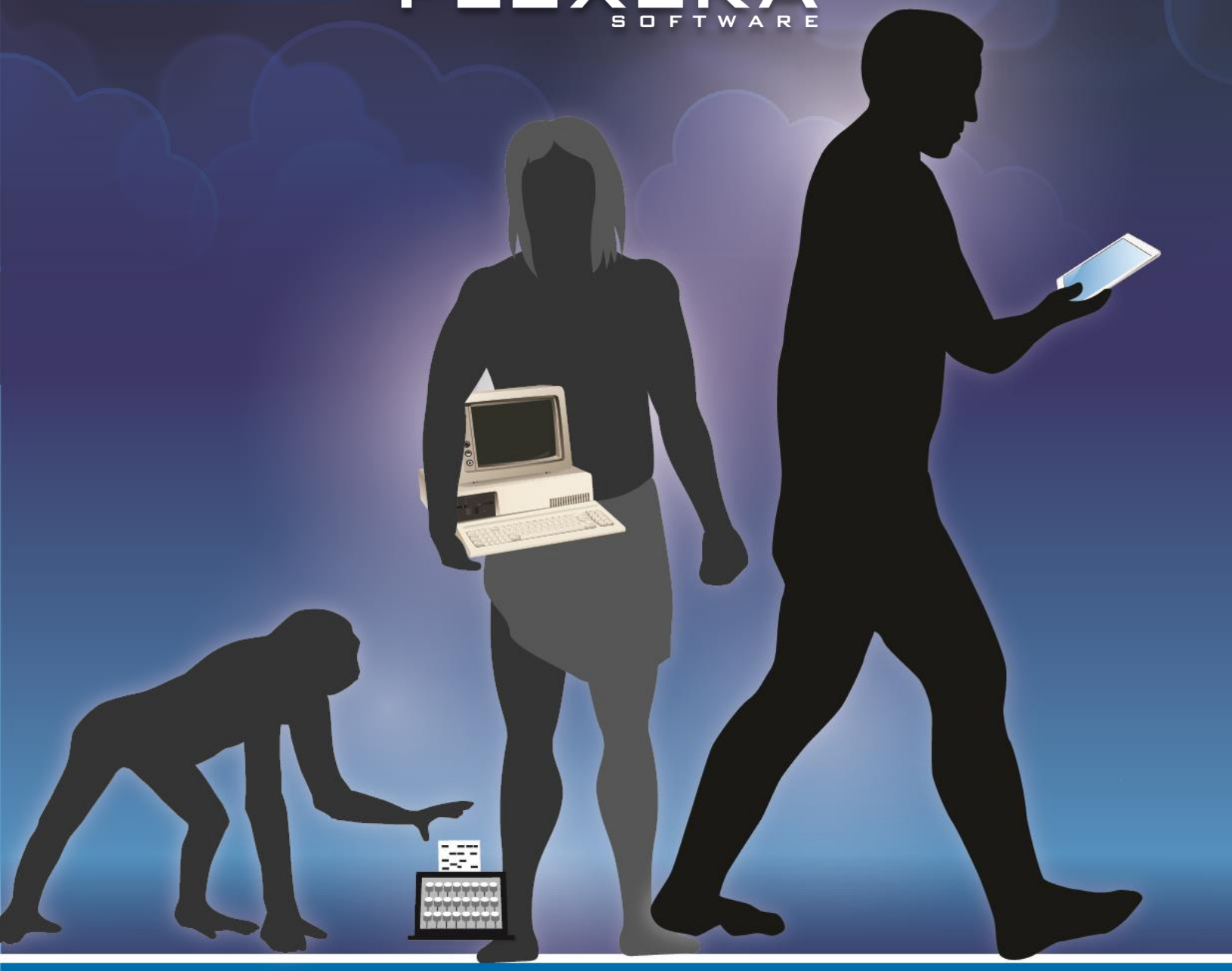
Software Asset Management.Next

How Security Risks & the Shift to the Cloud Are Transforming SAM

Key Trends in Software Pricing & Licensing Survey – 2016 Report

FLEXERA® SOFTWARE



Software Asset Management's Journey to Strategic Importance

In the not too distant past, only outlier organizations viewed software as a unique corporate asset requiring specialized people, processes and technology to manage. Most organizations barely understood the true complexities and risks around procuring software, remaining in compliance with licensing agreements, and understanding their "shelfware" situation (i.e. what software they own but are not using) – let alone doing something about it.

Then the climate changed – creating an element of tension and dysfunction between the world's software buyers and sellers. Software companies, seeing an opportunity to bolster revenues in increasingly challenging economic times, started to more aggressively exercise their contractual rights to conduct software license compliance audits. Teams of auditors started descending on enterprises globally, forcing their customers to engage in lengthy, time and resource consuming license reviews. These audits were resulting in enormous "true-ups" – findings that enterprises were out of compliance with their contracts and owed their vendors additional fees.

Fast forward to 2016 and the extent of audit pain in today's enterprises is clear. A Flexera Software Report released earlier this year revealed that 65 percent of enterprises faced a vendor software license compliance audit within the past year, and 23 percent were audited three times or more. It also found that 44 percent of enterprises paid $100,000 or more in true-up costs to their software vendors in the past year, and 20 percent paid $1,000,000 or more.

The pain organizations have endured in defending against intrusive software license audits has driven the urgency for more mature Software Asset Management (SAM) programs. SAM has introduced people, processes and automation around software discovery, inventory, compliance and license optimization. Gartner estimates that companies implementing SAM can achieve up to 30% software spending reductions within one year[1].

But SAM itself has had to continuously evolve since it was first introduced. Why? Because the software landscape today looks nothing like it did in the early 2000s. The cloud, virtualization, Software as a Service (SaaS) and mobility are redefining how software is delivered, how it's paid for and how users access that software. The rise of the cloud, Internet-connected devices – (The Internet of Things), software vulnerabilities and cyber-crime are redefining what software asset management must entail. And software vulnerability concerns are driving SAM to the forefront as security teams – like SAM teams – must understand what software they have before they can understand whether they are exposed to dangerous vulnerabilities.

[1] Gartner: Toolkit: Evaluate Software Asset Management Savings With SAM Tool Justification Calculator, Hank Marquis, Gary Spivak, May 12, 2016.

This report explores the changes in the software landscape and its implications for the next generation of SAM solutions – SAM.Next.

SAM Must Evolve as Virtualization & SaaS Go Mainstream

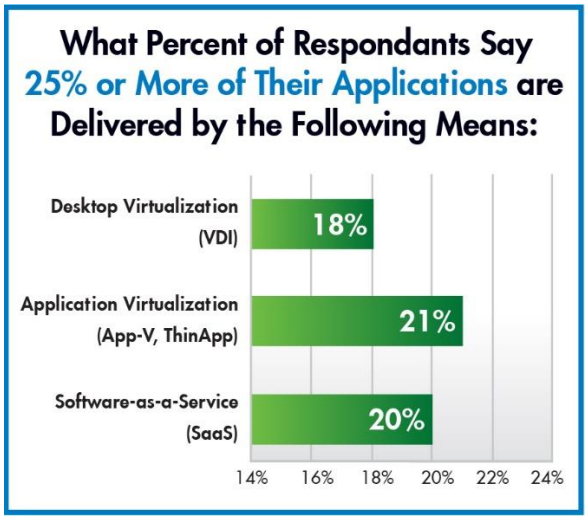
In the early days of SAM, the types of software and the environments in which software ran were far less complex. And by extension, so was the SAM technology required to manage, optimize and secure software assets. For instance, Microsoft® had a virtual monopoly on enterprise desktop operating systems (OS) in the 80's, 90's and early 2000's. Though its dominance is still undisputed – it is no longer the fortress OS. Today slightly less than three quarters of respondents – 73 percent – say that 80 percent or more of their desktop apps run on Microsoft Windows – and that number will decline to 64 percent within the next two years.

Moreover, in recent years IT Operations professionals have sought to move away from the cost and inflexibility forced upon them by having to manage on premises installed software running on local hardware.

For instance, Salesforce.com captured the imagination of organizations seeking to benefit from enterprise-grade software without having to manage it themselves. As that company demonstrated the healthy demand for SaaS software, software vendors have taken note, and increasingly now offer SaaS versions of their on-premises software. Most software start-ups increasingly are bypassing on-premises altogether, offering only SaaS versions of their products.

Likewise, the ability to virtualize applications or entire desktop environments (virtualization desktop infrastructure (VDI)) to make them independent of the hardware on which they run, has created enormous flexibility for enterprises that want users to be able to access their data, environments and applications, wherever they may be on whatever devices they may be using.

The trends towards SaaS and virtualization are clear based on the enterprises we surveyed. 20 percent of respondents say more than a quarter of their software is now SaaS-based. And 39 percent say more than a quarter is virtualized (either via VDI or Application Virtualization).



WHY DOES THIS MATTER?

What's the takeaway given these trends? Organizations must understand that SaaS and virtualization—including application, desktop and server virtualization, may introduce hidden cost and risk from a SAM and license optimization perspective.

Consider virtualization. While there may be cost and/or efficiency benefits from using virtualization technologies – organizations must also consider potential cost risks from a licensing perspective. For instance, each vendor has particular virtualization rules within their license agreements. Non-compliance with those agreements could (and often does) result in true-up liabilities far exceeding the cost savings from virtualization.

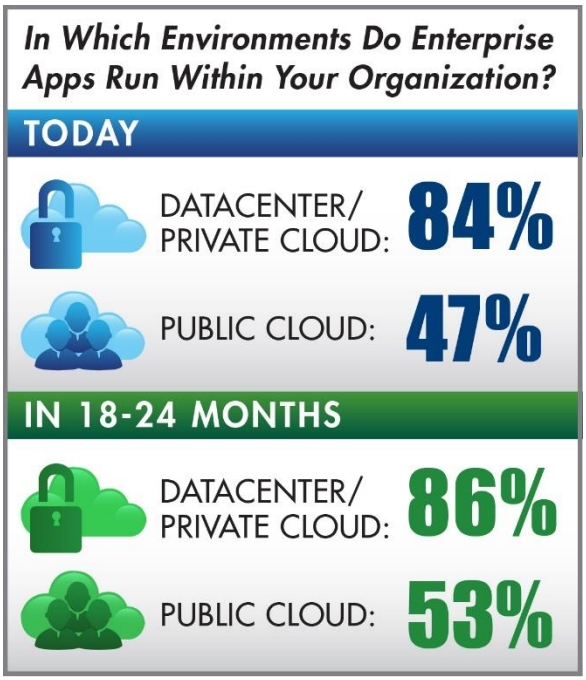
Consider SaaS. Some organizations wrongly believe that the need for SAM disappears when they deploy a SaaS solution. In actuality, the opposite is true – because while compliance issues may not be as prevalent – waste due to non-use or under-use is rampant with SaaS software. Why?

Most organizations fail to adequately monitor SaaS product use, resulting in over-licensed situations where subscriptions are paid for but not fully used. Software License Optimization best practices, processes and technology can and should be applied to SaaS software. Doing so would allow Asset Managers to ensure the licenses subscribed to are actually being used – eliminating waste.

SAM Protection from the Gathering Clouds

The same forces giving rise to SaaS and virtualization are also ushering in the age of the Infrastructure as a Service (IaaS). Organizations looking to lower their infrastructure costs, complexity and overhead are moving their software licenses to run on public, private and hybrid clouds.

Many organizations are looking to cloud environments to run their enterprise applications. For instance, 84 percent of organizations run at least some of their enterprise apps in a private cloud today. Within two years, this will increase to 86 percent. 47 percent of organizations run at least some of their enterprise applications in a public cloud. Within two years, this will increase to 53 percent.



WHY DOES THIS MATTER?

Organizations wrongly believe that if they move to the cloud, their SAM challenges disappear. In reality, the opposite is true – they become more complicated.

There are two critical themes organizations must consider before moving apps to the cloud (be it a public, private or hybrid cloud.) First they must look at the software license implications of moving an existing software package to the cloud (Bring your Own Software and License-BYOSL). Second, they must consider cloud infrastructure costs.

Bring Your Own Software and License:

Companies that bring their own software licenses to the cloud face particular risk. Where they run the software makes a difference from a licensing perspective. That's because software use is subject to licensing terms. And, just as occurred with the advent of virtualization, different software vendors have developed differing and often confusing rules associated with using their software in cloud environments. It's critical to understand that the license an organization has previously negotiated may or may not cover cloud based usage. Some vendors, for instance, may require customers to buy special licenses, while others may explicitly prohibit their software from running in the cloud.

Many datacenter server software products are licensed using CPU-based metrics and have specific terms for virtualization. For example, some IBM software is licensed using Processor Value Units (PVUs) and has specific requirements when the software runs on virtual machines. So, if an organization runs IBM software in a cloud, it will have to comply with IBM's rules and only run software in IBM's authorized public cloud environments (As described in the IBM Public Cloud BYOSL Policy). Otherwise IBM will want to know either the full CPU capacity of the physical machine running the IBM software, or the virtual capacity allocated to that software, in the case of sub-capacity licensing. This could present a difficult challenge as public vendors do not share their physical hardware information, and even if the data is obtained enterprises may be required by their contracts to pay for "full capacity," even though the instance that their software runs in is one of many virtual machines running on that server. And this can be very costly.

Cloud Infrastructure Costs

Public cloud offerings provide an attractive value proposition. They allow IT to get out of the business of running datacenters, where for years most of the budgets have been spent on hardware and software maintenance and upgrades. Instead, IT can focus on innovation, looking for better ways to support the business.

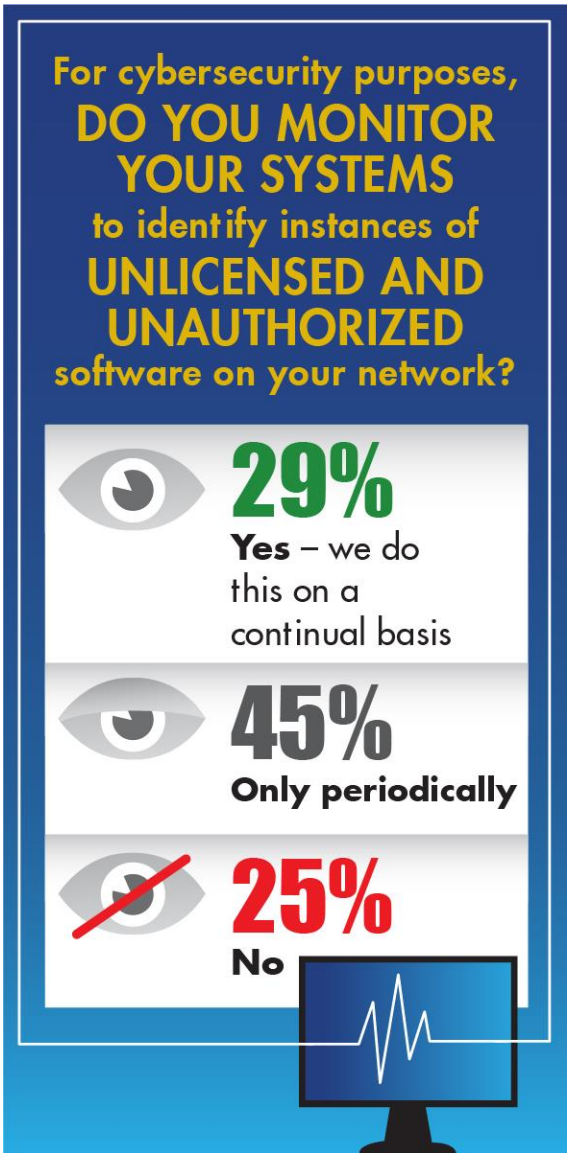
In Infrastructure as a Service (IaaS), organizations have the ability to only incur costs when they need the capacity. They simply turn on the cloud instances (virtual machines) for the amount of time needed. When the instance is turned off, the organization stops paying for it. However, most companies are not used to turning virtual machines off – which means oftentimes they pay for more cloud service than they actually need. The cost of the wasted usage appears small – pennies per hour. But, because a large organization may have hundreds or thousands of these…the pennies add up quickly. This is the risk of investing in cloud infrastructure services without proactively optimizing your infrastructure costs using SAM and license optimization tools.

Cloud services can provide real benefits, but, regardless of the type of Cloud services used, organizations need to consider employing software license optimization processes and technology to optimize their investment in cloud infrastructure. SAM tools must (and some already are) evolving to provide this type of optimization.

Software Vulnerability Management: Where SAM and Cybersecurity Meet

Security standards and requirements frameworks have been developed by myriad organizations over the years to address risks to enterprise systems and their critical data. The SANS Institute, one of the largest sources for information security training and security certification in the world, has created a prioritized list of security controls that would have the greatest impact in improving an organization's risk posture against real-world threats. The second SANS Critical Security Control dictates that organizations must actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and removed.

According to our survey data enterprises are falling far short when it comes to security. Only 29 percent of organizations continually monitor their systems for security purposes to identify unlicensed and unauthorized software. The rest do so only periodically or not at all.



WHY DOES THIS MATTER?

Most organizations have multiple sources of software and hardware inventory data. But they usually do not have a means to consolidate that data from across all their systems and environments. Nor the ability to arrive at an accurate, normalized inventory that can provide high-level insight into what authorized versus unauthorized software is running on the corporate network. And it is this lack of continual management-level insight that renders the very foundation of their security program vulnerable.

Companies invest considerable resources in achieving continual optimization to know, on an ongoing basis that they are only buying the software they need, using what they have and are in compliance with contract terms. That pristine SAM data being used so effectively is also of enormous value to security teams that need to understand what software exists in the IT environment, and whether or not that software is licensed and authorized for use. SAM solutions are now being utilized not only to support license compliance and cost reduction, but also security initiatives, like Software Vulnerability Management. Next-generation SAM tools actually integrate with Software Vulnerability Management solutions, bringing together IT Ops and security teams, enabling them to share the same software inventory data for their respective purposes.

The Bottom Line

SAM has moved from the fringes to the mainstream. Enterprises have experienced the pain and risk that occurs when their software assets are not managed properly, and SAM people, processes and technology are being implemented across organizations of all sizes to address the problem.

But the software landscape is constantly evolving. Virtualization, SaaS and the cloud are redefining the software asset management landscape too. SAM must evolve to redefine how software is managed in these new environments. And as software becomes the primary attack vector by which hackers invade corporate networks and threaten corporate security – SAM must also evolve to play its important role in corporate security.

Survey Background

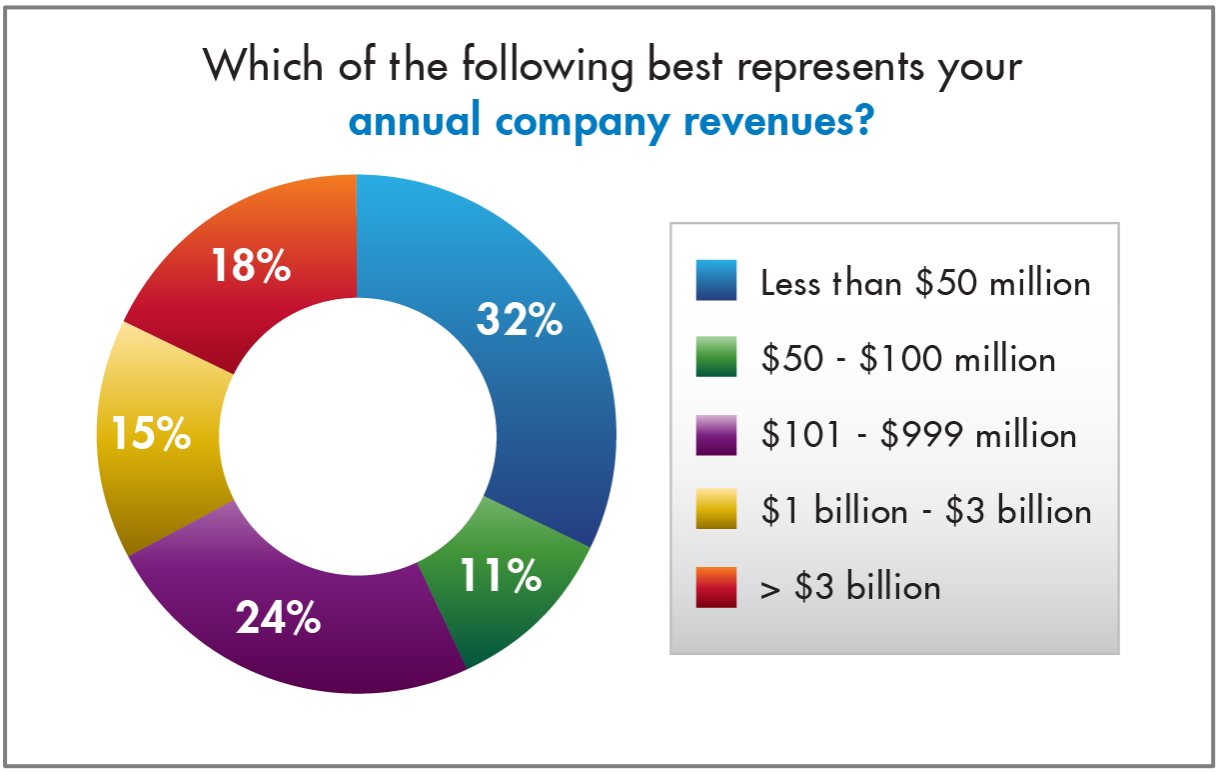
The *2016 Key Trends in Software Pricing and Licensing* survey was conducted by Flexera Software. This annual research project looks at software licensing, pricing and enforcement trends and best practices. The survey reaches out to executives at application producers (software vendors and intelligent device manufacturers) and enterprises who use and manage software and devices. Now in its tenth year, the survey is made available to the industry at large each year.

Methodology and Sampling

In total, 489 respondents participated in the survey, including 221 respondents to our enterprise survey and 268 respondents to our application producer survey.

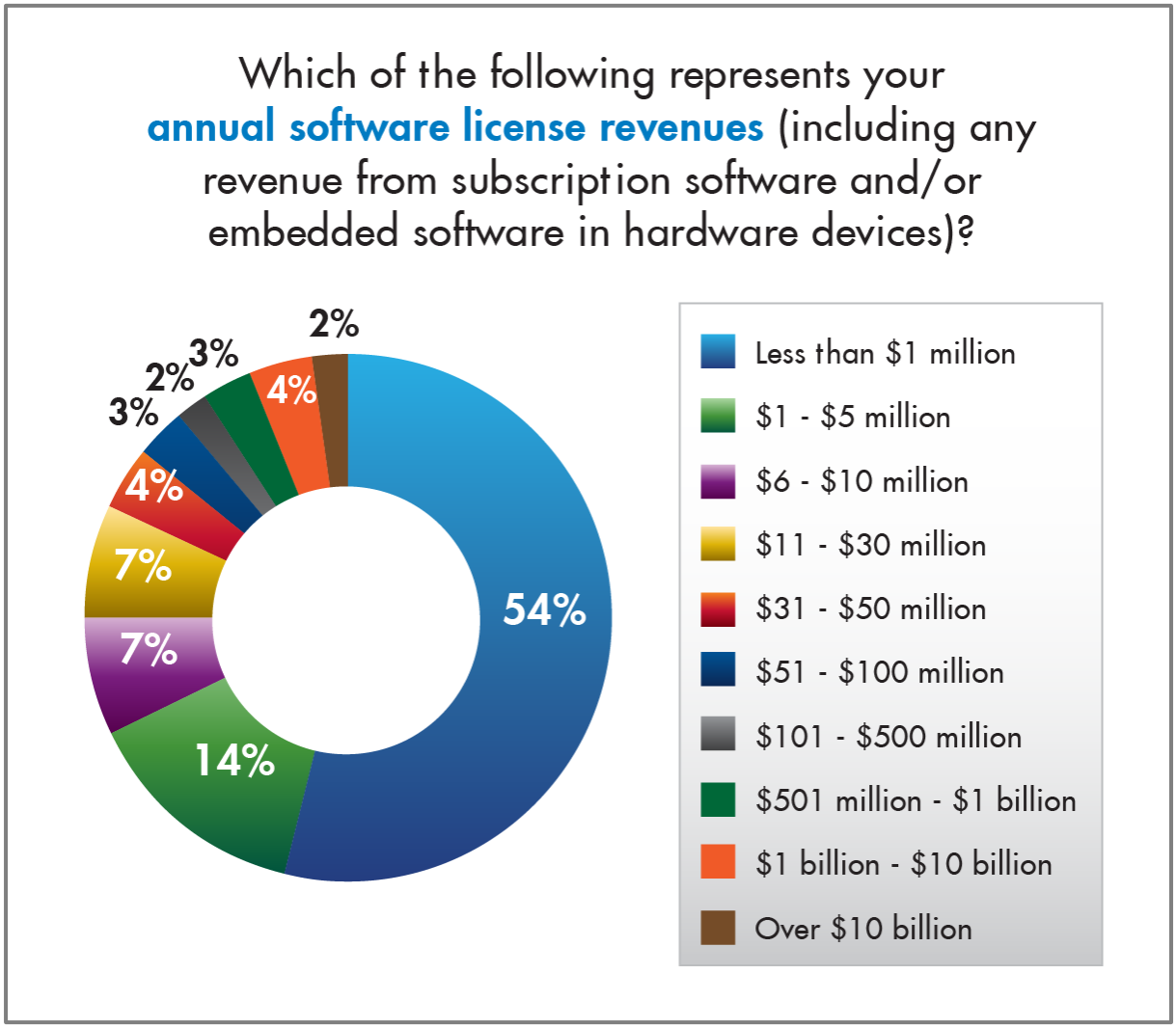
Enterprise Demographics

33% of the enterprise respondents were from larger enterprises of $1 billion or more in revenues and 18% were from companies with $3 billion in revenues or more. Among other places, 56% of respondents were from the United States, and the remainder from 37 countries across all continents.

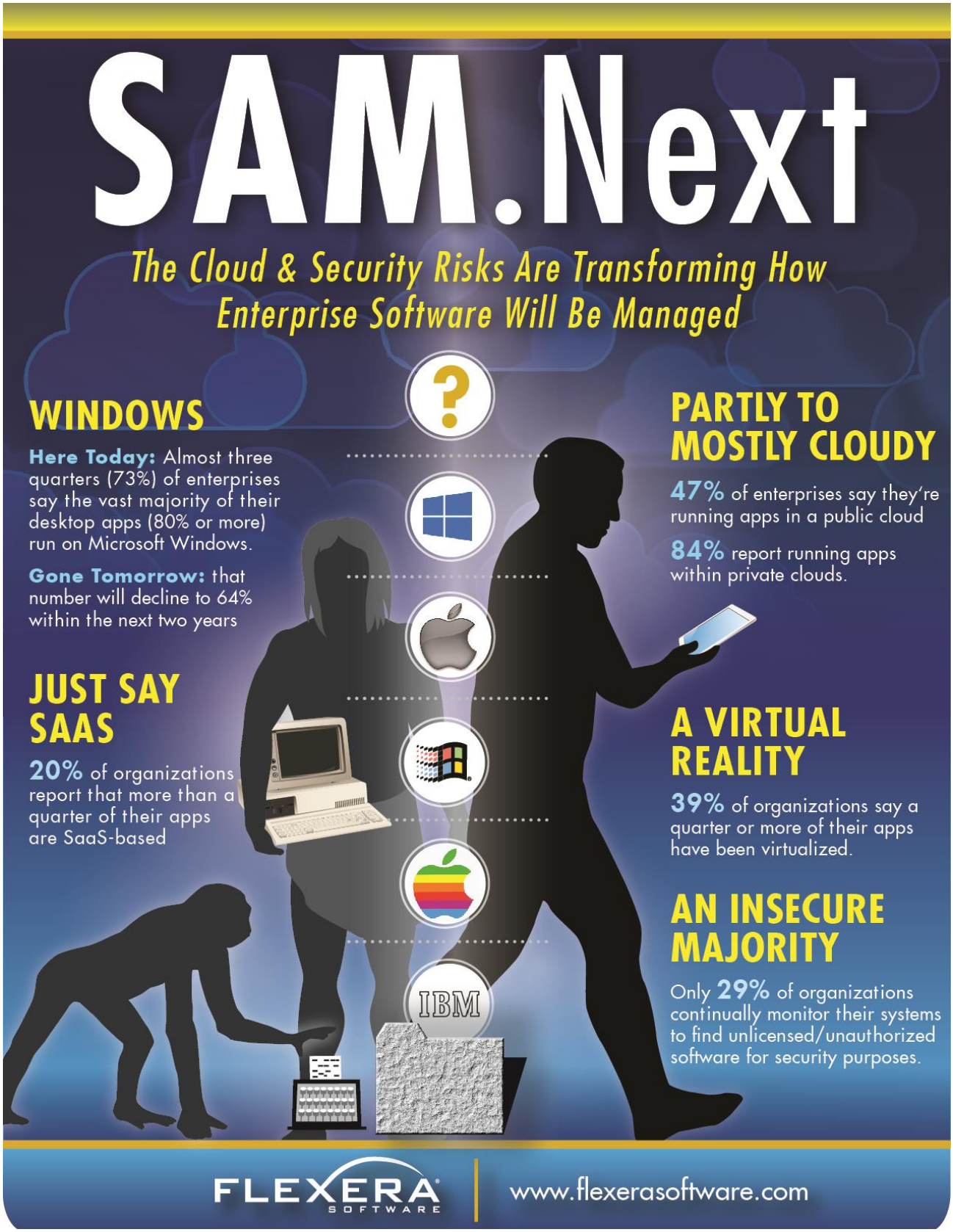


Application Producer Demographics

The largest segment of application producer respondents (54%) come from companies with under $1 million in revenues. 6% of the respondents were from companies with $1 billion or more in revenues. Among other places, 60% of respondents are from North America, and the remainder from 31 countries across all continents.



Infographic



About Flexera Software

Flexera Software helps application producers and enterprises increase application usage and security, enhancing the value they derive from their software. Our software licensing, compliance, cyber security and installation solutions are essential to ensure continuous licensing compliance, optimized software investments, and to future-proof businesses against the risks and costs of constantly changing technology. A marketplace leader for more than 25 years, 80,000+ customers turn to Flexera Software as a trusted and neutral source of knowledge and expertise, and for the automation and intelligence designed into our products. For more information, please go to: www.flexerasoftware.com.

FLEXERA®
SOFTWARE

www.flexerasoftware.com