HOW THE RAPID SHIFT TO REMOTE WORK IMPACTED I.T. COMPLEXITY AND POST-PANDEMIC SECURITY TRENDS

Finance Edition
As financial services 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 and security teams have certainly risen to the occasion to keep organizations and their employees productive through one of the wildest years in history. Humans are resilient creatures, and those in the technology world certainly did not disappoint. But as the world begins to recover from it all, technology has evolved with some notable changes, requiring organizations to rethink many of their operational fundamentals. To discover how organizations were impacted, Axonius partnered with ESG to survey IT and security professionals across a wide range of industries. This report shares the overall results and highlights areas where respondents from the finance industry differed significantly from other industries.
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.**

In general, how complex is your organization’s IT environment relative to two years ago? (Percent of respondents, N=500)
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. Financial services organizations were also more likely to report a move to multicloud environments, which added to their IT complexity in the last year.

### 63% of Organizations in the Financial Services Industry 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

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased number of remote workers</td>
<td>55%</td>
</tr>
<tr>
<td>Change to technology infrastructure necessitated by privacy and security regulations</td>
<td>51%</td>
</tr>
<tr>
<td>Increased device type diversity and complexity</td>
<td>49%</td>
</tr>
<tr>
<td>Increased use of public cloud infrastructure</td>
<td>48%</td>
</tr>
<tr>
<td>Increase in the number of IT sanctioned applications</td>
<td>44%</td>
</tr>
<tr>
<td>Increase in number of cloud providers in use</td>
<td>40%</td>
</tr>
<tr>
<td>Rate at which cloud resources are created and/or depreciated</td>
<td>30%</td>
</tr>
<tr>
<td>Increased reliance on third-party vendors</td>
<td>30%</td>
</tr>
<tr>
<td>Increased use of shadow IT apps</td>
<td>27%</td>
</tr>
<tr>
<td>Siloed data and limited visibility</td>
<td>23%</td>
</tr>
<tr>
<td>Change in total number of employees</td>
<td>22%</td>
</tr>
</tbody>
</table>

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)
## The Move to Remote Work Drove Complexity

### Finance

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased number of remote workers</td>
<td>63%</td>
</tr>
<tr>
<td>Change to technology infrastructure necessitated by privacy and security regulations</td>
<td>51%</td>
</tr>
<tr>
<td>Increase in number of cloud providers in use</td>
<td>46%</td>
</tr>
<tr>
<td>Increased device type diversity and complexity</td>
<td>44%</td>
</tr>
<tr>
<td>Increased use of public cloud infrastructure</td>
<td>38%</td>
</tr>
<tr>
<td>Rate at which cloud resources are created and/or depreciated</td>
<td>36%</td>
</tr>
<tr>
<td>Increase in the number of IT sanctioned applications</td>
<td>35%</td>
</tr>
<tr>
<td>Increased use of shadow IT apps</td>
<td>35%</td>
</tr>
<tr>
<td>Increased reliance on third-party vendors</td>
<td>31%</td>
</tr>
<tr>
<td>Siloed data and limited visibility</td>
<td>28%</td>
</tr>
<tr>
<td>Change in total number of employees</td>
<td>24%</td>
</tr>
</tbody>
</table>

What do you believe are the biggest reasons your organization’s IT environment has become more complex? (Percent of respondents, N=104, 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.

**VISIBILITY REMAINS A CHALLENGE**

Many organizations report widening visibility gaps in their cloud infrastructure (79%), end-user devices (75%), and IoT device initiatives (75%), according to ESG research.

**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.

<table>
<thead>
<tr>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Neither Agree Nor Disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>54%</td>
<td>25%</td>
<td>12%</td>
<td>6%</td>
<td>3%</td>
</tr>
</tbody>
</table>

(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.

<table>
<thead>
<tr>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Neither Agree Nor Disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>25%</td>
<td>15%</td>
<td>6%</td>
<td>4%</td>
</tr>
</tbody>
</table>

(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.

<table>
<thead>
<tr>
<th>Agree</th>
<th>Strongly Agree</th>
<th>Neither Agree Nor Disagree</th>
<th>Disagree</th>
<th>Strongly Disagree</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>48%</td>
<td>27%</td>
<td>14%</td>
<td>8%</td>
<td>3%</td>
<td>1%</td>
</tr>
</tbody>
</table>

(Percent of respondents, N=483)
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.

**FINANCIAL SERVICES ORGANIZATIONS WERE AMONG THE MOST IMPACTED BY WORKERS SHIFTING TO REMOTE WORK DURING THE PANDEMIC (22% A YEAR AGO, COMPARED TO 64% TODAY).**
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)

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

POST-PANDEMIC, 46% OF WORKERS IN FINANCIAL SERVICES WILL REMAIN REMOTE – AN INCREASE OF 109% RELATIVE TO BEFORE THE PANDEMIC.

Remote Workers Overall

12 months ago 23%
Today 58%
Post-Pandemic 40%

Increase of 2.5X
Increase of nearly 2X

Remote Workers in Finance

12 months ago 22%
Today 64%
Post-Pandemic 46%
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)

- 57% increase
- 25% increase significantly
- 16% remain about the same
- 7% not very prepared
- 1% decrease somewhat

4 out of 5 plan to increase investments in asset inventory

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)

- 36% completely prepared
- 56% increase somewhat
- 16% completely prepared
- 7% not very prepared
- 1% decrease somewhat

Cybersecurity Asset Management Trends 2021
How the Rapid Shift to Remote Work Impacted IT Complexity and Post-Pandemic Security Trends
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.**

- **52%** MODERATELY ACCELERATED CLOUD USAGE
- **35%** SIGNIFICANTLY ACCELERATED CLOUD USAGE
- **9%** NOT HAD AN IMPACT ON CLOUD USAGE
- **4%** MODERATELY SLOWED CLOUD USAGE
- **1%** SIGNIFICANTLY SLOWED CLOUD USAGE

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)

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.

**OVER HALF OF IT INFRASTRUCTURE RESIDE IN THE CLOUD**

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**

- Data spread across different tools, clouds and IT infrastructure: 50%
- Number of different cloud use case makes proper policy enforcement complex: 42%
- Lack of familiarity with clouds infrastructure providers’ tools: 41%
- Difficulty identifying workload configurations that are out of compliance with industry best practices/regulatory frameworks: 41%
- Rate of growth in number of instances is too much to keep up with: 40%
- Rapidly changing/temporal nature of cloud-hosted VM instances makes it hard to maintain visibility: 40%
- Existing on-premises tools don’t work well in the cloud: 36%
- Audit and asset management tasks are too manual: 32%
- None of the above: 4%
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*

Respondents that agree they have a cloud visibility gap (N=386)

Respondents that are neutral about having a cloud visibility gap (N=57)

Respondents that disagree that they have a cloud visibility gap (N=37)

Approximately how many times has your organization experienced a security incident over the past year specifically related to its cloud infrastructure (IaaS/PaaS)?
The move to remote work required most organizations to reprioritize plans, delaying some initiatives while accelerating others. The overnight need to support non-corporate devices forced teams to implement stopgap policies for BYOD devices. Many also report deferring planned IoT projects while focusing on remote work enablement and accelerated digital transformation initiatives. Reprioritization will continue as organizations prepare for a new, hybrid operating environment.
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.**

**FINANCIAL SERVICES ORGANIZATIONS WERE THE MOST ACCEPTING OF PERSONAL DEVICES, WITH ONLY 17% PROHIBITING PERSONAL DEVICE USE**

---

**BYOD POLICIES HAVE CHANGED DRAMATICALLY FROM 2020**

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage of employees prohibited from using personal devices for work</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>49%</td>
</tr>
<tr>
<td>2021</td>
<td>29%</td>
</tr>
</tbody>
</table>

Employees are prohibited from using their own devices for work applications. (Percent of respondents, N=500)
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. Financial services organizations reported the highest number – 11 – of incidents over the past year related to end-user devices.

Organizations that have eliminated visibility gaps report a \textbf{50\% reduction} in end-user device security incidents relative to those with visibility gaps (average of 10 incidents vs. 5).

\begin{itemize}
  \item \textbf{Respondents that agree they have a cloud visibility gap (N=369)}
  \item \textbf{Respondents that are neutral about having a cloud visibility gap (N=68)}
  \item \textbf{Respondents that disagree they have a cloud visibility gap (N=47)}
\end{itemize}

\begin{center}
\begin{tabular}{c|c|c}
   & 10 & 8 & 5 \\
\hline
Respondents that agree they have a cloud visibility gap (N=369) & 10 & 8 & 5 \\
Respondents that are neutral about having a cloud visibility gap (N=68) & 8 & 8 & 5 \\
Respondents that disagree they have a cloud visibility gap (N=47) & 5 & 5 & 5 \\
\end{tabular}
\end{center}

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)

- 51% IAM POLICY ENFORCEMENT IS MODERATELY HARDER
- 14% IAM POLICY ENFORCEMENT IS SIGNIFICANTLY HARDER
- 3% IAM POLICY ENFORCEMENT IS SIGNIFICANTLY EASIER
- 18% IAM POLICY ENFORCEMENT IS MODERATELY EASIER
- 14% NO CHANGE
- 65% think that IAM is more challenging as a result of supporting more remote workers.
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**

- IOT INITIATIVES UNDERWAY TODAY **39%**
- DEVELOPING IOT INITIATIVES AND WILL LAUNCH THEM IN THE NEXT 12 MONTHS **37%**
- INTERESTED IN DEVELOPING IOT INITIATIVES **21%**
- NO PLANS OR INTEREST IN IOT INITIATIVES AT THIS TIME **03%**

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

Which of the following best represents your organization’s strategy for maintaining visibility (i.e., configuration, security agents, OS patches applied, etc.) over its IoT devices over the next few years?

(Percent of respondents, N=483)
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.

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.

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)

IOT IS HAPPENING, BUT MOST LACK VISIBILITY

<table>
<thead>
<tr>
<th>Level of Agreement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreee</td>
<td>48%</td>
</tr>
<tr>
<td>Strongly Agree</td>
<td>27%</td>
</tr>
<tr>
<td>Neither Agree nor Disagree</td>
<td>14%</td>
</tr>
<tr>
<td>Disagree</td>
<td>8%</td>
</tr>
<tr>
<td>Strongly Disagree</td>
<td>3%</td>
</tr>
<tr>
<td>Don’t Know</td>
<td>1%</td>
</tr>
</tbody>
</table>

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)
The pandemic has increased the attack surface for many organizations. Without proper visibility into their operating infrastructure, IT and security teams risk losing control. Most report challenges and visibility gaps, making IT asset inventory discovery and management a priority.
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**

![Bar chart showing the distribution of tools used for asset inventory](chart.png)

How many mechanisms/systems/tools does your organization use to inventory its IT assets (i.e., desktops, laptops, mobile devices, IoT devices, on-premises and cloud-resident infrastructure, etc.)? (Percent of respondents, N=500)

- 1: 2%
- 2 to 3: 16%
- 4 to 5: 27%
- 6 to 10: 32%
- 11 to 20: 14%
- More than 20: 6%
- Don’t know: 2%

Estimated mean = 8 tools (Down from 10.5 in 2020)
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.

**How often does your organization generate a comprehensive asset inventory in support of a compliance/governance/audit activity? (Percent of respondents, N=500)**

- **Weekly**: 20%
- **Monthly**: 35%
- **Quarterly**: 29%
- **Twice annually**: 9%
- **Annually or less often**: 6%
- **Don't know**: 1%
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%
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, bring needed continuous attack surface visibility, resulting in improved security posture and a reduction in the cost of asset inventory.

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.

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.

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.

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.

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.

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.

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.
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

- 5,000 TO 9,999: 31%
- 2,500 TO 4,999: 23%
- 1,000 TO 2,499: 20%
- 20,000 OR MORE: 13%
- 10,000 TO 19,999: 13%
- 5,000 TO 9,999: 31%

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

RESPONDENTS BY INDUSTRY

- FINANCIAL: 21%
- MANUFACTURING: 18%
- OTHER: 15%
- RETAIL/WHOLESALE: 14%
- HEALTHCARE: 8%
- BUSINESS SERVICES: 6%
- COMMUNICATION & MEDIA: 5%
- TECHNOLOGY: 1%

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

RESPONDENTS BY ANNUAL REVENUE

- $100 million to $249.999 million: 6%
- $250 million to $499.999 million: 9%
- $500 million to $999.999 million: 19%
- $1 billion to $9.999 million: 28%
- $5 billion to $19.999 million: 15%
- $10 billion to $19.999 million: 11%
- $20 billion to $39.999 million: 5%
- $40 billion or more: 7%

How the Rapid Shit to Remote Work Impacted IT Complexity and Post-Pandemic Security Trends