

ASSET MANAGEMENT TRENDS 2021 CYBERSECURITY AS
CYBERSECURITY ASSET MANAGEMENT TRENDS 2021
TY ASSET MANAGEMENT TRENDS 2021 CYBERSECURIT
ENDS CYBERSECURITY ASSET MANAGEMENT TRENDS
SECURITY ASSET MANAGEMENT **HOW THE** 2021 CYB
ASSET MANAGEMENT TRENDS 2021 **RAPID SHIFT TO** ASSI
CYBERSECURITY ASSET MANAGEMENT TRENDS 2021
NDS **REMOTE** 2021 CYBERSECURITY ASSET MANAGEM
SECURITY ASSET MANAGEMENT TRENDS 2021 **WORK**
SECURITY ASSET MANAGEMENT TRENDS 2021 CYBER
TY ASSET MANAGEMENT TRENDS 2021 CYBERSECURIT
SECURITY ASSET MANAGEMENT **IMPACTED I.T.** 2021 CYB
ASSET MANAGEMENT **COMPLEXITY AND** 2021 CYBERSE
CYBERSECURITY ASSET MANAGEMENT TRENDS 2021
Y ASSET MANAGEMENT **POST-PANDEMIC** 2021 CYBERS
SET MANAGEMENT TRENDS **SECURITY PRIORITIES** ASSET
CYBERSECURITY ASSET MANAGEMENT TRENDS 2021
TY ASSET MANAGEMENT TRENDS 2021 CYBERSECUR
ASSET MANAGEMENT TRENDS 2021 CYBERSECURITY AS
CYBERSECURITY ASSET MANAGEMENT TRENDS 2021
TY ASSET MANAGEMENT TRENDS 2021 CYBERSECURIT
CYBERSECURITY ASSET MANAGEMENT TRENDS 2021
TY ASSET MANAGEMENT TRENDS 2021 CYBERSECURIT
ASSET MANAGEMENT TRENDS 2021 CYBERSECURITY AS



AXONIUS



a division of TechTarget

As organizations prepare for a “new normal” coming out of the pandemic, IT and security teams face new challenges associated with the trajectory of IT infrastructure. In a short time, the pandemic has proven out a new operating model for many, while concurrently resetting worker expectations.

IT and security teams responded urgently, with many deploying stopgap measures to support ongoing business operations. As the post-pandemic reality comes into focus, these same teams will need to formalize policies, infrastructure, and operations to effectively secure and scale their businesses.

CONTINUOUS VISIBILITY INTO ALL ASPECTS OF IT

INFRASTRUCTURE – BEGINNING WITH AN ACCURATE ASSET

INVENTORY OF DEVICES AND WORKLOADS – IS

FOUNDATIONAL TO THIS EFFORT.

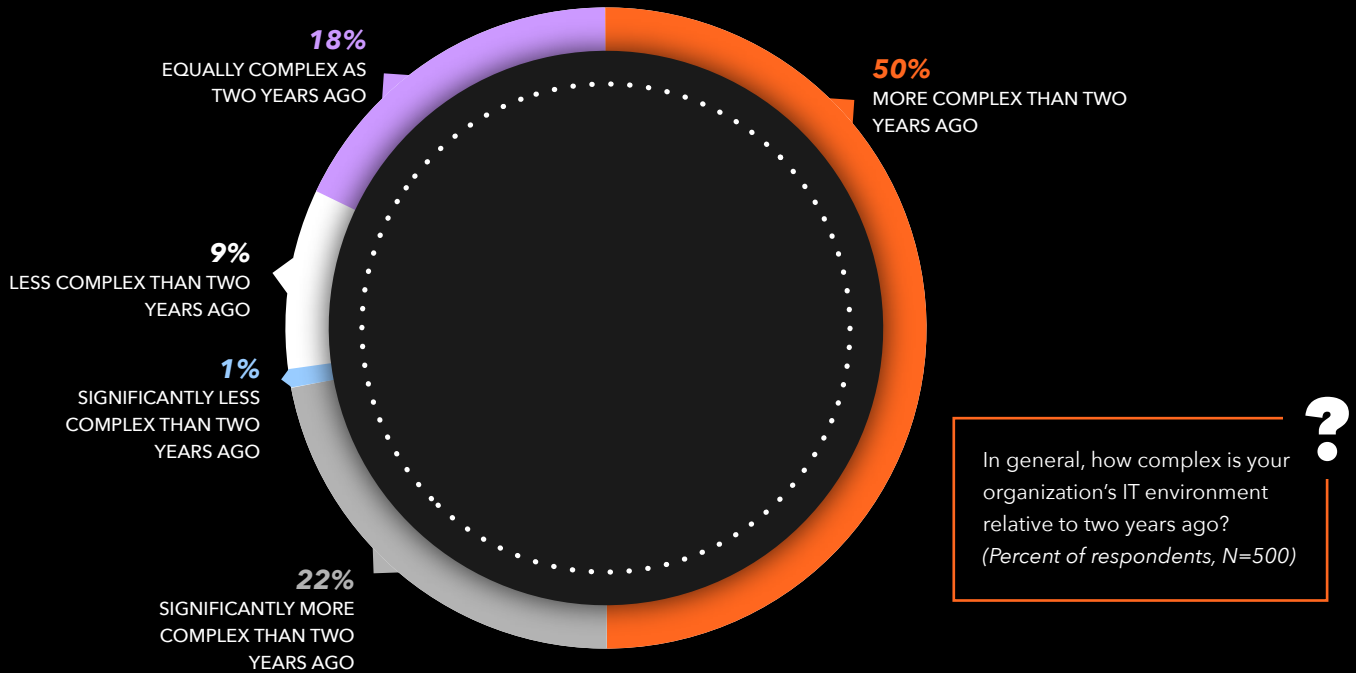
For many, this is an urgent priority for the coming year.

IT COMPLEXITY INCREASES WITH THE RAPID SHIFT TO REMOTE WORK

Modern IT infrastructure has grown to become highly diverse and dynamic, leaving many IT and security teams with a growing complexity problem. Research from Enterprise Strategy Group (ESG) shows:

72% OF RESPONDENTS REPORT INCREASED COMPLEXITY IN THEIR ENVIRONMENTS OVER THE PAST TWO YEARS.

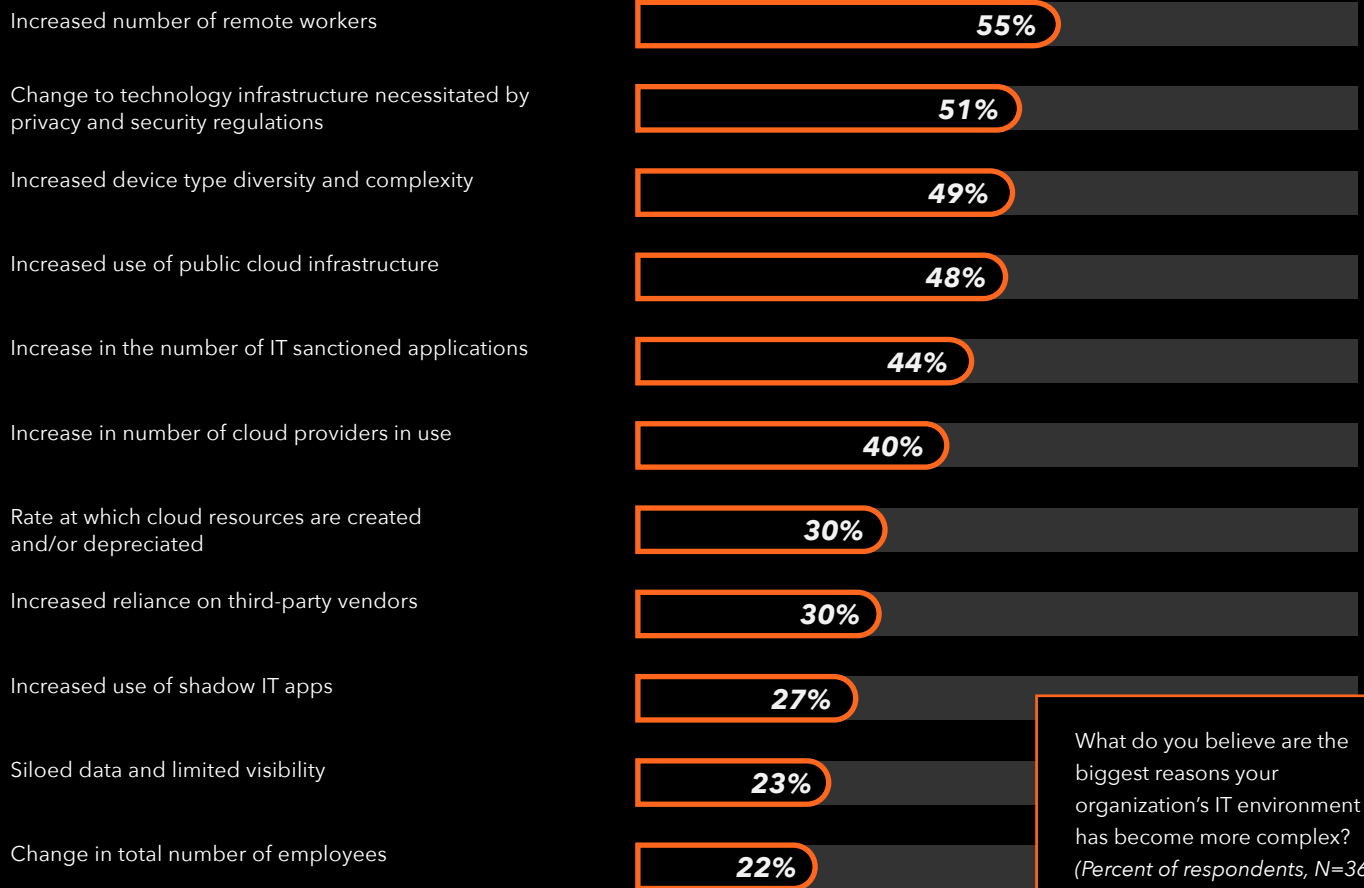
COMPLEXITY CONTINUES TO RISE, DESPITE INCREASED INVESTMENTS



The recent, rapid shift to remote work has further exacerbated the problem, leaving many IT and security teams blind to the personal networks and devices powering the remote workers.

55% OF ORGANIZATIONS REPORT THE MOVE TO REMOTE WORK IS A DRIVER OF INCREASED COMPLEXITY (THE NO. 1 MOST FREQUENTLY REPORTED CAUSE).

THE MOVE TO REMOTE WORK DROVE COMPLEXITY



What do you believe are the biggest reasons your organization's IT environment has become more complex?
(Percent of respondents, N=364, five responses accepted)

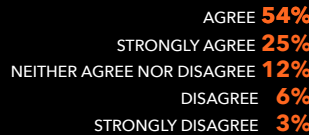
In concert with this move, digital transformation initiatives have accelerated the use of modern cloud operating models as businesses seize the opportunity to engage digitally within this new work paradigm. Managing and securing this increasingly complex environment begins with a basic

understanding of the individual IT assets involved in operating the business – from core business applications, to productivity and collaboration tools, to intelligent, internet-connected devices required to operate infrastructure supporting the efficient creation and delivery of products and services.

Collectively, these assets represent an attack surface that must be protected against an ever-expanding threat landscape used by adversaries to compromise infrastructure and carry out malicious activities. When IT and security teams lack visibility into any part of their attack surface, they lose the ability to meet security and operational objectives, putting the business at risk.

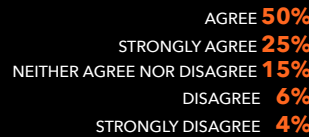
MANY ORGANIZATIONS REPORT WIDENING VISIBILITY GAPS IN THEIR CLOUD INFRASTRUCTURE (79%), END-USER DEVICES (75%), AND IOT DEVICE INITIATIVES (75%), ACCORDING TO ESG RESEARCH.

● VISIBILITY REMAINS A CHALLENGE



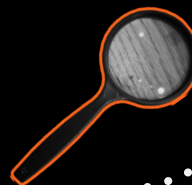
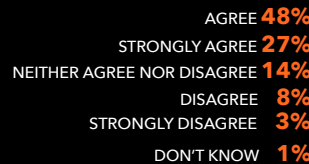
CLOUD VISIBILITY GAP IS WIDENING

Rate your level of agreement with the following statement: My organization has a visibility gap between what we can/could quickly and easily see about cloud infrastructure (IaaS/PaaS) assets and what we want to be able to see to effectively mitigate risk.
(Percent of respondents, N=500)



MOST ORGANIZATIONS LACK THE VISIBILITY THEY WANT INTO END-USER DEVICES

Rate your level of agreement with the following statement: My organization has a visibility gap between what we can quickly and easily see about end-user devices and what we want to be able to see to effectively mitigate risk.
(Percent of respondents, N=500)



IOT IS HAPPENING, BUT MOST LACK VISIBILITY

Rate your level of agreement with the following statement: My organization has/will have a visibility gap between what we can quickly and easily see about IoT devices and what we want to be able to see to effectively mitigate risk.
(Percent of respondents, N=483)



MORE DEVICE AND OPERATING DIVERSITY

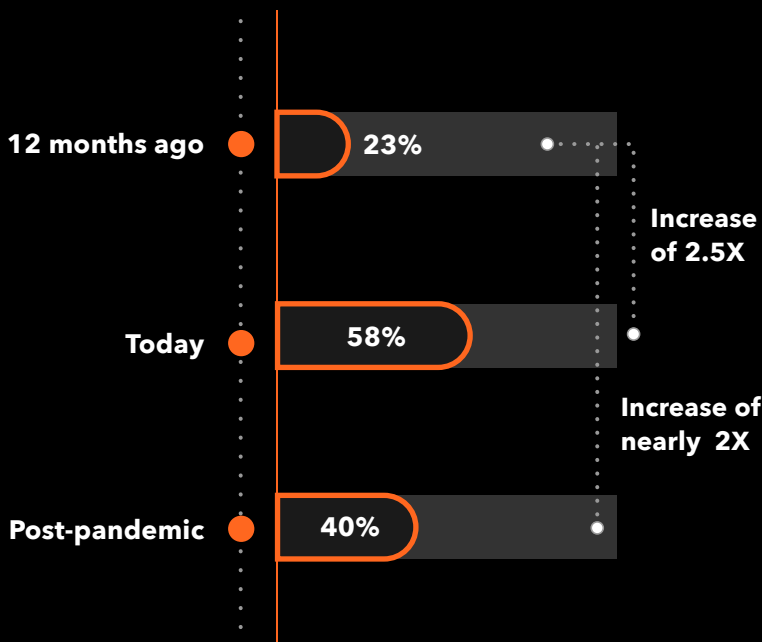
As IT and security teams see the light at the end of the tunnel, they are preparing for a “new normal” in IT operating environments. This preparation begins with understanding where and how workers will operate, where and how applications and services will operate, and how workers will interact with critical business and collaboration systems.

While many report workers will return to the office, others are expected to continue working remote.

ON AVERAGE, RESPONDENTS EXPECT 40% OF THEIR ORGANIZATION’S WORKFORCE WILL BE REMOTE WORKERS AFTER THE COVID-19 OUTBREAK IS CONTROLLED—AN INCREASE OF 74% RELATIVE TO BEFORE THE PANDEMIC.

THE NUMBER OF REMOTE WORKERS HAS MORE THAN DOUBLED SINCE THE PANDEMIC AND WILL NOT SNAP BACK TO PRE-PANDEMIC LEVELS

Percentage of remote workers

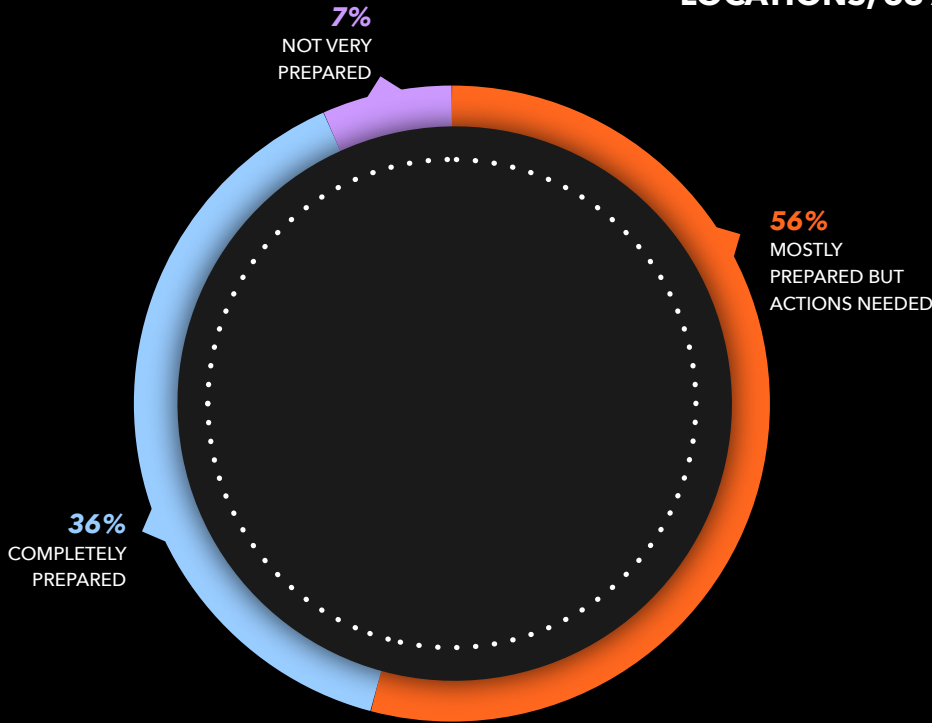


Twelve months ago, prior to the COVID-19 outbreak, approximately what percentage of your organization’s employees were remote users? What percentage of your organization’s total employees are remote users today?
(Mean, N=498)

Once the COVID-19 outbreak is controlled and it is safe for employees to return to the office, what percentage of your workforce do you expect will still work predominantly remotely?
(Mean, N=449)



WHILE MOST FEEL PREPARED FOR THE RETURN TO CORPORATE LOCATIONS, 63% REPORT THERE IS WORK TO BE DONE

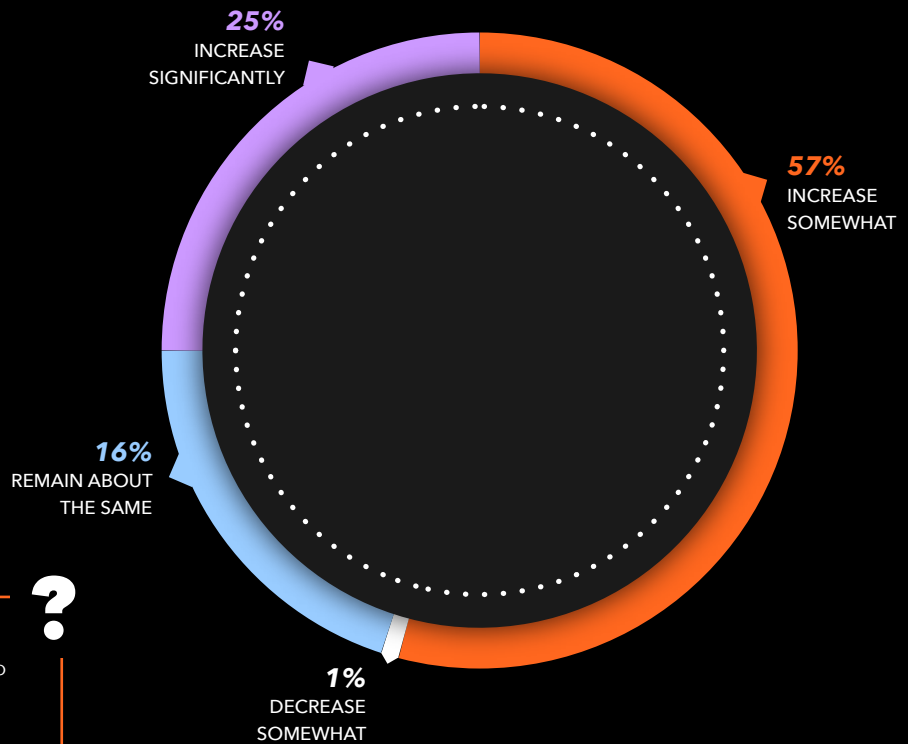


This requires organizations to develop a longer-term operating and security plan for a hybrid environment. Most are well underway preparing for this change, however 63% report they still have work to do.

How prepared do you believe your organization's network and security functions are for the coming influx of employees back to corporate locations (from remote work scenarios)?
(Percent of respondents, N=359)

4 OUT OF 5 PLAN TO INCREASE INVESTMENTS IN ASSET INVENTORY

Supporting the remote worker redirected both IT and security resources for much of 2020, deferring other previously planned initiatives. As organizations re-envision a state of normalcy, four out of five are planning investment to improve asset management to close visibility gaps.



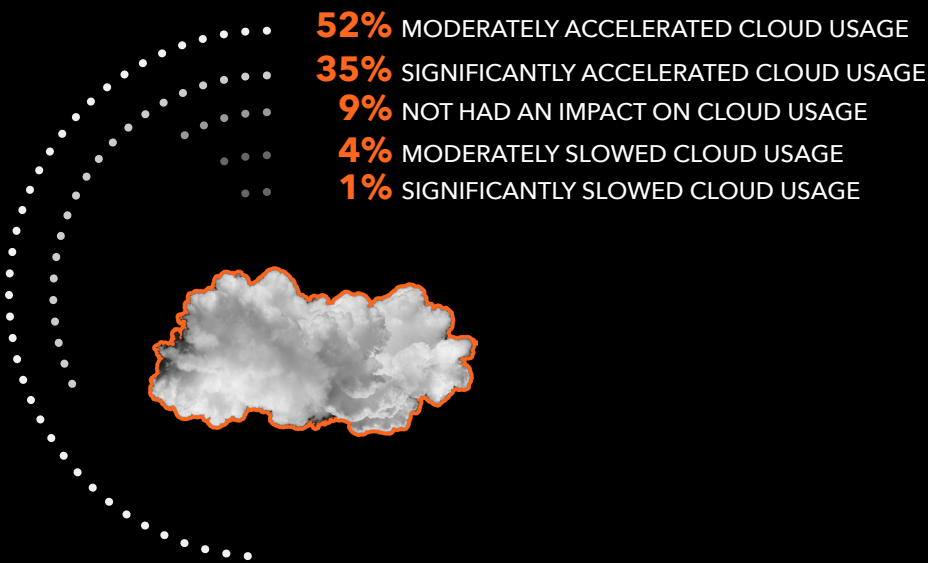
Over the next two years, how will your organization's spending on initiatives to improve asset management (including technologies, processes, services, etc.) change, if at all?
(Percent of respondents, N=500)

PUBLIC CLOUD CONTINUES TO ACCELERATE

While the move to public cloud was already well underway, the pandemic further accelerated the use of cloud-delivered productivity and collaboration tools while motivating businesses to expedite digital transformation initiatives, widely leveraging public cloud infrastructure.

IN FACT, 87% OF RESPONDENTS SAY THAT THE PANDEMIC HAS ACCELERATED PUBLIC CLOUD ADOPTION.

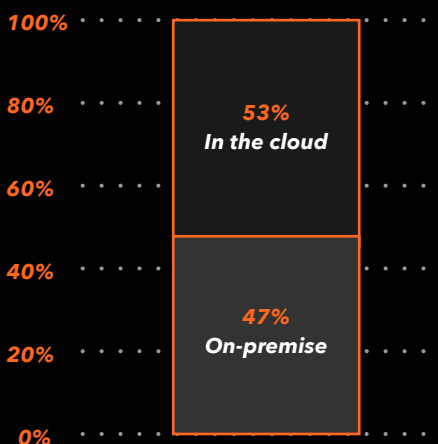
87% SAY THE PANDEMIC HAS ACCELERATED CLOUD INFRASTRUCTURE ADOPTION



Generally speaking, has the COVID-19 outbreak had an impact on your organization's use of public cloud infrastructure (IaaS/PaaS)?
(Percent of respondents, N=494)

OVER HALF OF IT INFRASTRUCTURE RESIDE IN THE CLOUD

With over half of IT infrastructure already residing in the cloud and digital transformation initiatives continuing to accelerate, public cloud has become a cornerstone of IT operations.

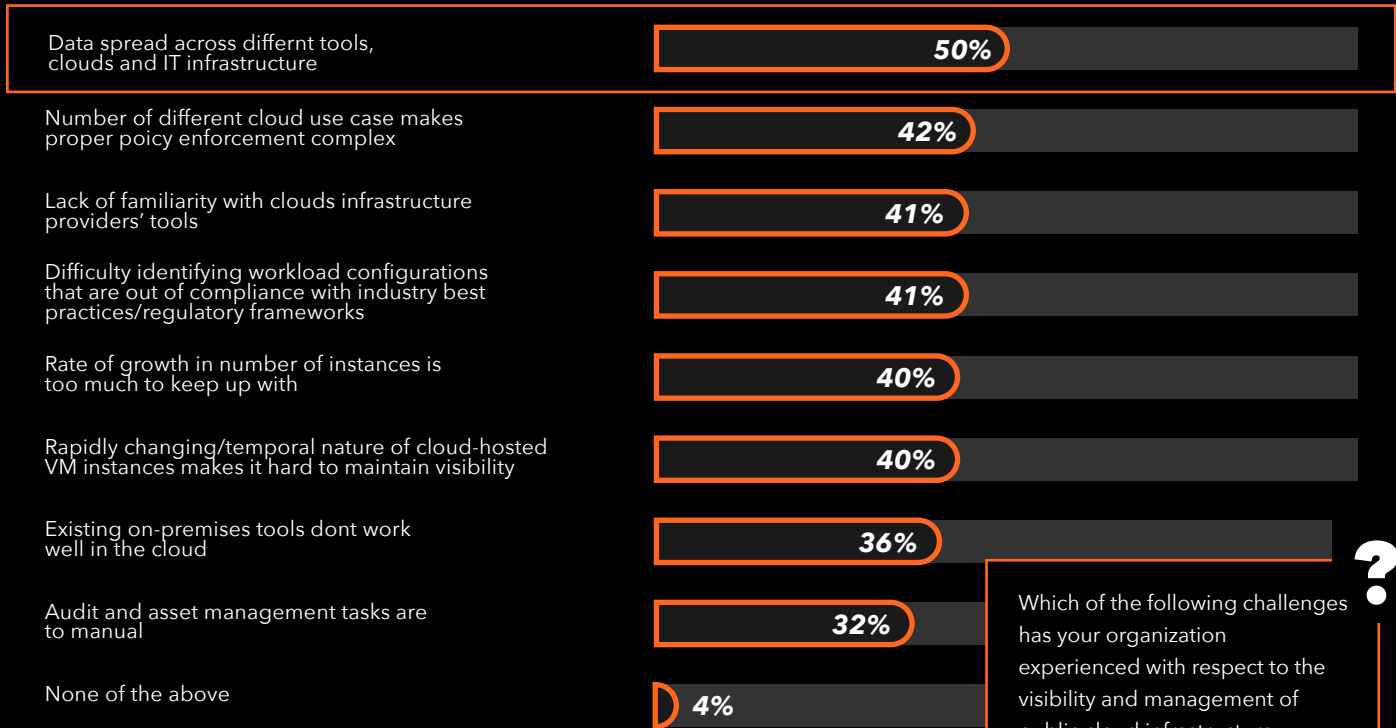


Approximately what percentage of your organization's IT infrastructure environment (e.g., storage, compute, containers, databases, etc.) do you believe is hosted in the cloud vs. on-premises?
(Mean, N=500)

These trends have spread data across a wide variety of infrastructure, multiple cloud service providers, and numerous SaaS applications, creating new complexity in securing and managing data privacy for critical data assets.

HALF OF ESG SURVEY RESPONDENTS REPORT VISIBILITY AND MANAGEMENT CHALLENGES WITH PUBLIC CLOUD INFRASTRUCTURE, ASSOCIATED WITH DATA SPREAD ACROSS DIFFERENT TOOLS, CLOUDS, AND INFRASTRUCTURE.

HALF REPORT VISIBILITY AND MANAGEMENT CHALLENGES ASSOCIATED WITH DATA SPRAWL

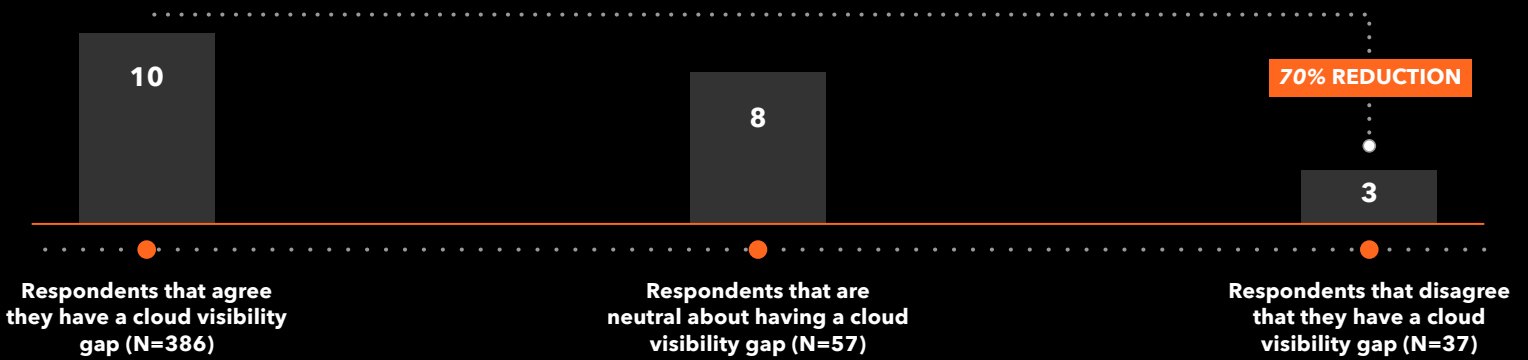


Which of the following challenges has your organization experienced with respect to the visibility and management of public cloud infrastructure (IaaS/PaaS)?
(Percent of respondents, N=494, multiple responses accepted)

When IT and security teams lack understanding about where critical data assets reside, they lack the ability to protect critical assets and uphold regulatory compliance laws. Moreover, our research shows a correlation between visibility gaps and security incidents like data loss or exploited vulnerabilities.

ORGANIZATIONS THAT HAVE ELIMINATED VISIBILITY GAPS REPORT A 70% REDUCTION IN PUBLIC CLOUD SECURITY INCIDENTS COMPARED TO THOSE WITH VISIBILITY GAPS (AN AVERAGE OF 10 INCIDENTS VS. 3).

BETTER CLOUD VISIBILITY CORRELATES TO A 70% REDUCTION IN SECURITY INCIDENTS



Approximately how many times has your organization experienced a security incident over the past year specifically related to its cloud infrastructure (IaaS/PaaS)?

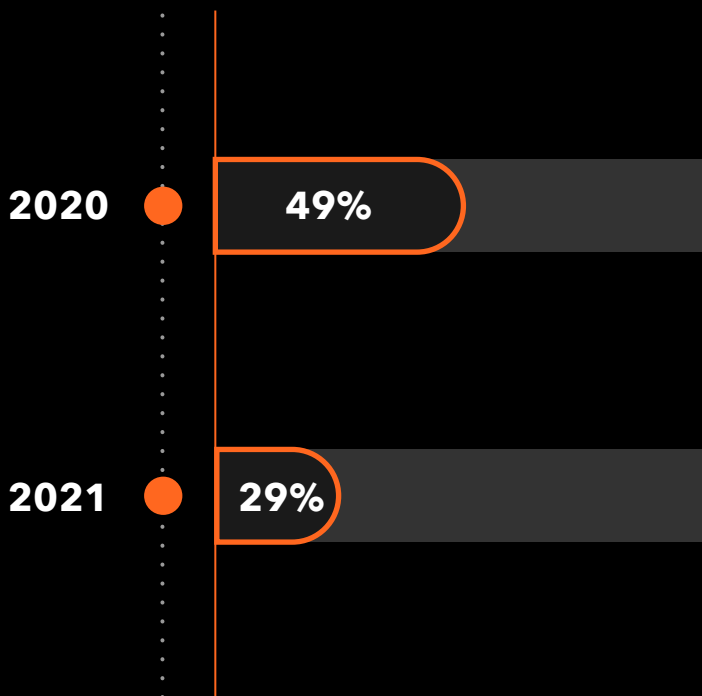
BYOD AND USER SERVICE POLICY ADAPT FOR THE REMOTE WORKER

The rapid move to remote work motivated a significant change in BYOD policies for many organizations. Pre-pandemic, half of organizations surveyed prohibited the use of personal devices for corporate activities.

POST-PANDEMIC, THIS NUMBER FELL TO **29%**, ADDING NEW MANAGEMENT AND SECURITY COMPLEXITY FOR THESE DEVICES.

BYOD POLICIES HAVE CHANGED DRAMATICALLY FROM 2020

Percentage of organizations prohibiting employees from using personal devices for work

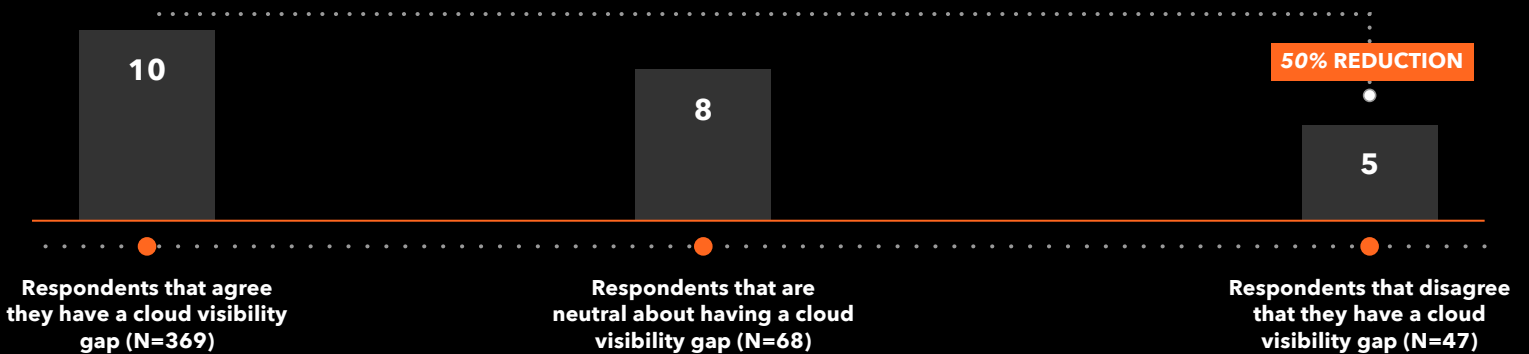


Are employees prohibited from using their own devices for work applications?

As workers depend on devices that are not corporate managed, they operate directly from endpoint to cloud workload, bypassing corporate infrastructure where other identity and access controls have traditionally been deployed. This creates blind spots for most organizations, which are again correlated with real security incidents like compromised systems.

ORGANIZATIONS THAT HAVE ELIMINATED VISIBILITY GAPS REPORT A 50% REDUCTION IN END-USER DEVICE SECURITY INCIDENTS RELATIVE TO THOSE WITH VISIBILITY GAPS (AVERAGE OF 10 INCIDENTS VS. 5).

CLOSING THE DEVICE VISIBILITY GAP CORRELATES TO A 50% REDUCTION IN SECURITY INCIDENTS



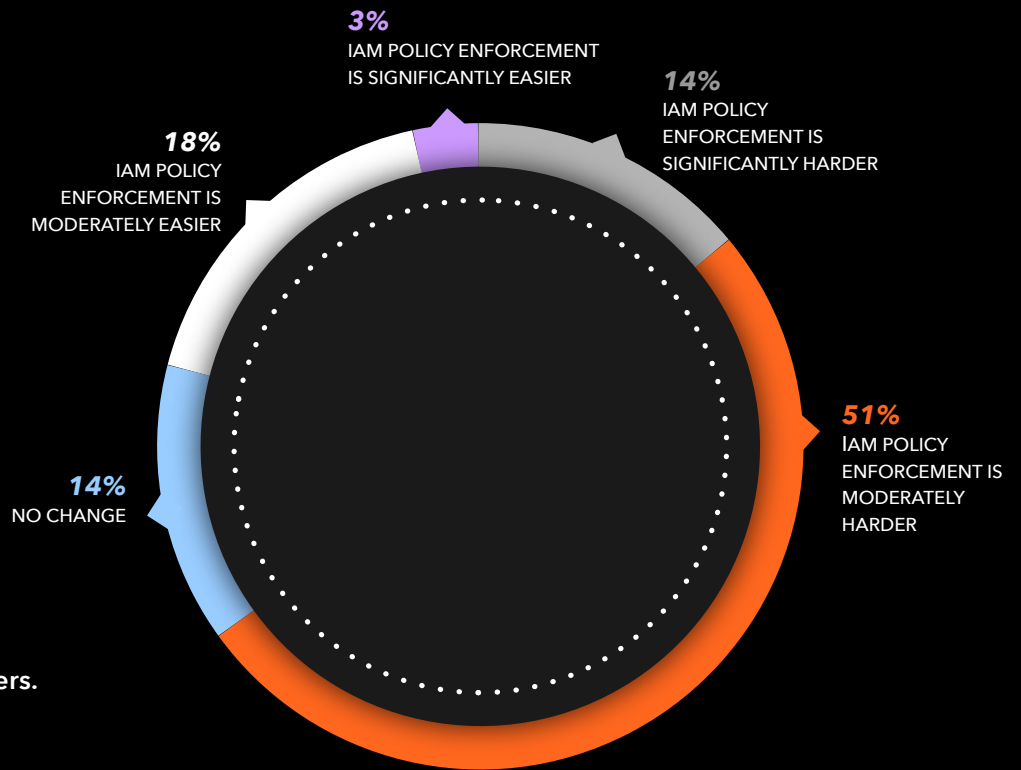
Approximately how many times has your organization experienced a security incident over the past year specifically related to its fleet of end-user devices (i.e., system compromise, exploited vulnerability, data breach, etc.)?

As device diversity increases, IT and security teams are putting more focus on identity and access management (IAM) solutions, with 65% reporting that IAM is more challenging as a result of supporting remote workers.

AS ORGANIZATIONS REESTABLISH A NEW NORMAL, OFFERING WORKERS NEW FLEXIBILITY TO USE NON-CORPORATE, PERSONAL DEVICES, MORE POLICY EVOLUTION IS EXPECTED – ALONG WITH ADDITIONAL FOCUS ON DIRECT-TO-CLOUD IAM SOLUTIONS.

IAM GAINS NEW IMPORTANCE

How has the increase in remote workers supported by your organization impacted the difficulty you associate with secure identity and access management (IAM) policy enforcement?
(Percent of respondents, N=449)



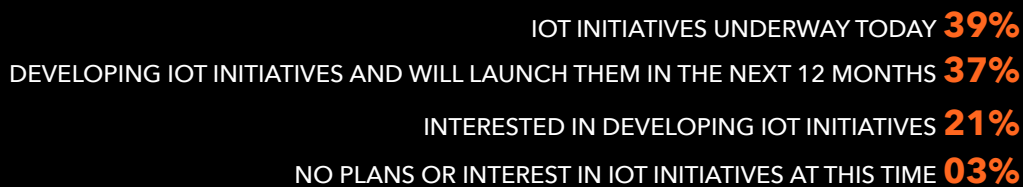
65% think that IAM is more challenging as a result of supporting more remote workers.

IOT PROJECTS DEFERRED AS RESOURCES REFOCUS ON REMOTE WORK

As the pandemic redirected IT and security resources to focus on supporting the remote worker and accelerated digital transformation, many IoT projects were furloughed.

OUR RESEARCH SHOWED A **16 PERCENTAGE-POINT DECLINE** IN THE PERCENTAGE OF ORGANIZATIONS WITH ACTIVE IOT PROJECTS (**55% A YEAR AGO COMPARED TO 39% TODAY**).

IOT PROJECTS DEFERRED DUE TO PANDEMIC



Based on this definition, how would you characterize your organization's internet-of-things (IoT) initiatives?
(Percent of respondents, N=500)

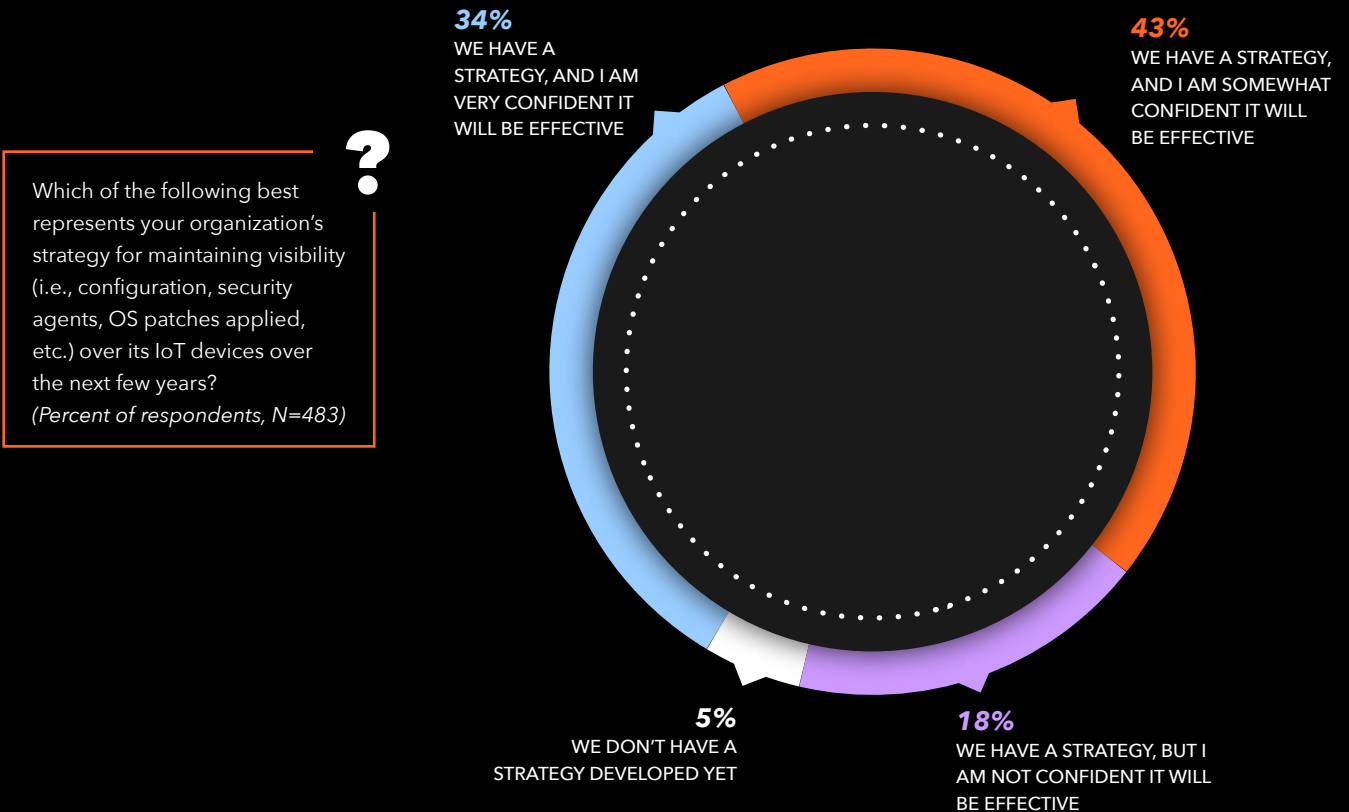


16% decline in active IoT projects

But IoT projects didn't go away. As organizations regain control over their new, multifaceted work environments, IoT projects will reignite, and organizations need to be ready.


WITH ONLY 34% REPORTING THEY HAVE A STRONG STRATEGY FOR MAINTAINING IOT DEVICE VISIBILITY, THERE IS WORK TO BE DONE.

ONLY ONE-THIRD ARE CONFIDENT IN THEIR IOT VISIBILITY STRATEGY



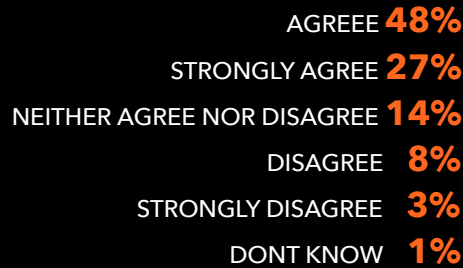
Proof of that fact: 75% of organizations believe they have or will have a visibility gap between what they can quickly and easily see about IoT devices, and what they want to be able to see to effectively mitigate risk.

● IOT IS HAPPENING, BUT MOST LACK VISIBILITY



 Please rate your level of agreement with the following statement: My organization has/will have a visibility gap between what we can quickly and easily see about IoT devices and what we want to be able to see to effectively mitigate risk.

(Percent of respondents, N=483)



Sixty-two percent report facing challenges with the variety of devices in use, making it difficult to know what agents should be installed and configurations should be in place. New strategies will be required.

● DIVERSITY IN IOT DEVICE TYPES IS THE LEADING CAUSE OF MANAGEMENT AND SECURITY CHALLENGES

Variety of devices in use/that will be in use makes it hard to know what agents should be installed and what configurations should be in place



Rate of growth in devices is/will be too much to keep up with



Tools we use don't support many of the connected devices we are/will support




Audit and asset management tasks are too manual



None of the above





 Which of the following challenges, if any, has or will your organization experience with respect to the visibility and management of IoT devices?

(Percent of respondents, N=483, multiple responses accepted)

MOST DEPEND ON MULTIPLE, INADEQUATE TOOLS FOR IT ASSET INVENTORY

Organizations continue to report challenges in keeping up with asset inventory and visibility.



The manual collection of data from multiple, separate, and overlapping tools



Involvement by different organizations and people who **manage these various tools**



Problems with deduplication



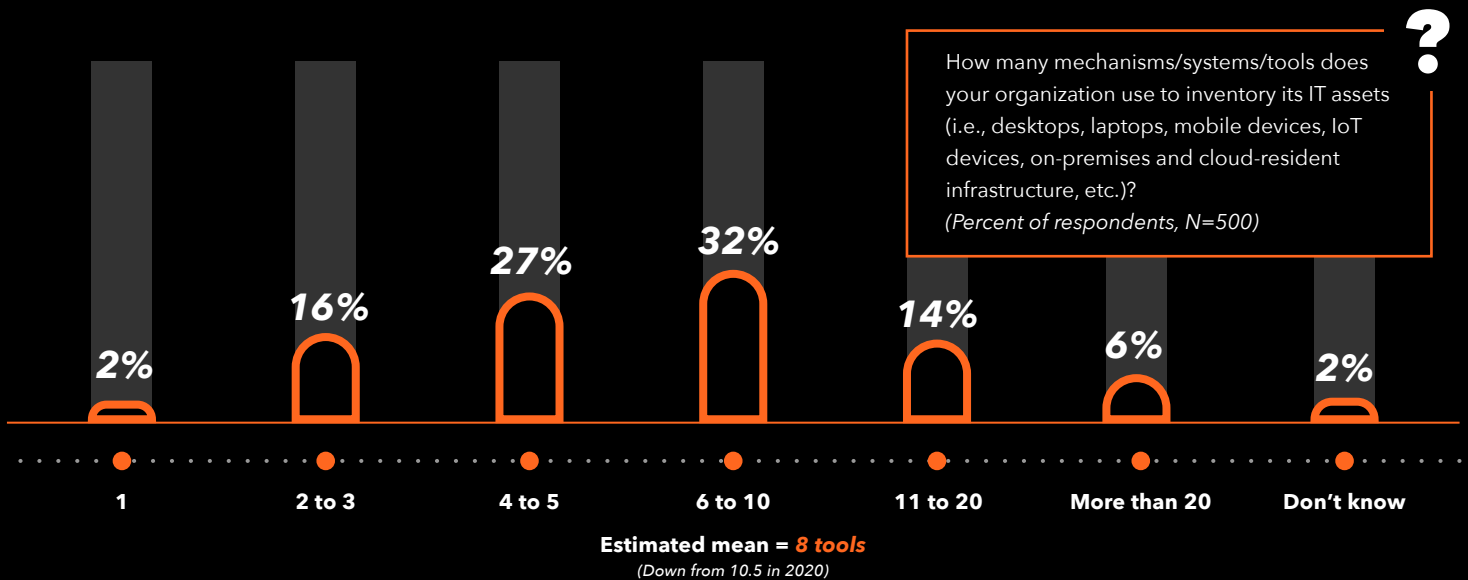
The pace of change for new devices and workloads



Lack of detailed visibility from the tools in use

On average, organizations depend on eight different tools to pull together asset inventories, while reporting intensively manual processes to pull together the data.

ON AVERAGE, 8 TOOLS ARE USED FOR ASSET INVENTORY

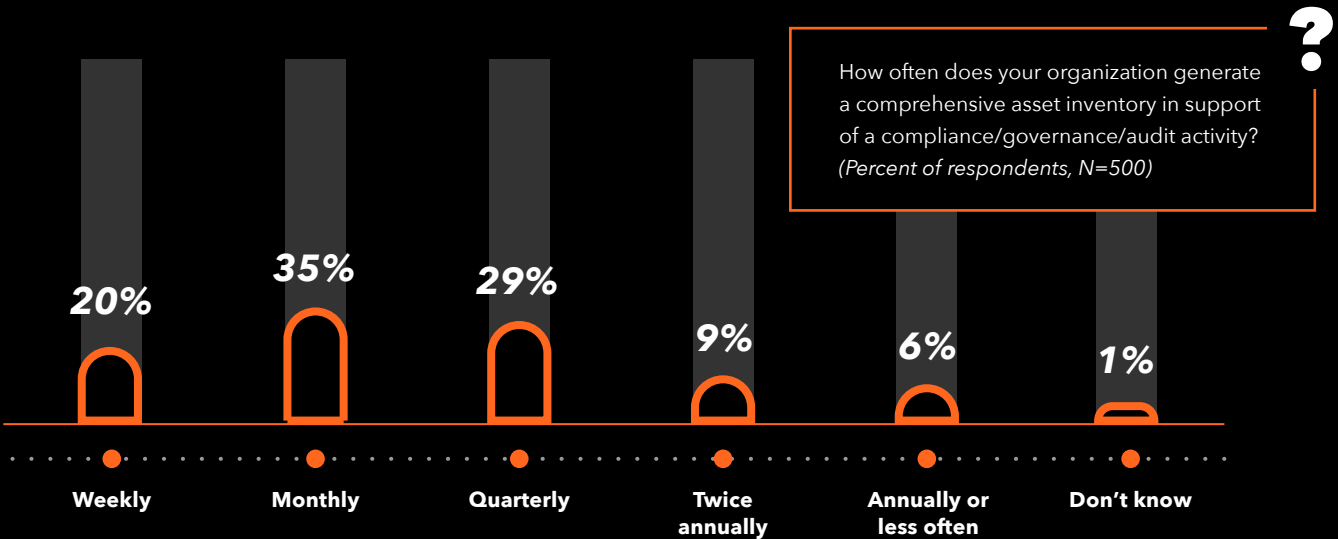


IT TAKES 86 PERSON-HOURS, ON AVERAGE, TO GENERATE AN ASSET INVENTORY, UTILIZING A COMBINATION OF TOOLS THAT WEREN'T BUILT FOR THIS TASK, INCLUDING:

- Endpoint management
- Endpoint security
- Network access controls
- Network scanning
- Configuration and patch management
- Vulnerability assessment

With this kind of effort, **nearly two-thirds (64%) report asset inventory as an event versus a process**, only updating inventories monthly or quarterly. This cadence leaves significant visibility gaps in-between, resulting in unmeasurable business risk.

● TWO-THIRDS REPORT ASSET INVENTORY AS AN EVENT



Looking back to **research data from last year**, organizations have made little progress solving this problem.

THE GOOD NEWS IS THAT 82% REPORT PLANS TO INCREASE INVESTMENTS THIS YEAR TO COMBAT THE PROBLEM.

● **4 OUT OF 5 PLAN TO INCREASE INVESTMENTS IN ASSET INVENTORY**

Over the next two years, how will your organization's spending on initiatives to improve asset management (including technologies, processes, services, etc.) change, if at all?
(Percent of respondents, N=500)



INCREASE SOMEWHAT **57%**
INCREASE SIGNIFICANTLY **25%**
REMAIN ABOUT THE SAME **16%**
DECREASE SOMEWHAT **1%**



iN AN IDEAL WORLD

IN AN IDEAL WORLD **IN** AN IDEAL WORLD IN AN IDEAL WORLD IN AN IDEAL WORLD
WORLD IN AN IDEAL WORLD IN **AN** IDEAL WORLD IN AN IDEAL WORLD IN AN IDEAL
ORLD IN AN IDEAL WORLD IN AN **IDEAL** WORLD IN AN IDEAL WORLD IN AN IDEAL W
EAL WORLD IN AN IDEAL WORLD IN AN IDEAL **WORLD** IN AN IDEAL WORLD IN AN ID
AN IDEAL WORLD IN AN IDEAL WORLD IN AN IDEAL WORLD IN AN IDEAL WORLD IN
IN AN IDEAL WORLD IN AN IDEAL WORLD IN AN IDEAL WORLD IN AN IDEAL WORLD

This year's survey once again reinforces the desire to redeploy IT and security resources currently consumed in the arduous asset inventory process to other more important

activities, including vulnerability assessment, validating security controls and infrastructure, and improved threat investigations and response.

● IN AN IDEAL WORLD

- **IT and security teams would have a continuous inventory of all IT assets, configuration, and the operating software that powers them.** As new devices and workloads are added or changed, continuous visibility would be readily available, helping IT and security teams close gaps that expose organizations to security and operational risk.
- IT and security teams would share a common view of their infrastructure, **manifesting in a more collaborative, efficient workflow to manage and secure the environment.**
- As organizations return to some state of normalcy, getting asset inventory under control can help organizations free up security and IT resources, redeploying them to more important tasks.

IN 2021, ORGANIZATIONS WILL BE ABLE TO GET ASSET INVENTORY UNDER CONTROL, BRINGING NEEDED CONTINUOUS ATTACK SURFACE VISIBILITY. THIS WILL RESULT IN IMPROVED SECURITY POSTURE AND A REDUCTION IN THE COST OF ASSET INVENTORY.

**AXONIUS.COM** ●

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with over 300 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

330 MADISON AVE., 39TH FLOOR
NEW YORK, NY 10017
INFO@AXONIUS.COM

[REQUEST DEMO](#)

RESEARCH METHODOLOGY

To gather data for this eBook, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada), Western Europe (UK and Germany), and APAC (Australia, Hong Kong, New Zealand, and Singapore) between January 22, 2021 and February 12, 2021.

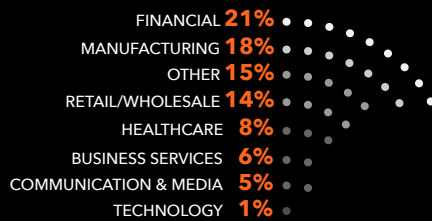
To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally knowledgeable with their organization’s cybersecurity environment and cloud infrastructure usage. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents. After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 500 IT and cybersecurity professionals.

RESPONDENTS BY NUMBER OF EMPLOYEES



How many total employees does your organization have worldwide?
(Percent of respondents, N=500)

RESPONDENTS BY INDUSTRY



What is your organization's primary industry?
(Percent of respondents, N=500)

RESPONDENTS BY ANNUAL REVENUE

