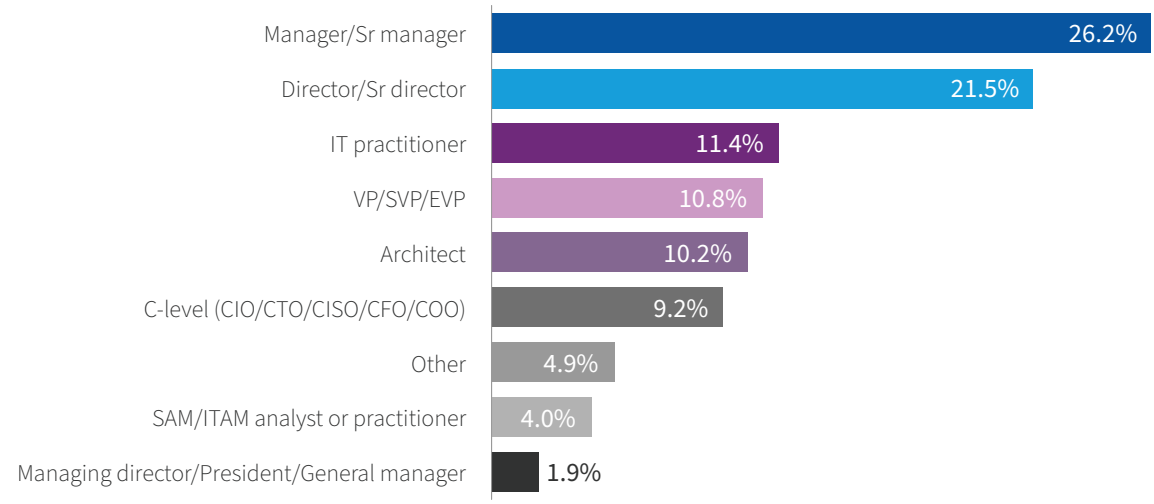
N=325

Source: Flexera 2021 State of IT Visibility Report

Respondents' top three job functions were *IT service management, the office of the CTO/CIO* and *infrastructure management*, and 26.2 percent noted their role was a *manager* or *senior manager*.

FIGURE 5

Most respondents are managers or directors



N=325

Source: Flexera 2021 State of IT Visibility Report

EOL, EOS and vulnerability review

This report augments survey responses with software asset lifecycle information from Flexera's Technopedia IT asset database and with vulnerability data compiled by Flexera's Secunia Research team. Technopedia provides intelligence on more than 4.1 million assets across the technology landscape and is updated daily. Secunia Research monitors more than 65,000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.

What does end-of-life and end-of-support review cover?

This report focuses specifically on software products. End-of-life and end-of-support (EOL/EOS) software asset lifecycle information for 2020 and 2021 is drawn from the Technopedia IT asset data repository. Technopedia's EOL/EOS data enables critical decision making about IT environments based on what software is no longer being patched or supported. Technopedia's lifecycle data enables risk forecasting in critical business services based on upcoming EOL/EOS dates. For resources that can't be upgraded, businesses can anticipate the impact of increased costs for extended support.

What does the vulnerability review cover?

The systems and applications monitored by Secunia Research are those in use in the environments of the customers of Flexera's Software Vulnerability Management solutions. The vulnerabilities verified by Secunia Research are described in Secunia Advisories and listed in the Flexera vulnerability database, detailing what IT security teams need to know to mitigate the vulnerability risk posed in their environments. The Secunia Advisory descriptions include criticality, attack vector, exploitability and solution status.

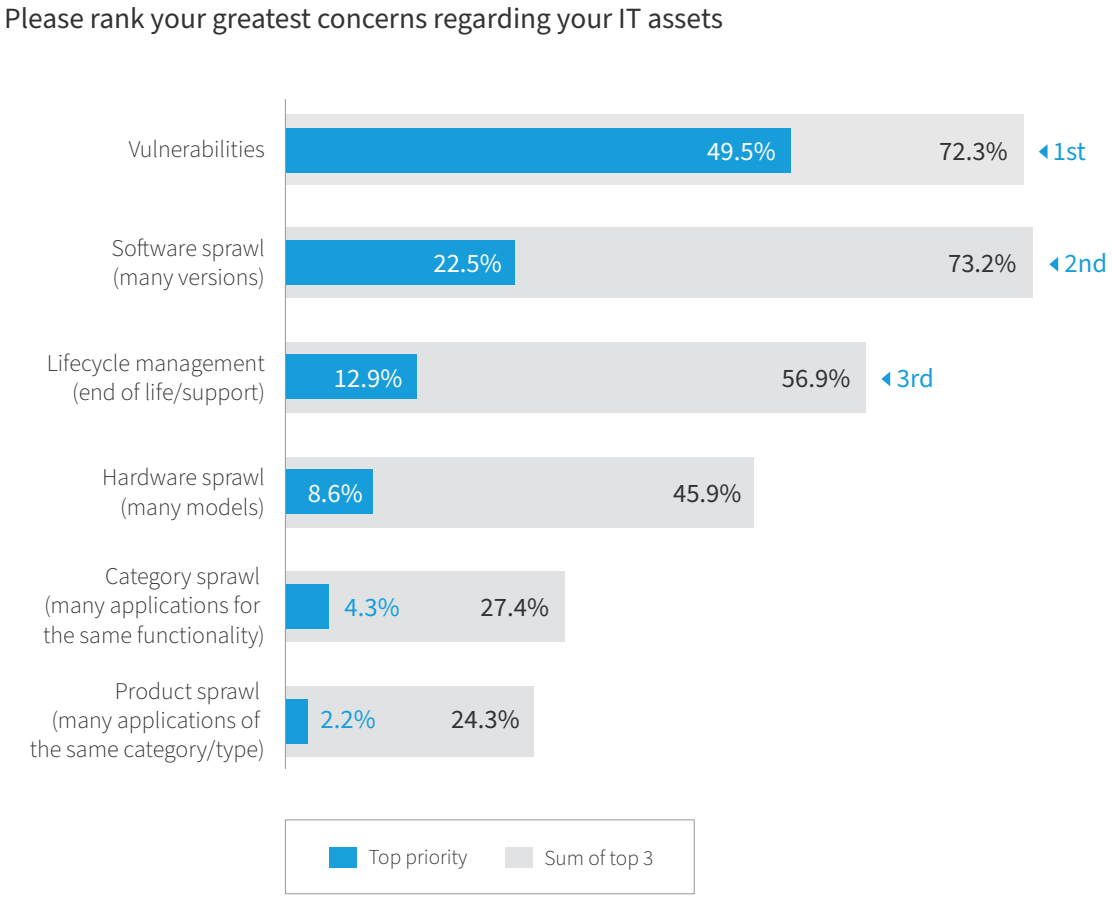
How do we count vulnerabilities?

Research housed in the vulnerability management space adopted different approaches to counting vulnerabilities. For this report, Secunia Research counts vulnerabilities per product release from a vendor that is EOL/EOS and in which the vulnerability appears. This method is applied to reflect the level of information customers need to keep their environments secure. Secunia provides verified intelligence listing all products affected by a given vulnerability.

Report highlights

Vulnerabilities and *software sprawl* were ranked by survey respondents as the top concerns about organizations' IT assets, as indicated by figure 11A.

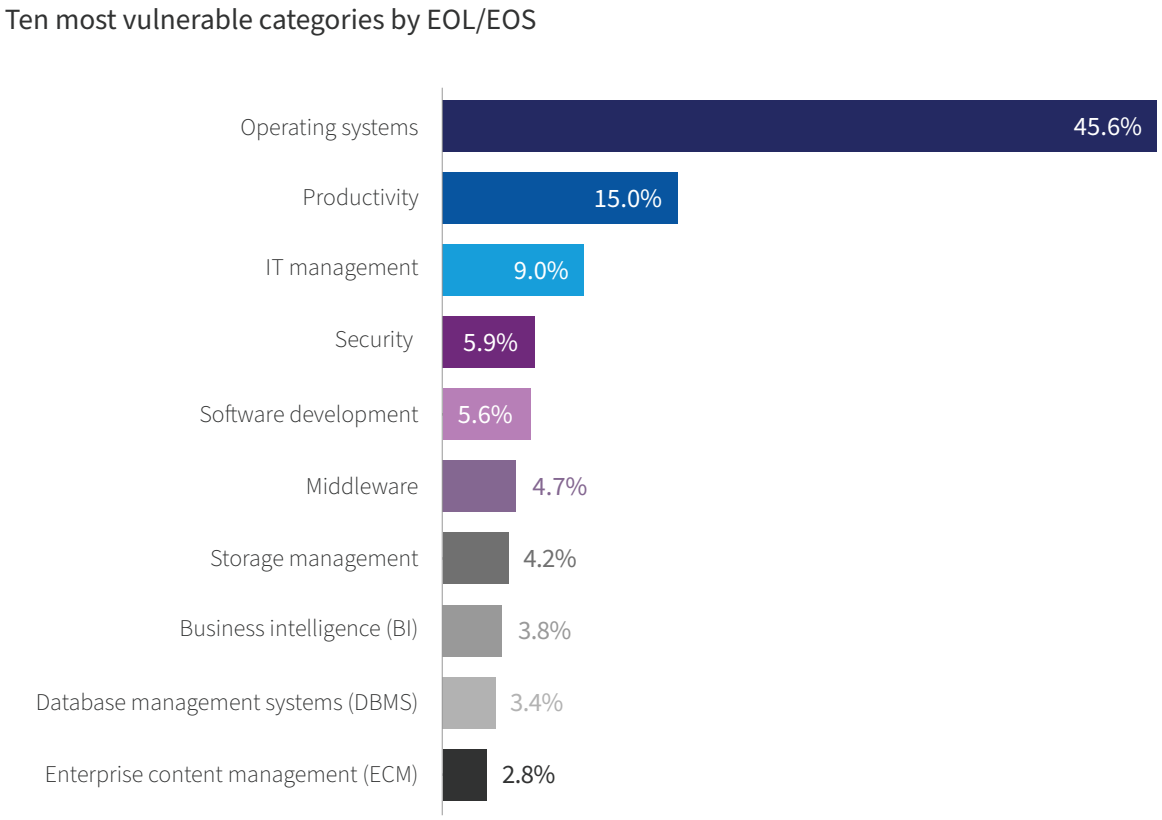
FIGURE 11A
Vulnerabilities lead the list of concerns about IT assets



N=325
Source: Flexera 2021 State of IT Visibility Report

In figure 34, respondents indicated that *operating systems* and *productivity* were the most vulnerable categories when considering EOL/EOS, followed by *IT management*.

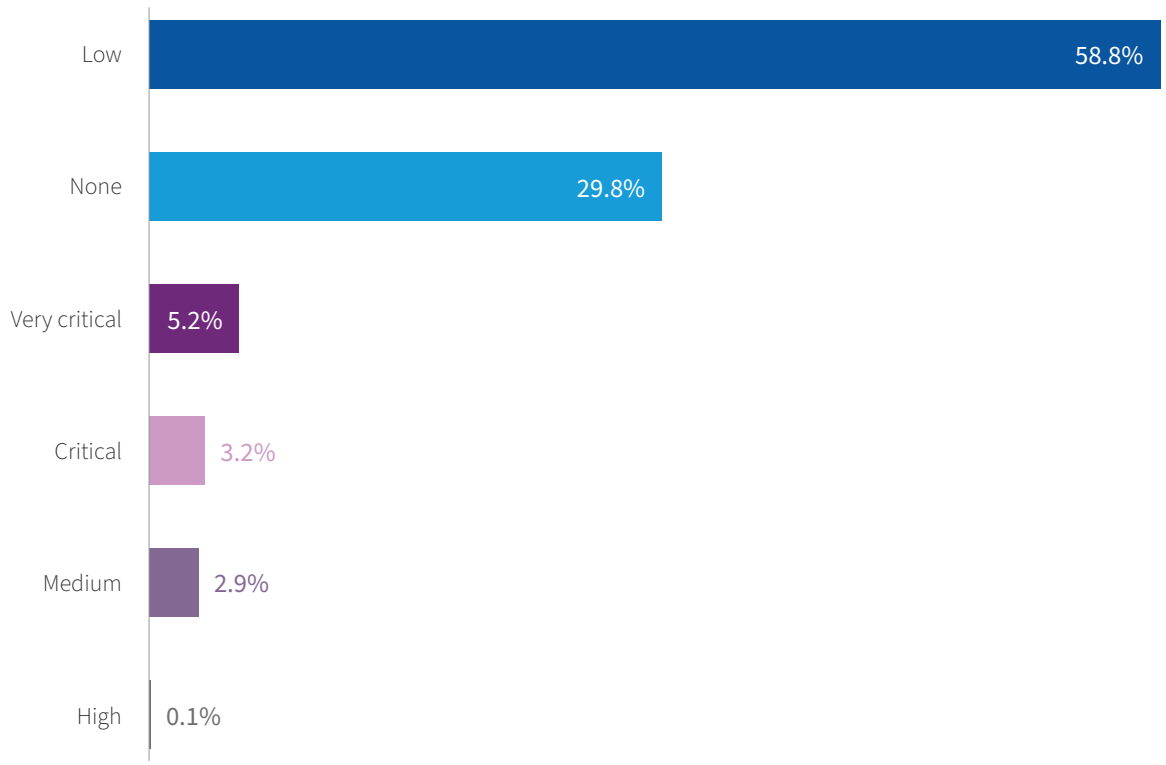
FIGURE 34
The most vulnerable category by EOL/EOS is *operating systems*



Source: Flexera 2021 State of IT Visibility Report

IT professionals need to be aware that most EOL/EOS software will have a low threat severity as shown in figure 26—but programs that focus solely on high-range and very critical threat scores will miss the majority of vulnerabilities in need of remediation by overlooking low-range scores.

FIGURE 26
Most vulnerabilities in EOL/EOS software have low threat severity



Source: Flexera 2021 State of IT Visibility Report

Survey insights

Survey insights

Priorities and initiatives for technology professionals in 2021

The COVID-19 pandemic has forever transformed the way enterprises do business. In the aftermath of this tumultuous year, the widespread changes in the way we use and perceive technology continue in 2021. Many organizations have moved to a remote workforce and were forced to invest in—and fast-track—their digital transformation initiatives.

This rapid evolution of the IT space opened the door for a variety of opportunities, but it also introduced a host of challenges. Remaining competitive in this new environment requires enterprises to optimize their technology investments. It is essential that IT leaders understand what has been, is now and will be running in their IT estates and the impact all of this will have on their business initiatives.

Flexera surveyed more than 300 global technology decision makers and users about these topics to better understand how they see their current and future IT management strategies. This section highlights some of the key takeaways and trends related to their priorities and initiatives in 2021 and beyond.

Visibility and data sharing vary across teams

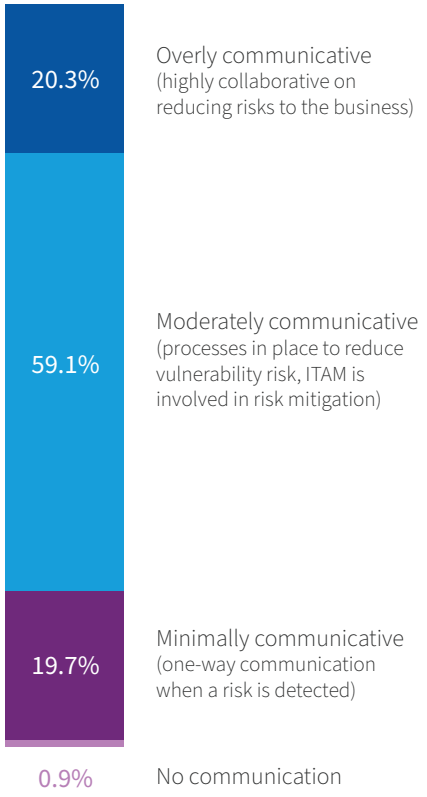
Security and IT are typically perceived as siloed programs, operating their domains with little cross-functionality. *Flexera 2021 State of IT Visibility Report* survey responses indicate there's more collaboration across the organization than anecdotal evidence may lead us to believe.

Across the respondents in this report, less than one percent had no communication between IT asset management (ITAM) teams and security operations (SecOps). The fact that 79.4 percent reported *moderate to over-communication* when it comes to vulnerability and risk mitigation practices is a positive sign that teams are addressing the increase in security exposure in the technology industry.

FIGURE 6

Good communication between teams is the rule

What is the relationship between security operations (or like team) and IT asset management teams?



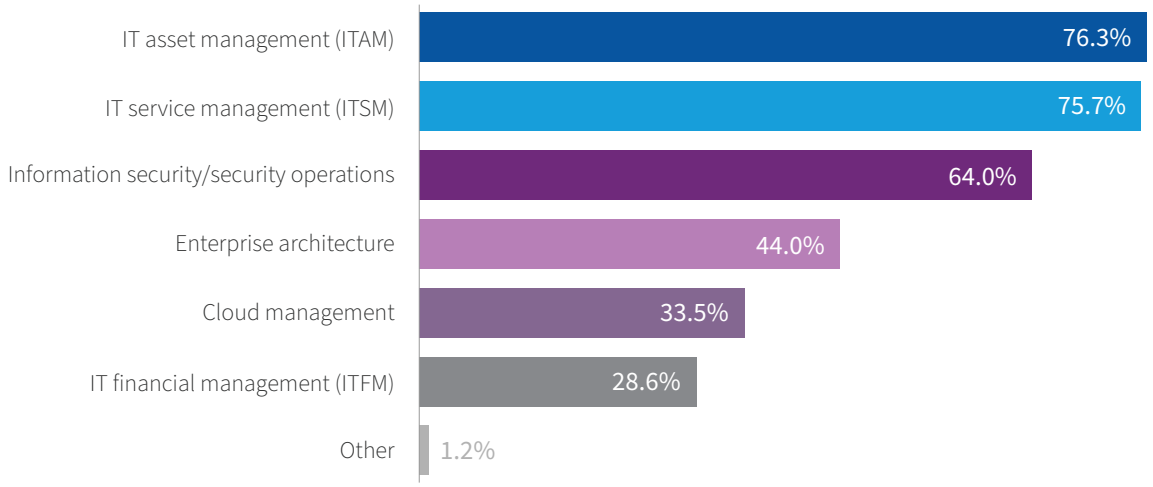
N=325
Source: Flexera 2021 State of IT Visibility Report

However, that sharing of data doesn't extend across all IT-related disciplines. *Enterprise architecture (EA)*, *cloud management* and *IT financial management (ITFM)* teams aren't receiving the same amount of interaction, with inventory data—the foundation on which many IT business initiatives are built—shared between these teams at 44, 33.5 and 28.6 percent, respectively. This low incidence of collaboration may be seen in EA projects such as IT network and service updates and how they line up with IT service management (ITSM) processes.

FIGURE 7

Inventory data sources are shared most by ITAM and ITSM

Which of the following teams use the same inventory data sources (check all that apply)?

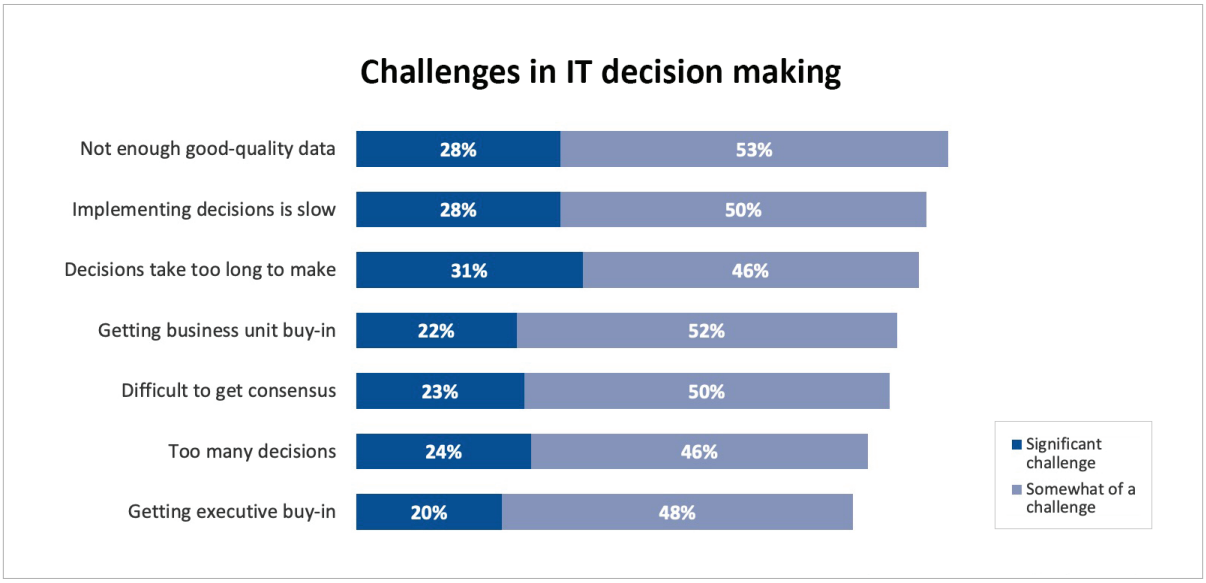


N=325

Source: Flexera 2021 State of IT Visibility Report

This also corresponds with the findings in *Flexera's 2021 State of Tech Spend Report*, in which respondents cited *not enough good-quality data* as the biggest challenge when asked what most hampers their ability to make technology decisions.

FIGURE 8
Lack of good data is the top challenge in IT decision making



N=474
Source: Flexera 2021 State of Tech Spend Report

Although EA, cloud and ITFM teams aren't always receiving the same data, organizations felt they have at least some—if not complete—visibility into the technology that powers their business outcomes. As illustrated in figure 9, only 5.2 percent of respondents said they did not know or did not feel they had accurate visibility into IT assets and their business outcomes.

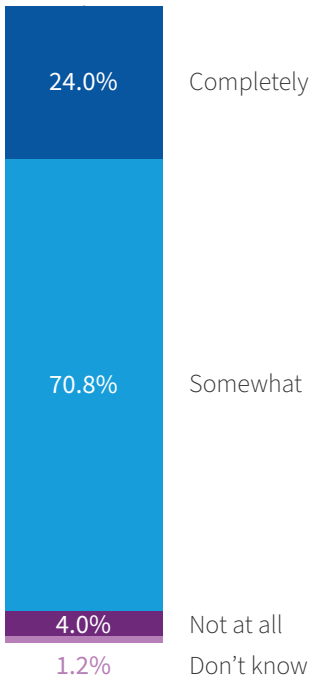
While most IT professionals feel they have this insight, it seems that visibility is limited to the on-premises space. Almost three-quarters (73.9 percent) of respondents reported accurate visibility into their *on-premises hardware*, and 68.3 percent reported accurate visibility into their *on-premises software*. That visibility drops considerably when we investigate *cloud instances* (45.9 percent), *SaaS* (40.9 percent) and *license position* (36.9 percent), where respondents were far less confident in the accuracy of their IT estates.

As the industry evolves toward an expanded purview of SAM teams and the need for foundational data across the ecosystem—often supplied by configuration management databases (CMDBs) or other similar data sources—this view of the hybrid estate will become increasingly important.

FIGURE 9

Less than 25% of organizations have complete visibility into IT assets

Does your organization have accurate visibility into your IT assets and their impact on business outcomes?



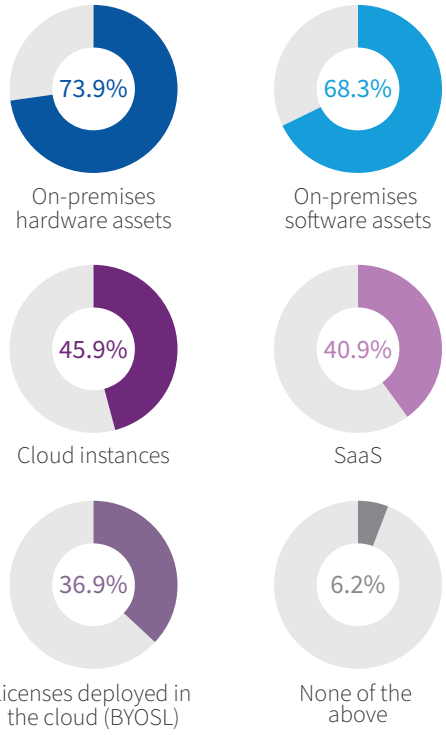
N=325
Source: Flexera 2021 State of IT Visibility Report

Flexera

FIGURE 10

Visibility into IT environments is limited outside of on-premises

Do you feel that you have accurate visibility into the following environments?



N=325
Source: Flexera 2021 State of IT Visibility Report

Flexera

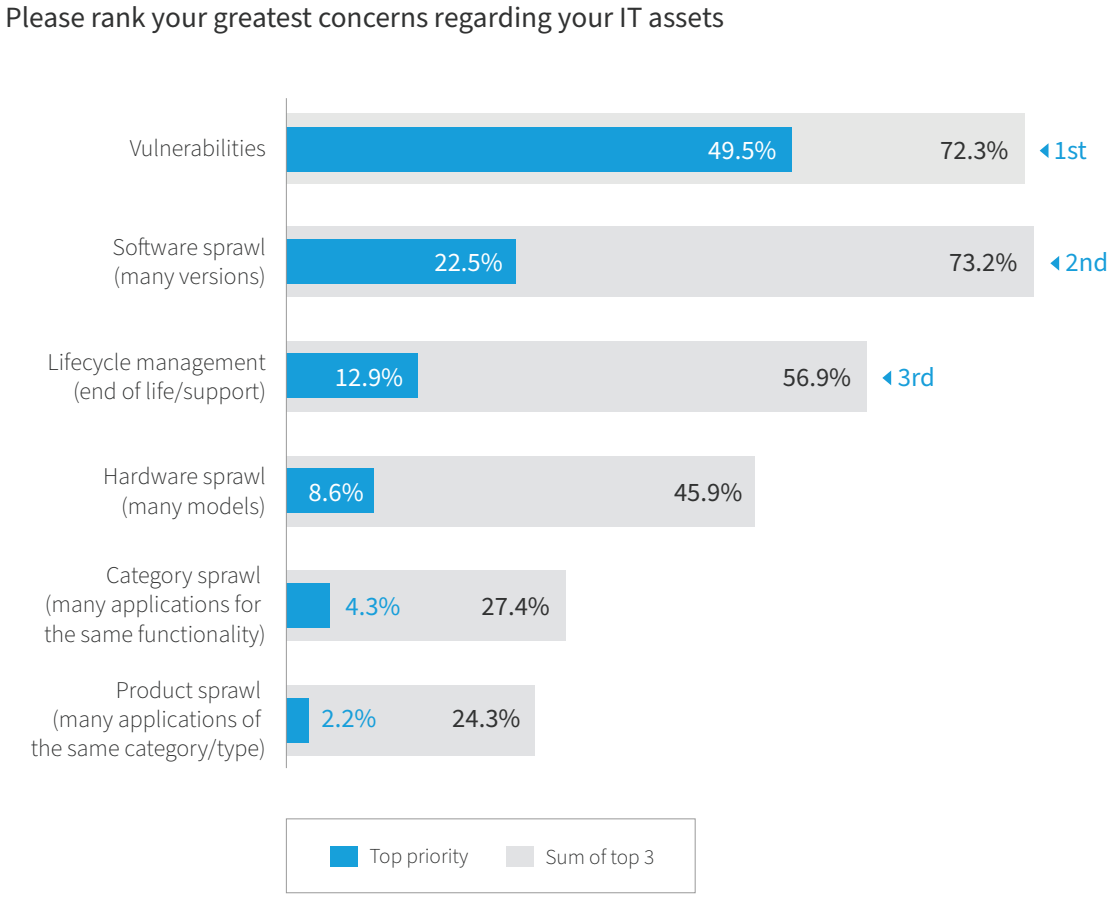
Vulnerability and lifecycle management is essential

Hackers—and the havoc they wreak—continue to make headlines and cause headaches for IT leaders. So it's no surprise that 49.5 percent of respondents ranked *vulnerabilities* as the greatest concern about their IT assets.

Following close behind were the *sprawl of software* and *lifecycle management.* Identifying which software applications have multiple versions installed across the organization helps reduce licensing fees through rationalization of software that's no longer in use. It also helps in the discovery of older versions of applications that could be at risk.

FIGURE 11A

Vulnerabilities lead the list of concerns about IT assets

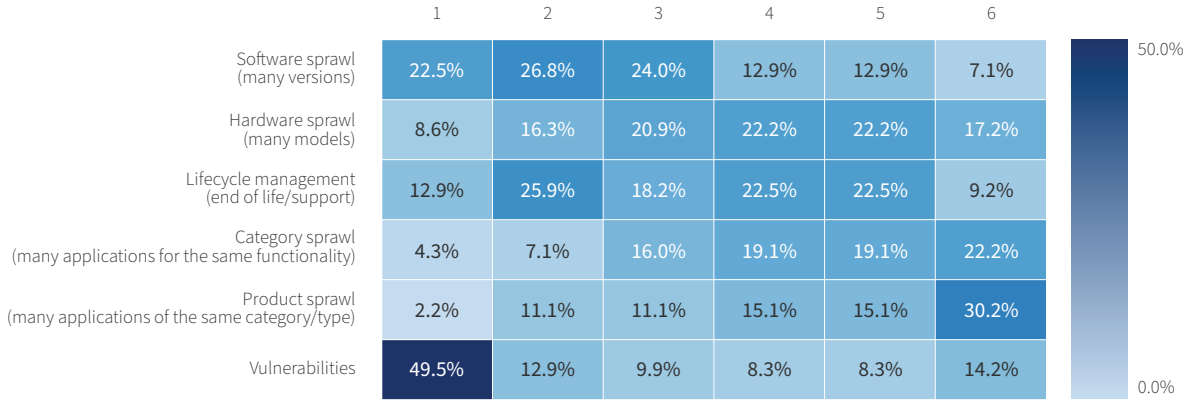


N=325
Source: Flexera 2021 State of IT Visibility Report

FIGURE 11B

Vulnerabilities lead the list of concerns about IT assets

Please rank your greatest concerns regarding your IT assets



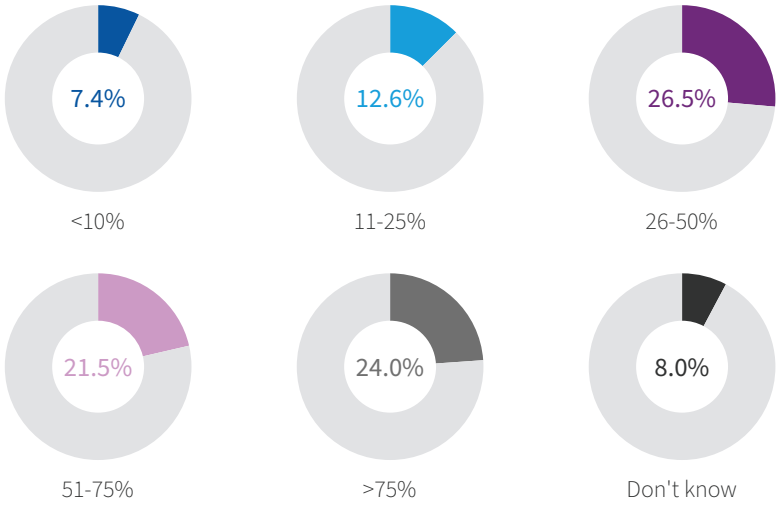
N=325
Source: Flexera 2021 State of IT Visibility Report

FLEXERA

FIGURE 12

Majority of respondents patch 50% or less of vulnerabilities

How many applications do you actively patch (estimated)?



N=325
Source: Flexera 2021 State of IT Visibility Report

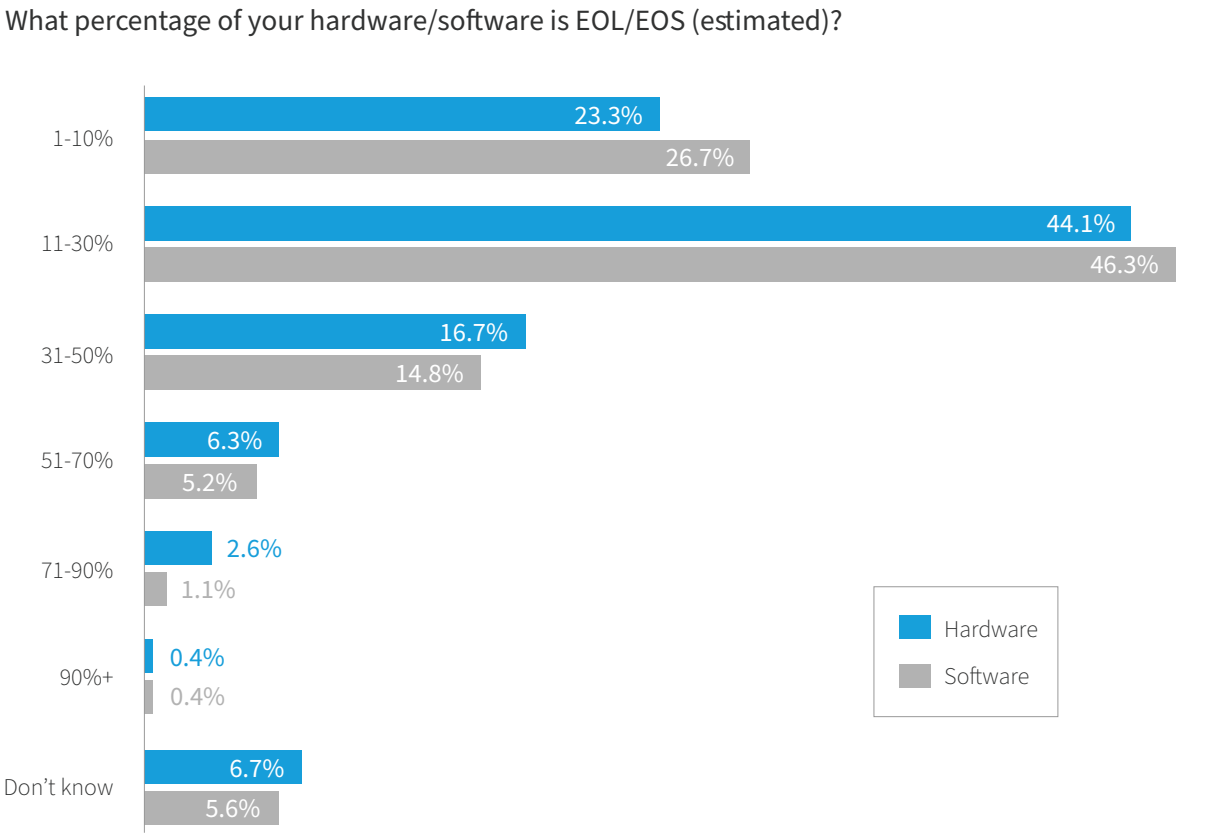
FLEXERA

Risk management can be an overwhelming endeavor, and can frequently outstrip the capacity of IT teams. As shown in figure 12, almost half (45.5 percent) of respondents patch half or more of their vulnerable applications. A majority—54.5 percent—patch less than 50 percent of vulnerabilities or aren't sure of what they're patching. Current and accurate IT asset data can help IT professionals understand where vulnerabilities arise and effectively prioritize what to patch.

Effective lifecycle management can reduce exposure to vulnerabilities and limit software sprawl, and respondents generally felt their on-premises IT estates were well-managed. Figure 13 shows that 67.4 percent reported that 30 percent or less of their hardware was EOL/EOS, and 73 percent said 30 percent or less of their software was EOL/EOS.

FIGURE 13

Majority of respondents indicated up to 30% of hardware/software is EOL/EOS



N=325

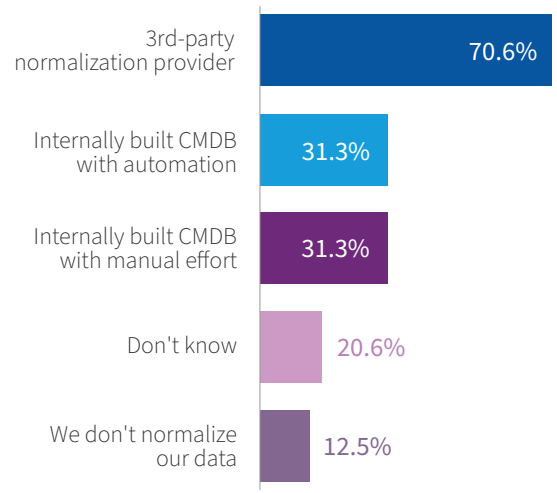
Source: Flexera 2021 State of IT Visibility Report

Normalization of data

These perceptions may be the result of a focus on data normalization, through which asset inventory data is confirmed as correct and is consolidated to remove duplicative and superfluous information. Figure 14 indicates that IT professionals are investing in the tools to improve their data foundations, with 70.6 percent of respondents using a *third-party tool* either on its own or *in combination with an internal CMDB effort*.

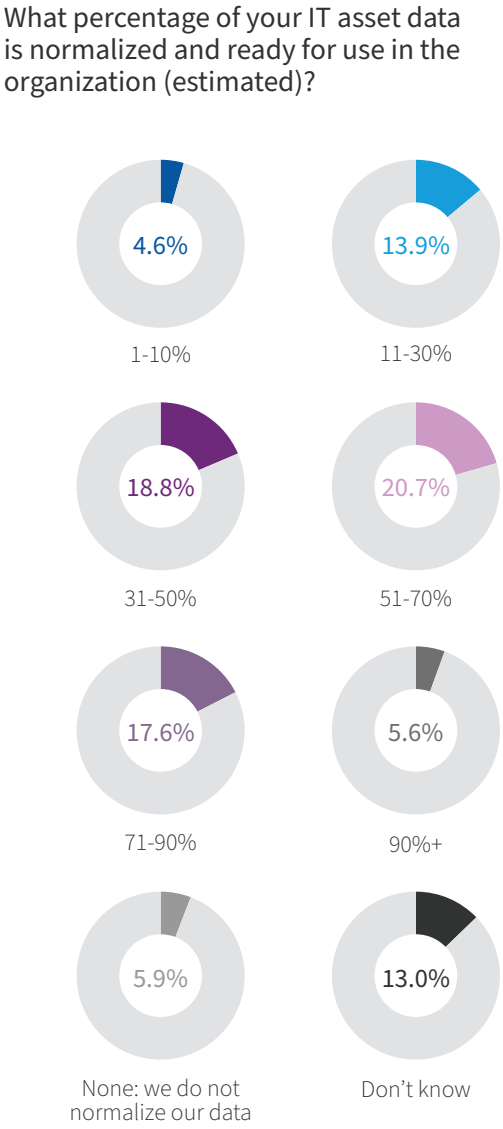
However, they're not getting the results they should. As shown in figure 15, more than half (56.2 percent) of survey respondents had 50 percent or less of their IT data normalized, weren't able to provide an estimate or had no effort to normalize in place.

FIGURE 14
Most organizations use normalization technologies



N=325
Source: Flexera 2021 State of IT Visibility Report

FIGURE 15
Only 50% or less of data is normalized for majority of respondents



N=325
Source: Flexera 2021 State of IT Visibility Report

Asset inventory data is enhanced with a business service context

A business service context can be of significant value in asset inventory data management. Such context shows how services such as customer relationship management (CRM) or payroll are powered by IT assets.

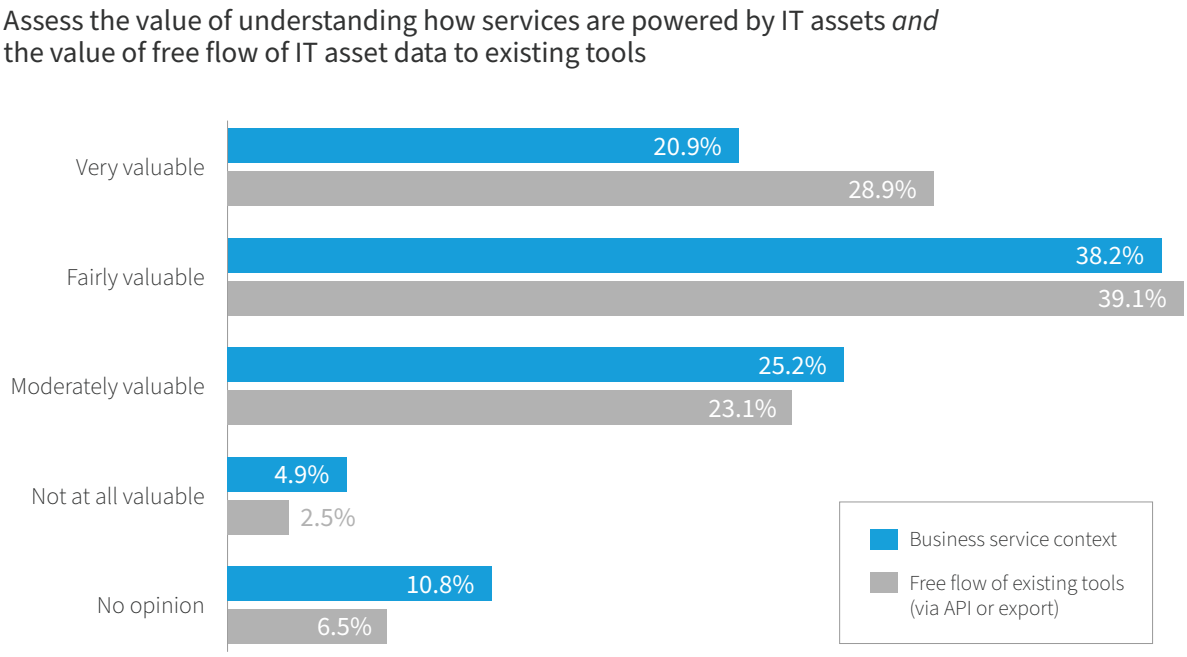
More than 80 percent (84.3) of respondents felt a business service context would be *moderately*, *fairly* or *very valuable*. And 91.1 percent responded similarly when asked about the perceived value of IT asset data's shareability between existing tools in the technology ecosystem.

The data indicates that IT professionals want to understand where their assets are affecting the business and how to use that data across their tooling. But getting clean and clear data across the IT estate remains a challenge.

Current and accurate IT asset data can help IT professionals better understand where their assets have sprawled, which assets have become obsolescent and where vulnerabilities arise in order to effectively prioritize remediation.

FIGURE 16

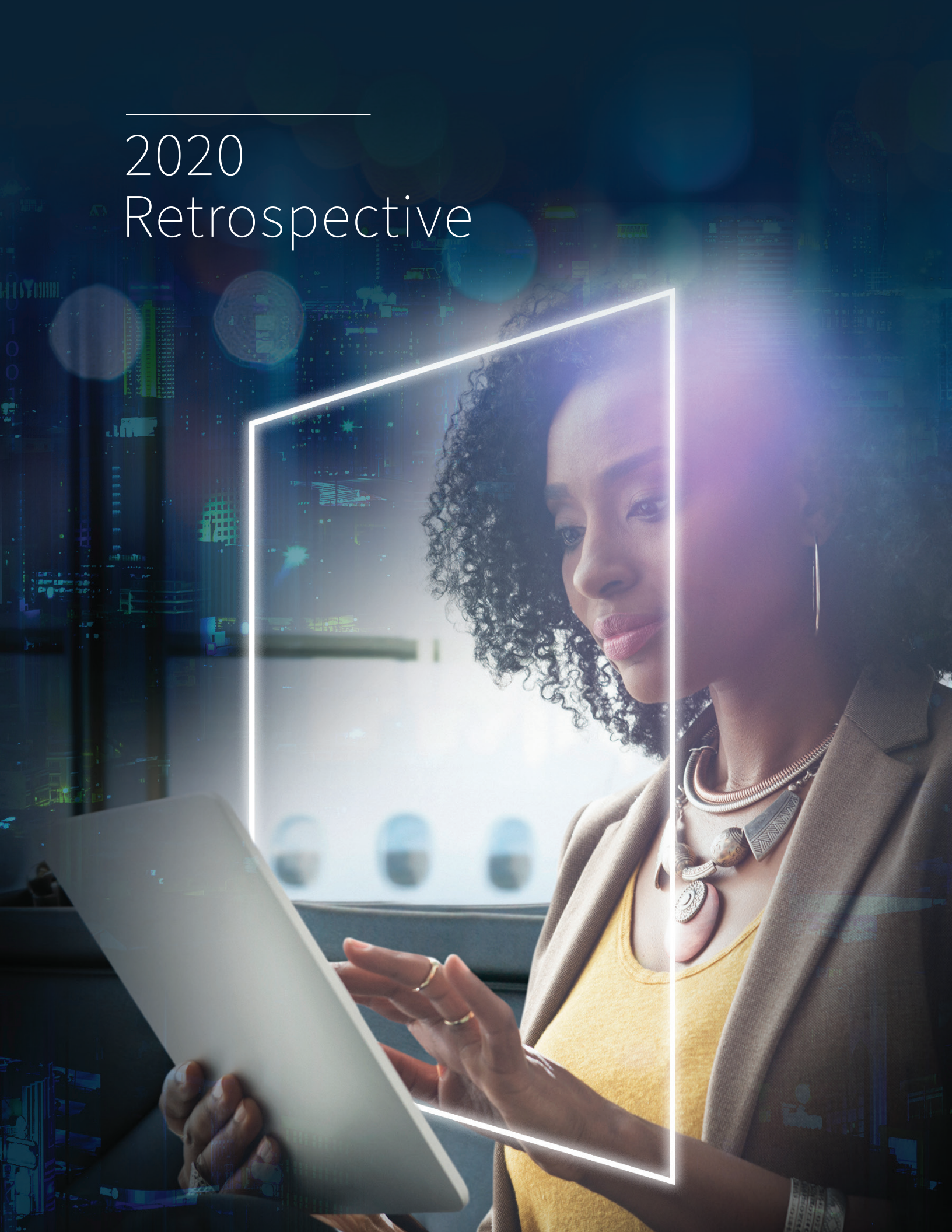
Respondents find context and application of IT asset data valuable



N=325

Source: Flexera 2021 State of IT Visibility Report

2020 Retrospective



2020 Retrospective

End of life, end of support and vulnerabilities

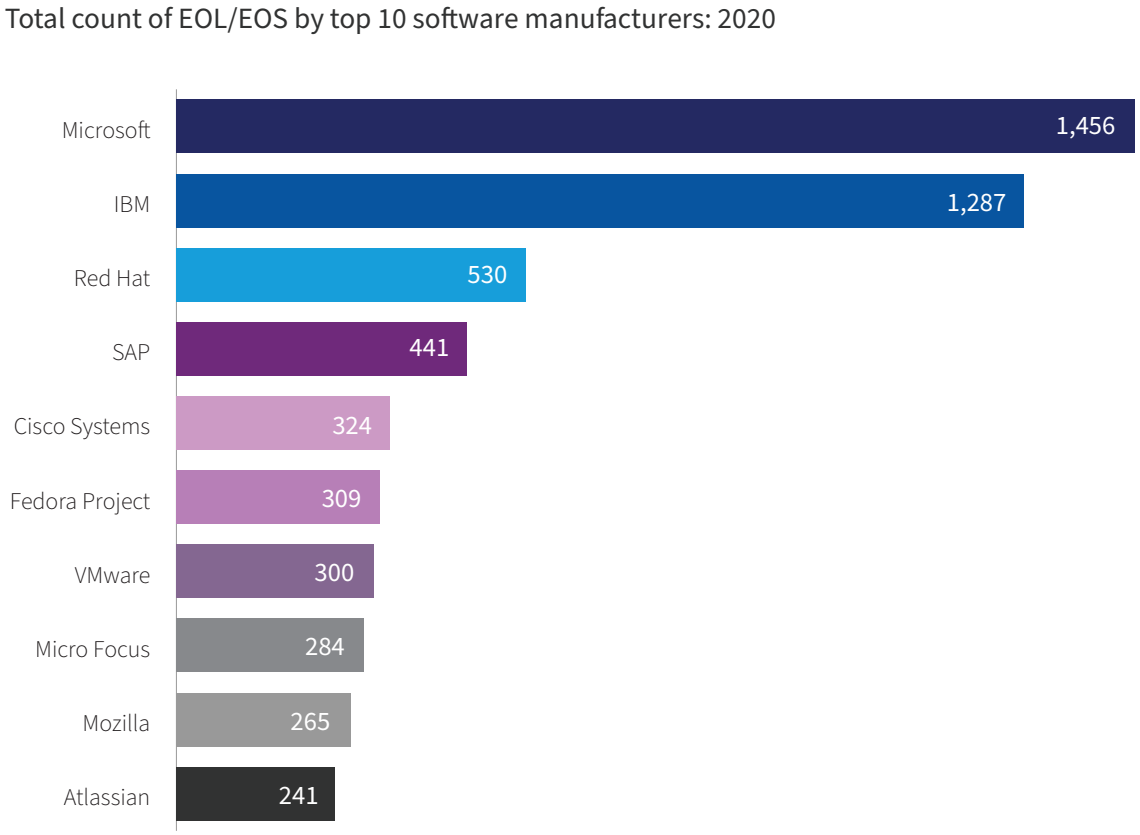
EOL and EOS review

Total count of EOL/EOS by manufacturer

The total count of EOL and EOS dates was tabulated by manufacturer. In 2020, *Microsoft* had the most products facing EOL/EOS, followed by *IBM* and *Red Hat*.

FIGURE 17

Microsoft had the most software EOL/EOS in 2020

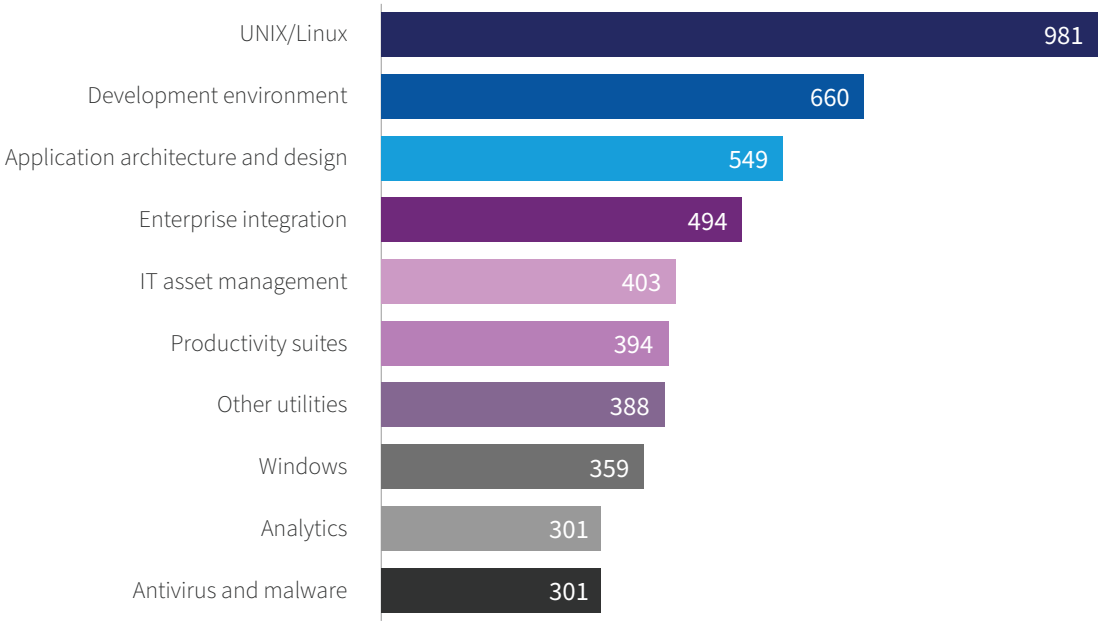


Source: Flexera 2021 State of IT Visibility Report

FIGURE 18

UNIX/Linux was the top subcategory for EOL/EOS in 2020

Total count of top 10 subcategories EOL/EOS: 2020



Source: Flexera 2021 State of IT Visibility Report

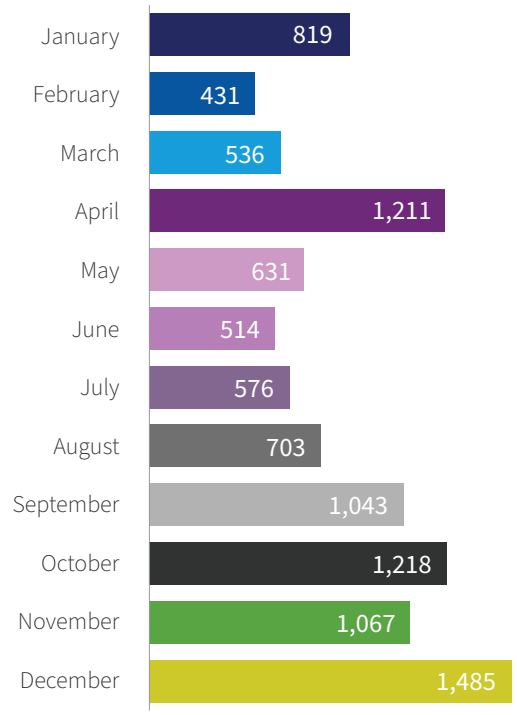
Total count of EOL/EOS by subcategory

The total count of EOL and EOS dates for 2020 was tabulated by subcategory. The subcategory with the largest number of EOL/EOS was *UNIX/Linux* (multitasking, multi-user computer operating systems, including Solaris and others). This was followed by *development environment*, *application architecture and design* and *enterprise integration*.

FIGURE 19

December was the top month for EOL/EOS in 2020

Total count of EOL/EOS by month: 2020



Source: Flexera 2021 State of IT Visibility Report

Flexera

Total count of EOL/EOS by month

For 2020, the total count of EOL/EOS dates was analyzed by month. *December* was the month with the most EOL/EOS dates, followed by *October* and *April*. Analyzing EOL/EOS counts by month can help organizations understand how to prioritize, understand trends and plan resources.

Vulnerability review

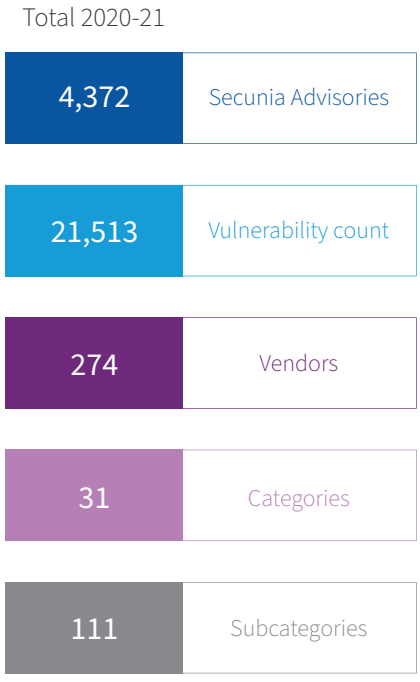
Vulnerabilities detected: EOL and EOS products

Advisories provided by Flexera's Secunia Research team cover all security vulnerabilities associated with a specific version of a product. The total number of Secunia Advisories for 2021 was 4,372. Within those advisories, the absolute number of vulnerabilities detected was 21,513, affecting all software releases for products included in the Technopedia database in 2020-21. These vulnerabilities were discovered across 274 manufacturers, 31 categories and 111 subcategories.

FIGURE 20

More than 21,000 vulnerabilities were detected in 2020-21

Security advisories and vulnerabilities in all EOL/EOS products



Source: Flexera 2021 State of IT Visibility Report

Flexera

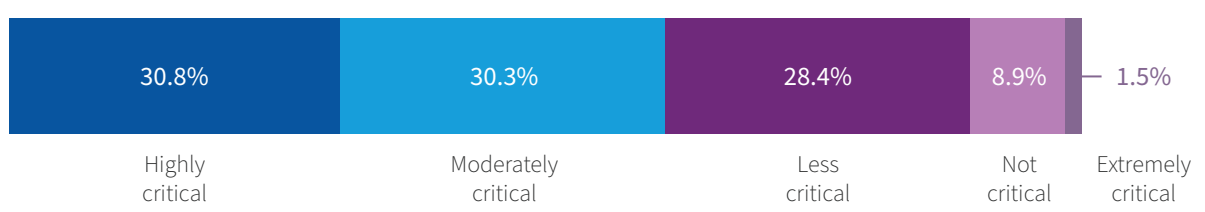
Advisory criticality: all products

The criticality of a vulnerability is expressed as a numeric value based on an assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors and if an exploit exists for the vulnerability. This number indicates the level of damage inflicted from an exploit if the vulnerability were to be exploited. Please refer to the appendix for details on advisory criticality breakdown measurement for this section.

Among vulnerabilities in 2020-21 EOL/EOS releases, 30.8 percent were rated as *highly critical* and 1.5 percent as *extremely critical*. *Moderately critical* (30.3 percent) and *less critical* (28.4 percent) rated advisory criticalities shared an almost-equal percentage of the scoring.

FIGURE 21

The majority of advisory criticality levels were moderate to high



Source: Flexera 2021 State of IT Visibility Report

Time-to-patch

Time-to-patch refers to the duration between disclosure of a vulnerability and the release of a patch, or fix, for said vulnerability. For EOL/EOS software in 2020-21, 90.3 percent of all vulnerabilities had a patch available on the day of disclosure. In the case of all Secunia Advisories (including those without EOL/EOS in 2020-21), 91.1 percent had a patch available on the day of disclosure—a significant increase from the 80.8 percent reported in 2019.

The results indicate that it's possible to remediate the majority of vulnerabilities. It's worth noting, however, that instead of issuing minor updates, some vendors choose to issue major product releases, which can be more complex for users and administrators to manage manually.

The 2020-21 time-to-patch results show that only 4.3 percent of all vulnerabilities were without a fix—whether a partial fix, vendor patch or workaround—for longer than the first day of disclosure.

This percentage is a representative proportion of software products that aren't patched immediately due to a lack of vendor resources, uncoordinated releases or—more rarely—zero-day vulnerabilities.

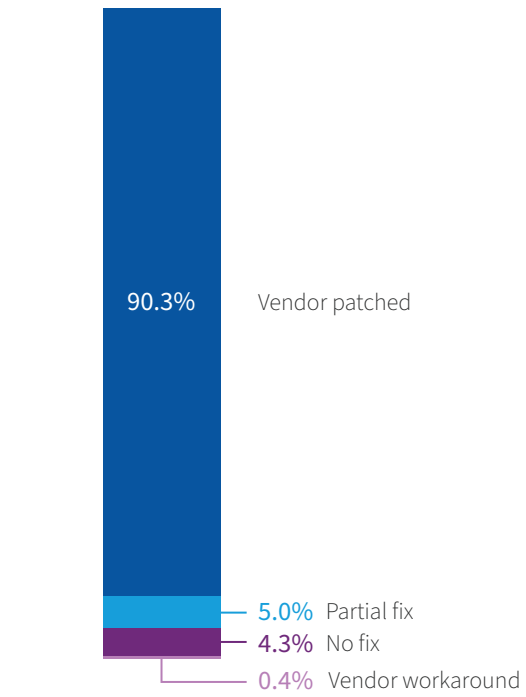
The fact that a percentage of vulnerabilities don't have patches on the first day of disclosure means that a variety of mitigating efforts are required to ensure sufficient protection in support of patch management efforts. This is particularly critical for organizations with a vast array of endpoints to manage, including devices not regularly connected to corporate networks.

Cooperation between vendors and researchers

As shown in figure 22, the fact that more than 90 percent of vulnerabilities in all EOL/EOS product releases in Flexera's database have a patch available on the day of disclosure represents a continued improvement in time-to-patch. In 2012, only 71 percent had a patch available on the day of disclosure, and in 2019 that figure had risen to 83.9 percent. The most likely explanation for the continuously improving time-to-patch rate is that researchers continue to coordinate their vulnerability reports with vendors and vulnerability programs, resulting in immediate patch availability for the majority of cases.

FIGURE 22

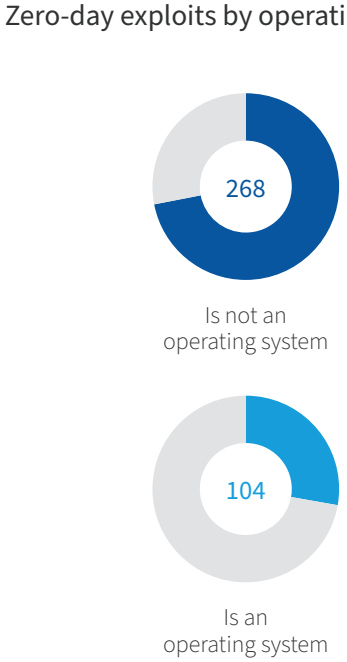
Most vendors offered patch on day of disclosure for EOL/EOS releases



Source: Flexera 2021 State of IT Visibility Report

FIGURE 23

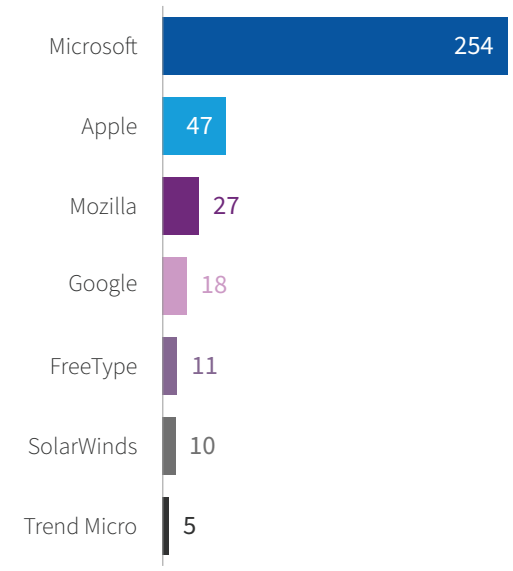
Operating systems comprise more than 25% of all zero-day exploits



Source: Flexera 2021 State of IT Visibility Report

FIGURE 24

Microsoft had the most zero-day exploits



Source: Flexera 2021 State of IT Visibility Report

Zero-day vulnerabilities

A zero-day vulnerability is a vulnerability that's actively exploited by hackers before it's publicly known. The number of zero-day vulnerabilities discovered in 2020 increased from the previous year, with 29 zero-day vulnerabilities compared to 20 in 2019. These zero-day vulnerabilities affected seven manufacturers and 372 software releases.

FIGURE 25
Most attacks originate from outside the organization

Attack vector levels for EOL/EOS software

Source: Flexera 2021 State of IT Visibility Report

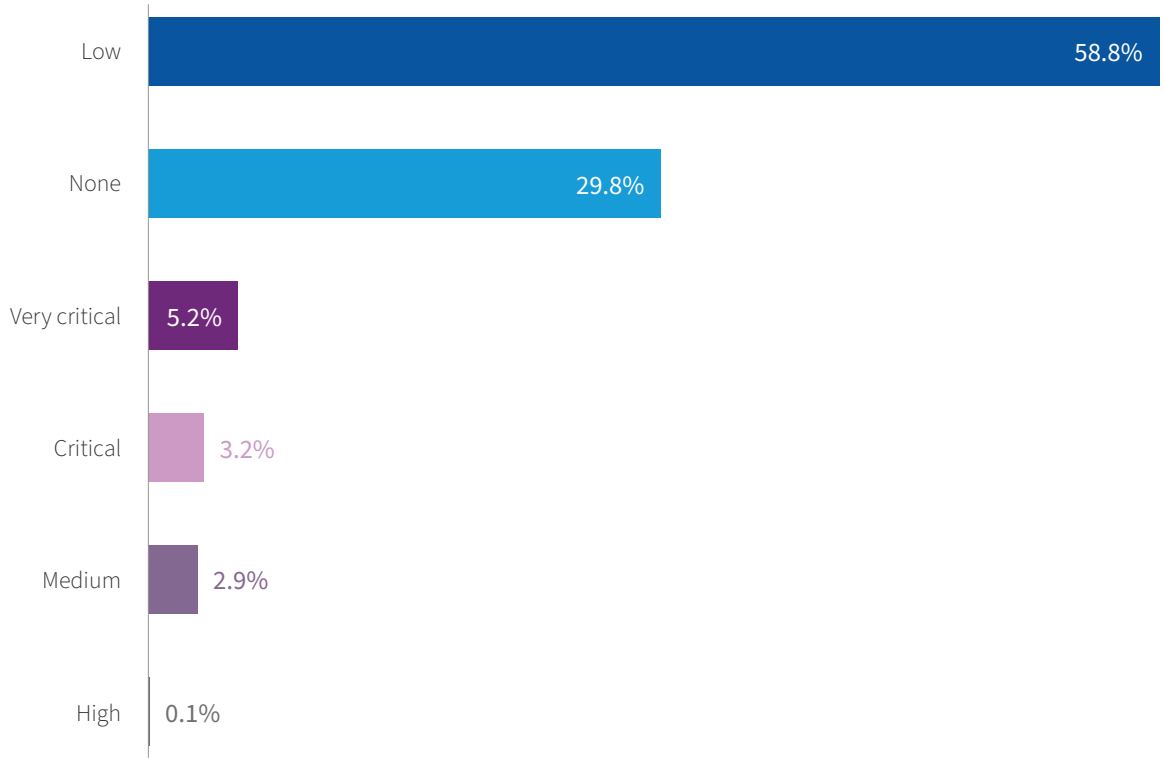
Attack vectors for EOL/EOS software

The avenue through which an attacker can trigger or reach the vulnerability in a product is referred to as an attack vector. Secunia Research classifies attack vectors in three categories: *from local system*, *from local network* or *from remote*.

For 2020-21 EOL/EOS software, almost three-quarters of attack vectors—72.4 percent—were in the remote classification.

FIGURE 26
Most vulnerabilities in EOL/EOS have low threat severity

Vulnerabilities in EOL/EOS software by severity of threat



Source: Flexera 2021 State of IT Visibility Report

Prioritizing with threat intelligence

Threat intelligence improves an IT team's ability to focus on the vulnerabilities that present the greatest threat by exposing those which are actually being exploited in the wild. The proprietary threat intelligence scoring system developed by Secunia Research issues a threat score which helps IT professionals prioritize their patch efforts.

For EOL/EOS software, the majority of vulnerabilities (58.8 percent) scored in the low range, while those scored as critical (3.2 percent) and very critical (5.2 percent) comprised only a small portion.

It's important to note that vulnerability scoring does not measure the criticality of the vulnerability; rather, it is focused on the likelihood of the vulnerability being exploited.

2021 Visibility

2021 Visibility

End of life, end of support and vulnerabilities

Integrating IT asset inventory data is crucial to mitigating risk in an organization and prioritizing strategic initiatives such as vulnerability remediation and application rationalization.

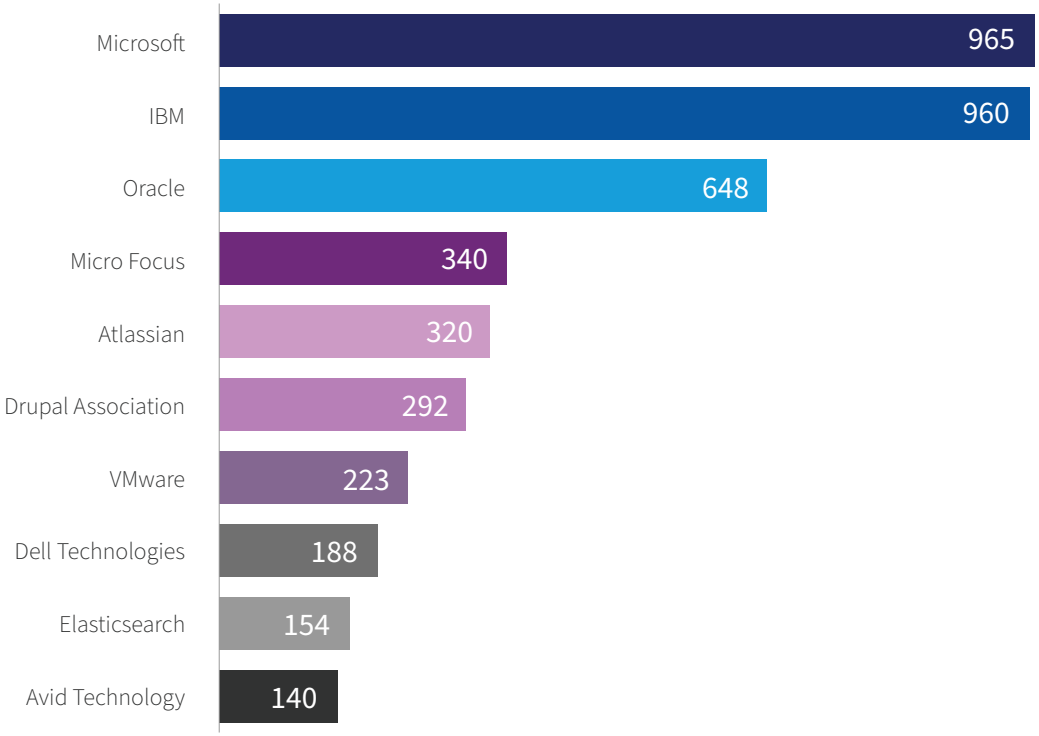
The data on outdated and vulnerable software provided by this report can assist IT professionals in planning for updates, remediation efforts and the retiring of old software. But what will guide these decisions most is data specific to the technology in each organization's IT ecosystem, along with their specific concerns and planning processes.

With that in mind, this section analyzes both the top-level overview of EOL/EOS and a contextualized view of those counts through the environments of our survey respondents.

FIGURE 27

Microsoft, IBM have most software at EOL/EOS in 2021

Total count of EOL/EOS for top 10 software manufacturers: 2021



Source: Flexera 2021 State of IT Visibility Report

Total count of EOL/EOS by manufacturer in 2021

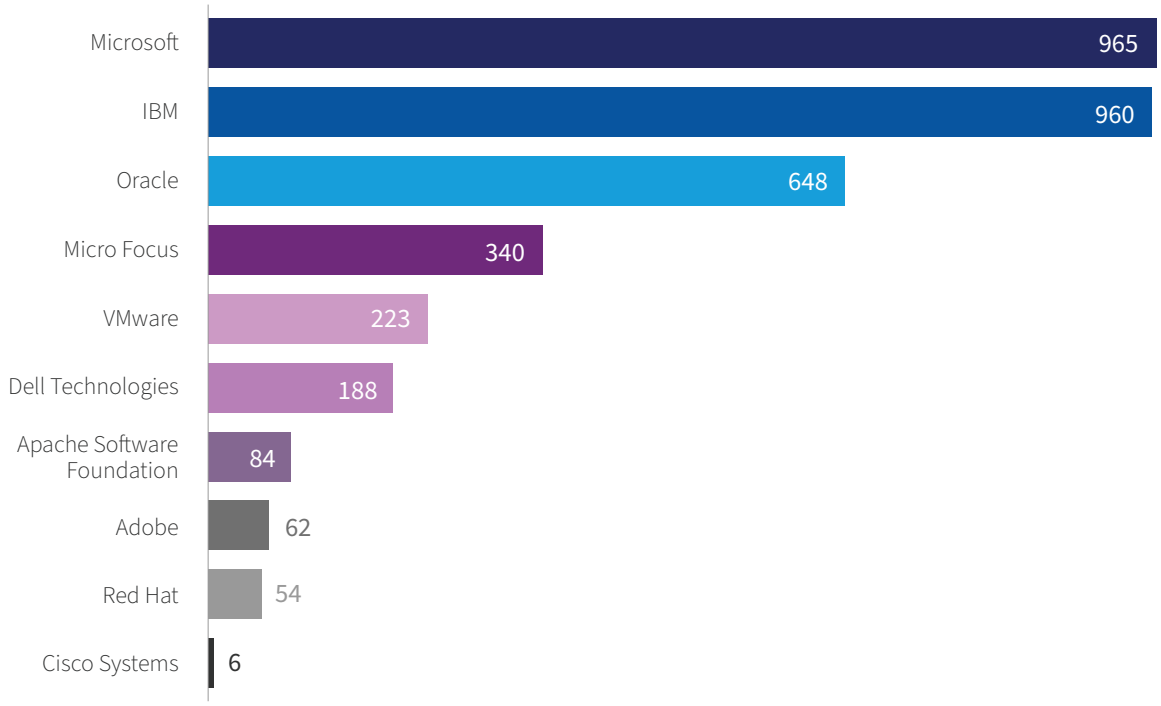
The total count of EOL and EOS dates was tabulated by manufacturer. Figure 27 shows that in 2021, *Microsoft* had the most products facing EOL/EOS, followed very closely by *IBM*.

These top manufacturers also correspond with manufacturers in survey respondents' IT estates. The total count of EOL and EOS dates was tabulated by the top manufacturers in survey respondents' IT estates, as self-reported. In 2021, *Microsoft* will lead the pack for the most products facing EOL/EOS in respondent environments, followed closely by *IBM*.

FIGURE 28

Microsoft, IBM lead EOL/EOS count for respondents' top manufacturers

Total count of EOL/EOS for respondents' top 10 software manufacturers: 2021



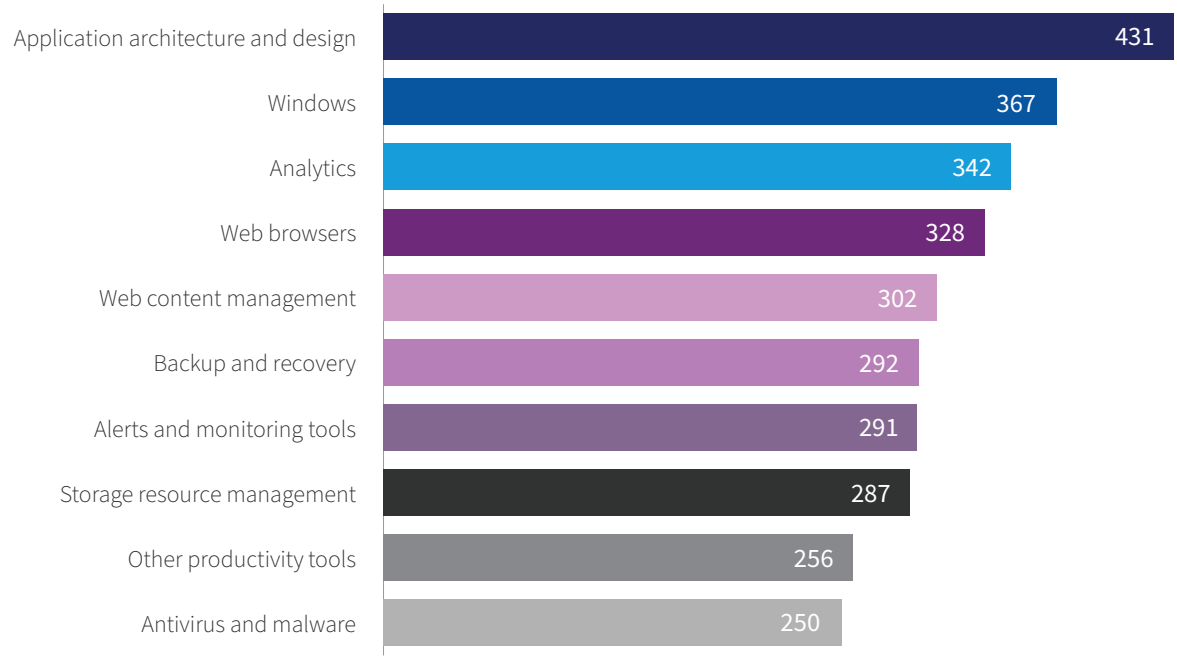
N=325

Source: Flexera 2021 State of IT Visibility Report

FIGURE 29

Application architecture and design is top EOL/EOS subcategory in 2021

Total count of top 10 subcategories for EOL/EOS: 2021



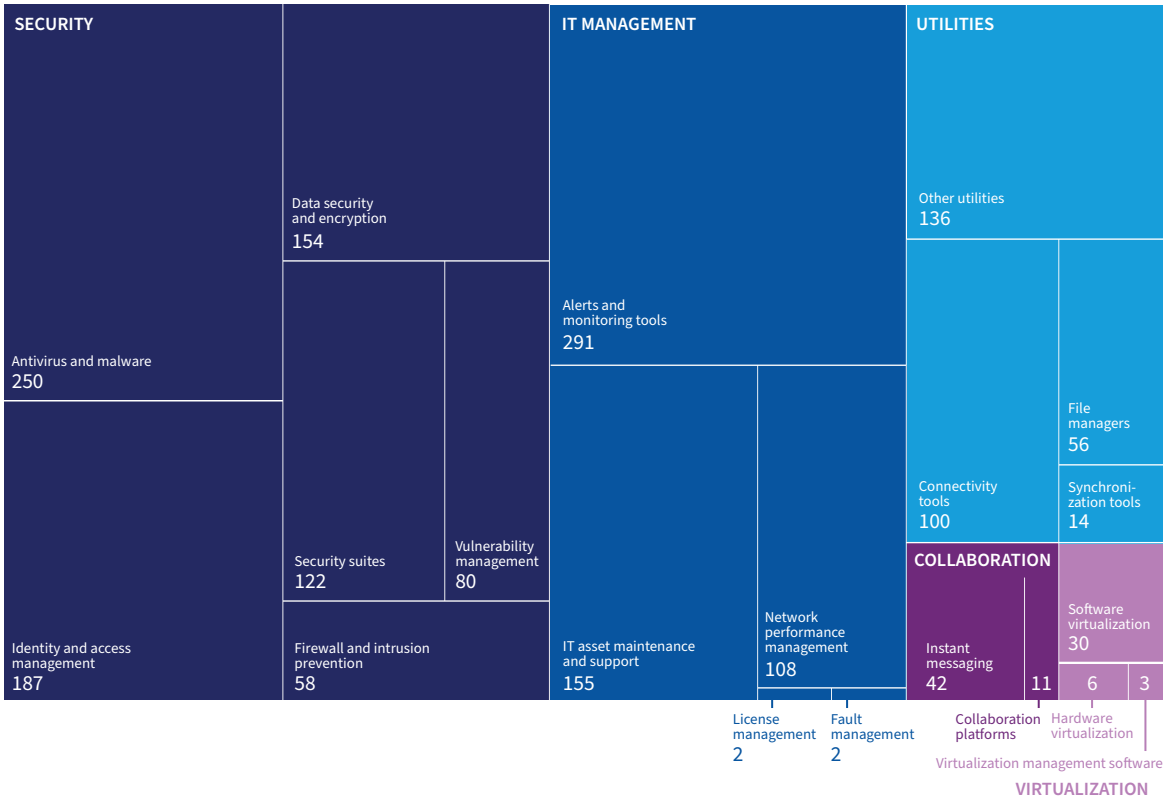
Source: Flexera 2021 State of IT Visibility Report

Total count of EOL/EOS by subcategories in 2021

This report also tabulated the total count of EOL and EOS dates for 2021 by subcategory. The subcategory with the largest number of EOL/EOS is *application architecture and design*, followed by *Windows* and *analytics*.

FIGURE 30

Security is respondents' top category for EOL/EOS in 2021



N=325

Source: Flexera 2021 State of IT Visibility Report

Respondents' top EOL/EOS categories in 2021

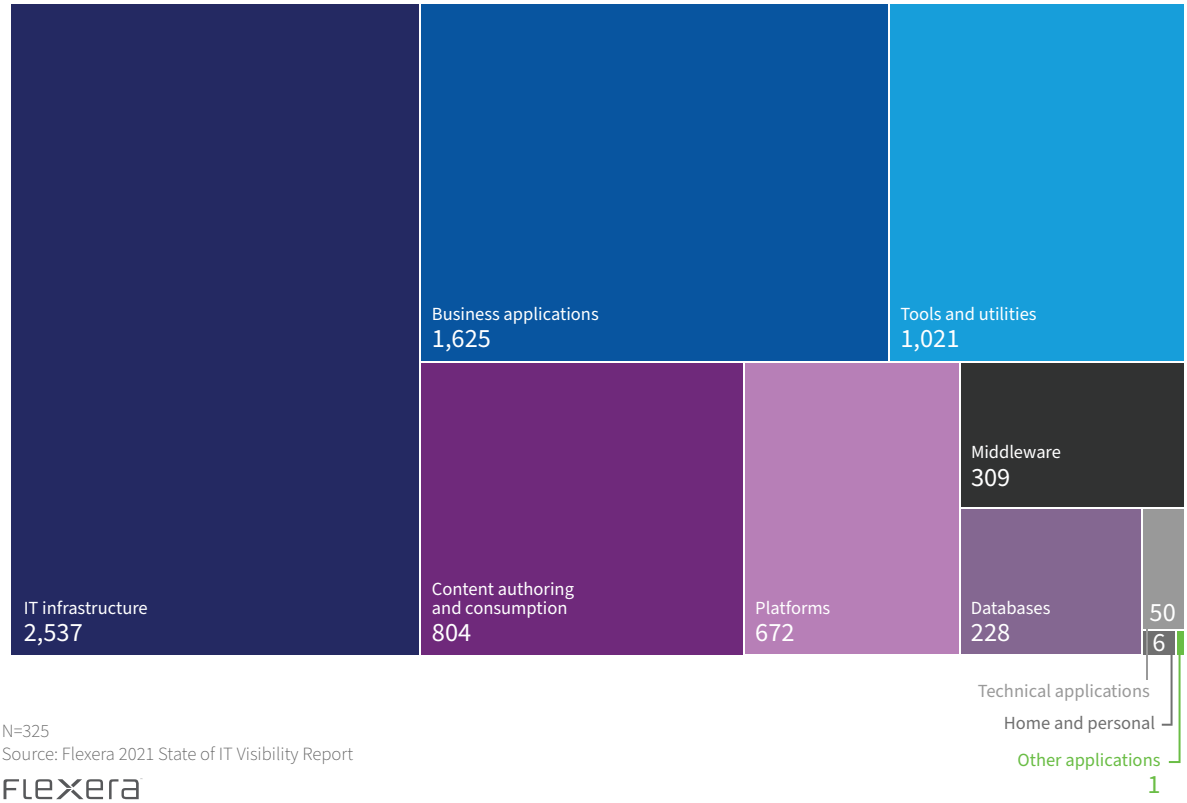
The top categories with EOL and EOS dates were tabulated by categories and subcategories included in our survey respondents' IT estates, as self-reported.

In 2021, *security*—including the subcategories of antivirus and malware, identity and access management, data security and encryption, security suites, vulnerability management, and firewall and intrusion prevention—was the EOL/EOS category most concerning our survey respondents. This was followed by *IT management*, which includes alerts and monitoring tools, IT asset maintenance and support, network performance management, license management and fault management.

FIGURE 31

IT infrastructure is respondents' top 2021 software category group

Top 10 software category groups for EOL/EOS by survey respondents: 2021



N=325
Source: Flexera 2021 State of IT Visibility Report

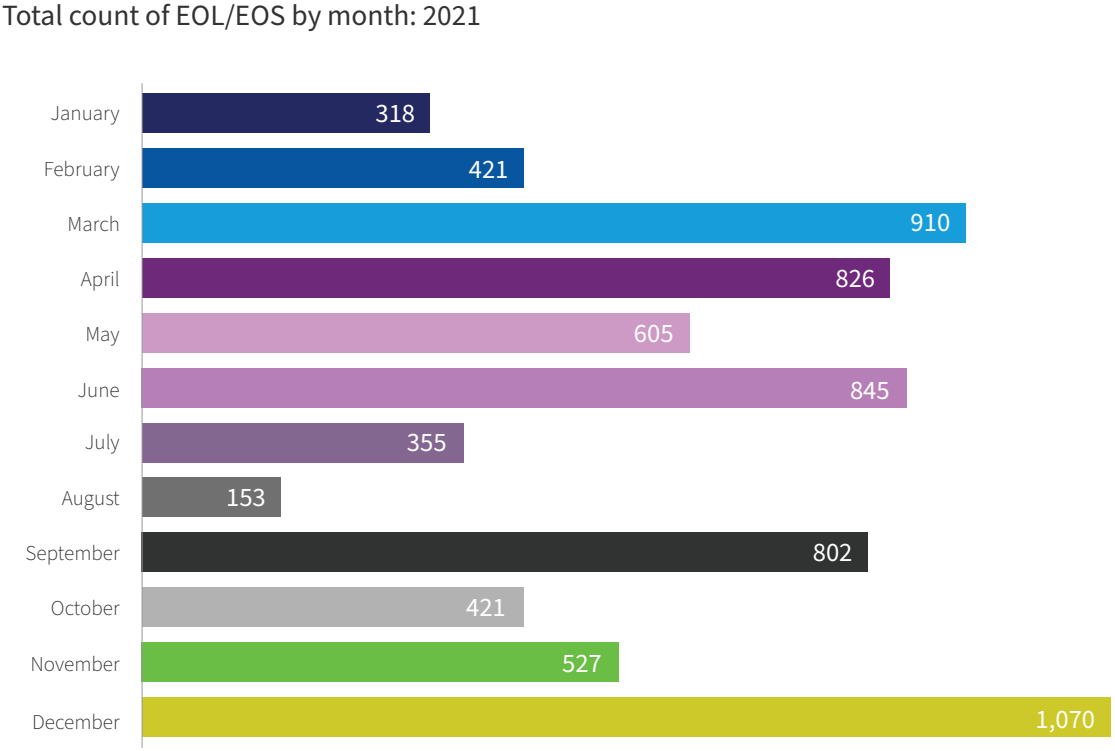
Respondents' top 10 EOL/EOS software category groups

The top category groups with EOL and EOS dates were tabulated by categories and subcategories included in our survey respondents' IT estates that make up overarching category groups, as self-reported.

In 2021, *IT infrastructure*—which includes configuration management, IT management, security and storage—has the most software coming to EOL and EOS. This is followed by *business applications* (including business intelligence, supply chain management and finance) and *tools and utilities* (including software development, distributed network architecture and utilities).

FIGURE 32

December is top month for EOL/EOS in 2021



Source: Flexera 2021 State of IT Visibility Report

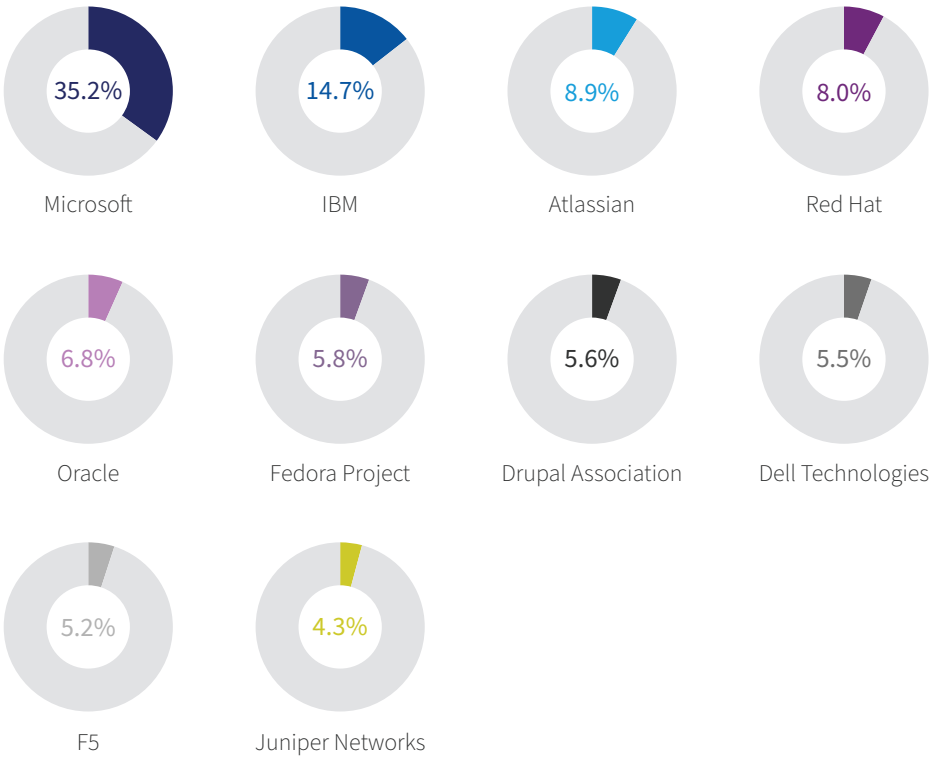
Total count of EOL/EOS by month in 2021

This report also analyzed the total count of EOL/EOS dates by month. Reviewing the EOL/EOS counts by month can help organizations understand how to prioritize, understand trends and plan resources. *December* was once again the month with the most EOL/EOS dates, followed by *March* and *June*.

FIGURE 33

Microsoft is the most vulnerable manufacturer by EOL/EOS

Ten most vulnerable software manufacturers by EOL/EOS



Source: Flexera 2021 State of IT Visibility Report

Where should you focus your attention?

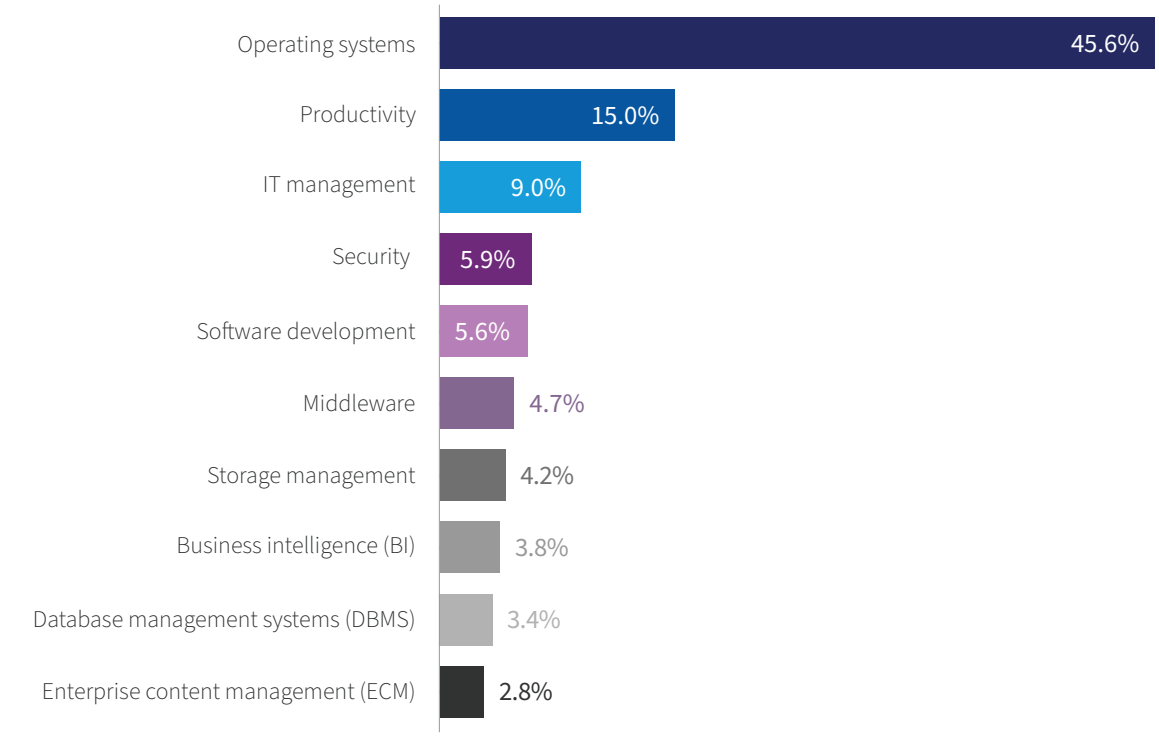
Understanding where you have the most EOL/EOS software is important for prioritizing updates. If you know a primary vendor has many of its products reaching EOL/EOS in a certain month or that a certain category of software has significant EOL/EOS at inflection points throughout the year, it's easier to prioritize those updates.

However, it's increasingly important—as noted by our survey respondents in figure 11A—to have visibility into vulnerabilities as well. With that in mind, consider how your organization can prioritize its EOL/EOS software as it relates to the vulnerability posture of that software.

Ten most vulnerable manufacturers by EOL/EOS

For products with the most releases reaching EOL/EOS in 2020 and 2021, the three manufacturers with the most vulnerabilities were *Microsoft* (35.2 percent), *IBM* (14.7 percent) and *Atlassian* (8.9 percent).

FIGURE 34
The most vulnerable category by EOL/EOS is *operating systems*



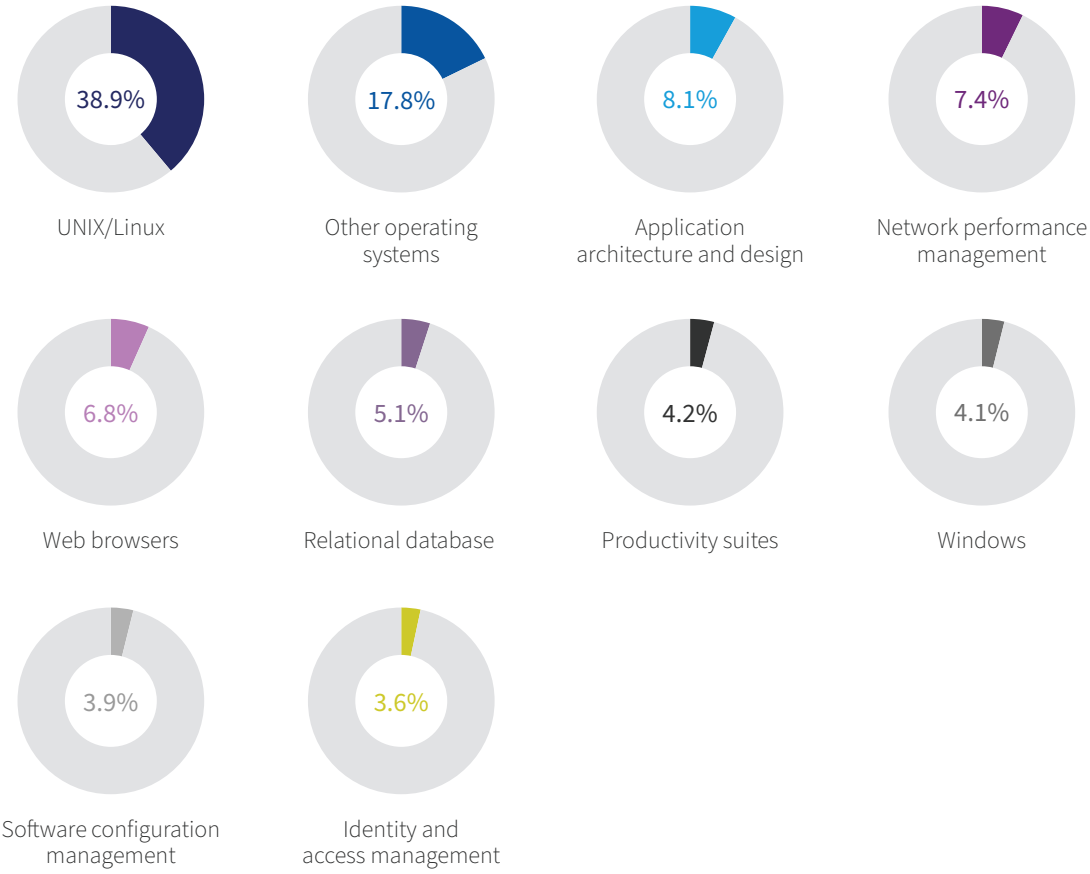
Source: Flexera 2021 State of IT Visibility Report

Ten most vulnerable categories by EOL/EOS

For products with releases reaching EOL/EOS in 2020 and 2021, the three most vulnerable categories were *operating systems* (45.6 percent), *productivity* (15 percent) and *IT management* (nine percent).

FIGURE 35

UNIX/Linux is the most vulnerable subcategory by EOL/EOS



Source: Flexera 2021 State of IT Visibility Report

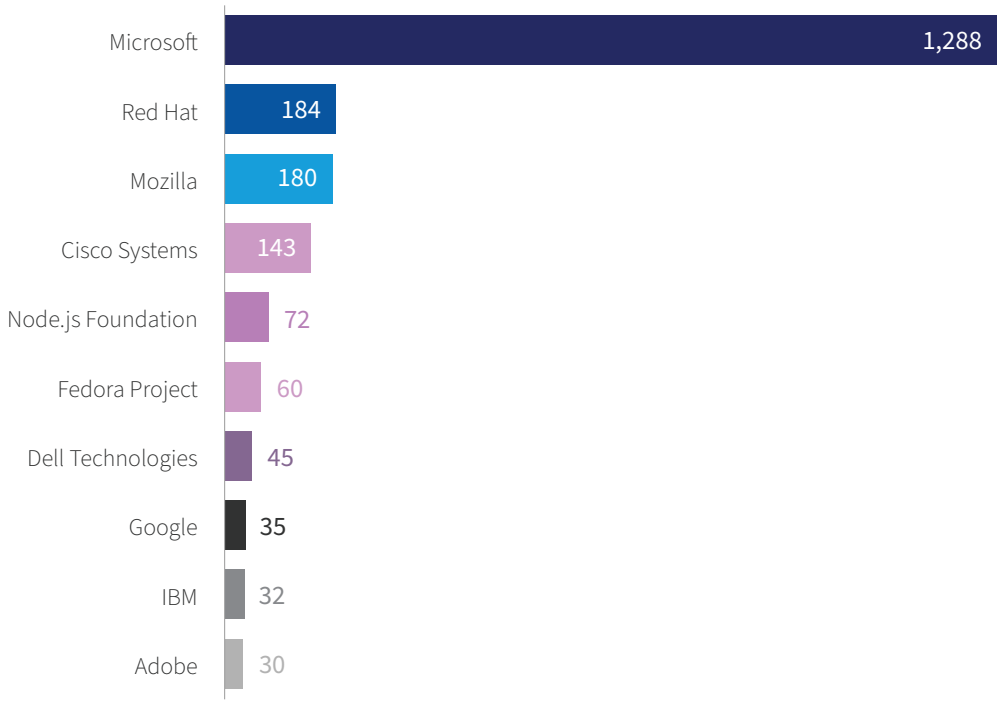
Ten most vulnerable subcategories by EOL/EOS

For products with releases reaching EOL/EOS in 2020 and 2021, the most vulnerable subcategories were *UNIX/Linux* (38.9 percent), *other operating systems* (17.8 percent) and *application architecture and design* (8.1 percent).

FIGURE 36

Microsoft is the most highly critical manufacturer by EOL/EOS

Ten most highly critical software manufacturers by EOL/EOS



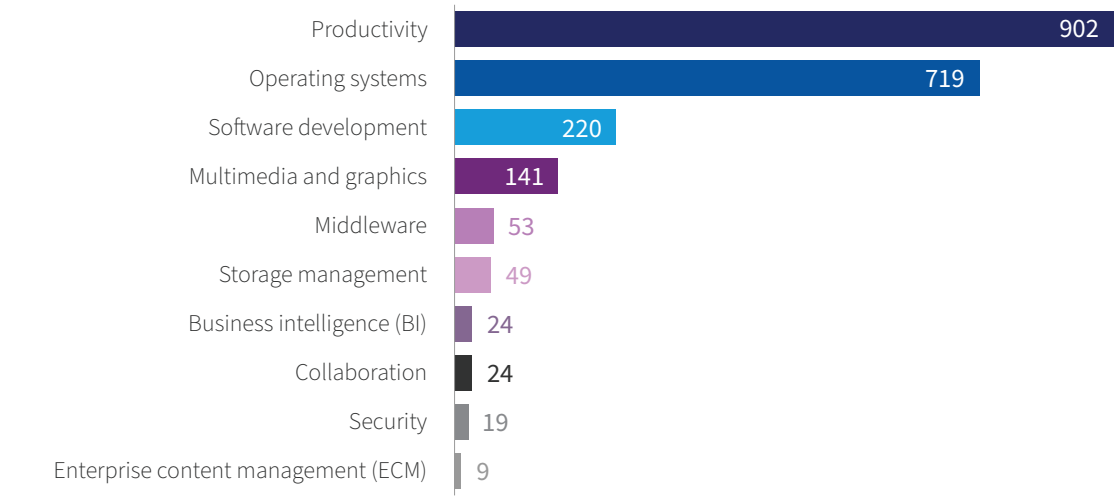
Source: Flexera 2021 State of IT Visibility Report

Ten most highly critical manufacturers by EOL/EOS

When viewing vulnerabilities against EOL/EOS manufacturers, *Microsoft* (with 1,288), *Red Hat* (184) and *Mozilla* (180) display the largest volume of highly critical vulnerabilities.

FIGURE 37

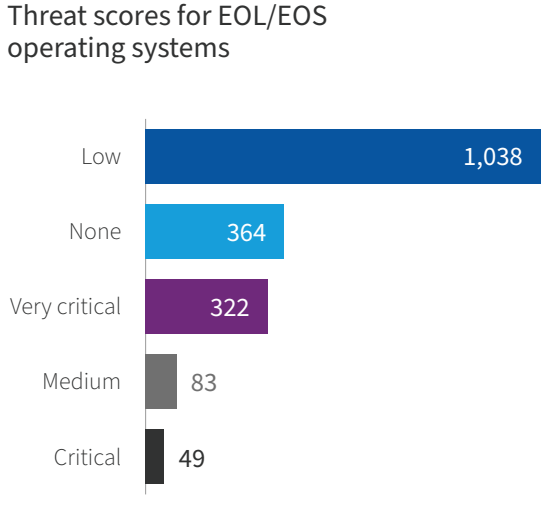
Productivity, *operating systems* are the most highly critical categories by EOL/EOS



Source: Flexera 2021 State of IT Visibility Report

FIGURE 38

The majority of threat scores for EOL/EOS operating systems are low level



Source: Flexera 2021 State of IT Visibility Report

Ten most highly critical categories by EOL/EOS

When viewing vulnerabilities against EOL/EOS categories, *productivity* (with 902) and *operating systems* (with 719) have significantly more highly critical vulnerabilities than any other critical category.

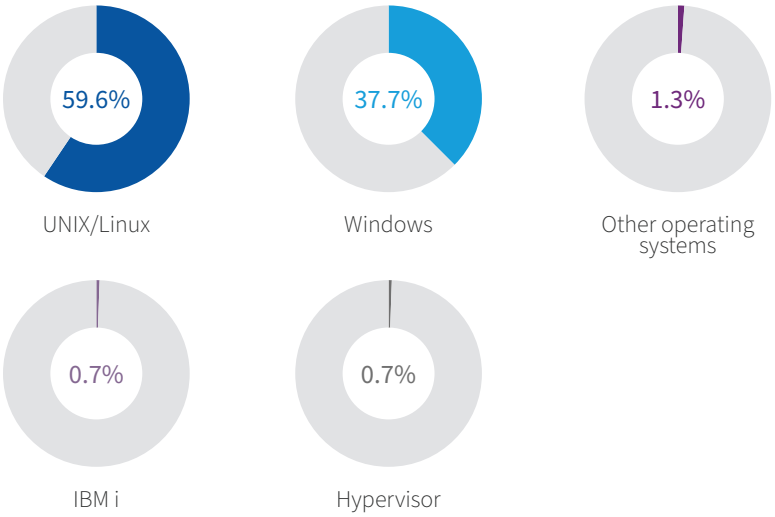
Threat scores for EOL/EOS operating systems

As shown in previous sections, EOL/EOS operating systems is the most vulnerable category and second-most critical category of software release. Secunia Research's threat intelligence scoring illustrates where those vulnerabilities lie.

The majority of vulnerabilities for operating systems (1,038) scored as low-level; only 322 were scored very critical. Security operations and IT asset teams will want to pay particularly close attention to this space when reviewing EOL/EOS software. While many will focus on the higher range (critical to very critical) threat scores, the low threat score level provides ample opportunity for hackers to breach the organization through operating systems.

FIGURE 39

UNIX/Linux most vulnerable EOL/EOS operating systems at low-level threat score



Source: Flexera 2021 State of IT Visibility Report

Most vulnerable EOL/EOS operating systems at low-level threat score

An operating system with a low-level threat score is the attack method through which a hacker will most likely gain access. It's therefore important to also understand what percentage of that risk is attributed to each operating system.

In many cases, because the vulnerabilities are so prevalent at a specific threat level (in this case, the low level), there's a greater likelihood that a breach can occur in an operating system through these vulnerabilities. *UNIX/Linux* has the majority of low-level threat scores at 59.6 percent, as shown in figure 39. This correlates to the overwhelming amount of EOL and EOS for UNIX/Linux in 2020-21. *Microsoft Windows* has the second most low-level threat scores, with 37.7 percent.

Summary

IT asset lifecycle management best practices

As we look at how organizations understand their IT infrastructure, and their risk and compliance positions, it's vital to understand how businesses interact internally toward common objectives and outcomes. The ***Flexera 2021 State of IT Visibility Report*** reveals that organizations need comprehensive, clear insights into technology for data-driven decision making and to maintain control and security. From on-premises software and hardware to SaaS and cloud, leveraging these insights can help IT professionals rise to the challenge of keeping IT assets secure, well-governed and cost effective.

While this report reviews top-level trends and dives deeper into specific areas of focus for prioritization, each IT environment is unique to the organization it serves. Whether operating systems, productivity, software development or more—IT leaders can apply these critical measures to their organization's specific needs.

Consider these best practices for your organization:

Understand your assets

When upgrading or replacing aging hardware or software assets, it's critical to have detailed information about exactly which versions, releases and hardware models you have deployed, along with information about possible upgrade paths, latest versions, discontinued lines and so on. Establishing this foundation helps you easily identify opportunities for consolidation or areas that require attention.

Know the EOL/EOS dates of products in your IT ecosystem

Most software vendors don't have a standard EOL/EOS policy; they instead offer a complicated support policy that requires deciphering. In many cases, EOL/EOS dates and policies are buried in the sales and marketing documents on their website—or aren't published at all. Flexera's comprehensive Technopedia IT asset data repository can augment your asset catalog with the EOL and EOS dates of all the products in your environment.

Collaborate cross-enterprise for your EOL and EOS strategy

EOL/EOS data may be owned by siloed groups within an organization. But EOL and EOS impact far more than any one group. From production and support to compliance and security, the entire business is affected by lifecycle management.

Make it a group effort to develop EOL and EOS planning. Collaborate with counterparts in IT management, IT support and security, procurement, finance and other departments within the organization to break down walls and share the data needed for a successful strategy.

Create a central repository or CMDB with consolidated and normalized inventory data that provides a rich source of information that stakeholders and other systems across the organization can access and exploit. To get the right information to the right people and systems, you'll need tools that:

- Analyze the data and organize it in a variety of ways to meet the information needs of different audiences
- Generate reports and dashboards tailored to your needs and the needs of your stakeholders
- Export the data to other systems to augment the data maintained by those systems
- Feed the data into other enterprise systems to power process automation

The clearer your visibility into your technology landscape, the greater the impact you can have on driving the success of your business.

Appendix:

Secunia Research software vulnerability tracking process

A vulnerability is an error in software that can be exploited, leading to a security impact and gain. Secunia Research validates, verifies and tests vulnerability information gathered and includes it in the Secunia Vulnerability Intelligence database with consistent and standard processes that have been constantly refined over the years.

Whenever a new vulnerability is reported, a Secunia Advisory is released after verification of the information. A Secunia Advisory provides details for the vulnerability, including description, risk rating, impact, attack vector, recommended mitigation, credits, references and more. Also included are any additional details discovered during verification and testing. This provides the information required for organizations to make appropriate decisions about how to protect systems.

After the first publication, the status of the vulnerability is tracked throughout its lifecycle. Updates are made to the corresponding Secunia Advisory as new relevant information becomes available.

Metrics used to count vulnerabilities

Secunia Advisory

The number of Secunia Advisories published in a given period of time is a first-order approximation of the number of security events in that period. Security events stand for the number of administrative actions required to keep the specific product secure throughout a given period.

Secunia vulnerability count

A vulnerability count is added to each Secunia Advisory to indicate the number of vulnerabilities covered by the Secunia Advisory. Using this count for statistical purposes is more accurate than counting common vulnerabilities and exposures (CVE) identifiers. Using vulnerability counts is, however, also not ideal as these are assigned per advisory. This means that one advisory may cover multiple products, but multiple advisories may also cover the same vulnerabilities in the same code base shared across different applications and even different vendors.

Common vulnerabilities and exposures (CVE)

Common vulnerabilities and exposures is a dictionary of publicly known information security vulnerabilities and exposures. CVE has become a de facto industry standard used to uniquely identify vulnerabilities that have achieved wide acceptance in the security industry. Using CVEs as vulnerability identifiers allows correlation of information about vulnerabilities between different security products and services. CVE information is assigned in Secunia Advisories.

The intention of CVE identifiers is not to provide reliable vulnerability counts. Instead, it is a very useful, unique identifier for pinpointing one or more vulnerabilities and correlating them between different sources. The problem with using CVE identifiers for counting vulnerabilities is that CVE abstraction rules may merge vulnerabilities of the same type in the same product versions into a single CVE, resulting in one CVE sometimes covering multiple vulnerabilities. This may result in lower-than-expected vulnerability counts.

Attack vectors

The way in which an attacker can trigger or reach the vulnerability in a product is referred to as an attack vector. Secunia Research classifies attack vectors in three categories: from local system, from local network or from remote.

From local system

From local system describes vulnerabilities for which the attacker is required to be a local user on the system to trigger the vulnerability.

From local network

From local network describes vulnerabilities for which the attack vector requires an attacker to be situated on the same network as a vulnerable system (not necessarily a LAN).

This category covers vulnerabilities in certain services such as DHCP, RPC and administrative services, which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems.

From remote

From remote describes other vulnerabilities for which the attacker isn't required to have access to the system or a local network in order to exploit the vulnerability. This category covers services that are acceptable to be exposed and reachable to the Internet (e.g., HTTP, HTTPS, SMTP). It also covers client applications used on the Internet and certain vulnerabilities where it's reasonable to assume that a security-conscious user could be tricked into performing certain actions.

Unique and shared vulnerabilities

Unique vulnerabilities

Vulnerabilities found in the software of this—and only this—vendor. These are vulnerabilities in the code developed by this vendor that aren't shared in the products of other vendors.

Shared vulnerabilities

Vulnerabilities found in the software of this and other vendors due to the sharing of either code, software libraries or product binaries. If vendor A develops code or products that are also used by vendor B, the vulnerabilities found in these components are categorized as shared vulnerabilities for both vendor A and vendor B.

Total vulnerabilities

The total number of vulnerabilities found in the products of the vendor, which can be unique or shared vulnerabilities. These are the vulnerabilities that affect the users of the vendor's products.

Secunia vulnerability criticality classification

The criticality of a vulnerability is based on the assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors, and if an exploit exists for the vulnerability and is being actively exploited prior to the release of a patch.

Extremely critical (5 of 5)

Typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation doesn't normally require any interaction and exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP and SMTP or in certain client systems, such as email applications or browsers.

Highly critical (4 of 5)

Typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation doesn't normally require any interaction but there are no known exploits available at the time of disclosure. Such vulnerabilities can exist in services like FTP, HTTP and SMTP or in client systems like email applications or browsers.

Moderately critical (3 of 5)

This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that aren't intended for use over the Internet. Typically used for remotely exploitable denial of service vulnerabilities against services like FTP, HTTP and SMTP, and for vulnerabilities that allow system compromises but require user interaction.

Less critical (2 of 5)

Typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.

Not critical (1 of 5)

Typically used for very limited privilege escalation vulnerabilities and locally exploitable denial of service vulnerabilities. This rating is also used for non-sensitive system information disclosure vulnerabilities (e.g., remote disclosure of installation path of applications).

About Flexera

Flexera delivers IT management solutions that enable enterprises to accelerate the return on their technology investments. We help organizations ***inform their IT*** with total visibility into complex hybrid ecosystems, so they can ***transform their IT*** by rightsizing across all platforms, reallocating spend, reducing risk and charting the most effective path to the cloud. Our technology value optimization solutions are delivered by 1,300+ team members helping more than 50,000 customers achieve their business outcomes. To learn more, visit **flexera.com**

Contact us for more information or a demo:

+1 800.809.5659 | +44 870.871.1111

sales@flexera.com

flexera.com