MeriTalk
Improving the Outcomes of Government IT

RSAConference™
Where the World Talks Security™

Underwritten by:
FORTINET FEDERAL

The Art of Human and AI Teaming in Cybersecurity

April 2024

Introduction

From relentless ransomware attacks to sophisticated social engineering, the cyber threat landscape is expanding at a breakneck pace. While **artificial intelligence** (AI) technologies, like machine learning (ML) and natural language processing (NLP), are not new to cybersecurity, their applications are quickly evolving from optional enhancements to strategic necessities. Today's AI will change cybersecurity – bringing unprecedented opportunities and challenges. How can cybersecurity professionals work with AI to address threats head-on and usher in a new era of cyber readiness?

To explore the state of AI in cybersecurity, MeriTalk and RSA Conference™ compiled qualitative data from five in-depth interviews with senior cybersecurity leaders, as well as quantitative data from 100 Federal and 100 private sector cybersecurity decision-makers.

The combined report explores:

- Prioritization and perceptions of AI for cybersecurity
- Early use cases and results
- Optimal workload for humans and AI
- Current governance and guardrails
- Remaining roadblocks
- Recommendations for embracing AI while mitigating risks

For this research, **AI** refers to applying advanced analysis and logic-based techniques, including ML, to interpret events, support and automate decisions, and take actions.

Executive Summary

Early AI efforts are strengthening cyber defenses:

While just **one in three** cybersecurity leaders **(31%)** say their organization is using AI for cyber today, another **50%** are actively working toward adoption

The majority of those implementing or utilizing AI **(54%)** say they've accelerated incident response times. Another **52%** successfully detected a vulnerability and **50%** proactively responded to a threat

80%

80% of all cyber leaders say **accelerating AI adoption** is critical to their organization's resilience against evolving threats

---

Cyber leaders say the future is collaborative:

86%

86% of cyber leaders feel human-AI collaboration will become the cornerstone of effective cybersecurity strategies

When it comes to their **ideal division of responsibilities**, cyber leaders want humans to keep majority ownership of strategic planning, innovation, and governance; and AI to take the lead on cyber risk assessments and threat detection and response

Autonomy, however, may still be years away – just **one in five** say they fully trust AI to automate cybersecurity decisions

---

Short-term goals focus on building AI knowledge, skillsets, and external partnerships:

Despite momentum, just **28%** of cyber leaders describe their organization's AI governance as robust. **Less than half** have documented policies for decision-making models or formal ethical or program testing guidelines, and just **40%** report policies specific to critical infrastructure

Additional barriers to progress include fears of increased attacks, lack of workforce skillsets, and data quality issues

Over the **next 12 months**, cyber leaders want their organizations to focus on researching additional AI use cases, expanding workforce education, and improving collaboration with external AI partners

The AI Imperative

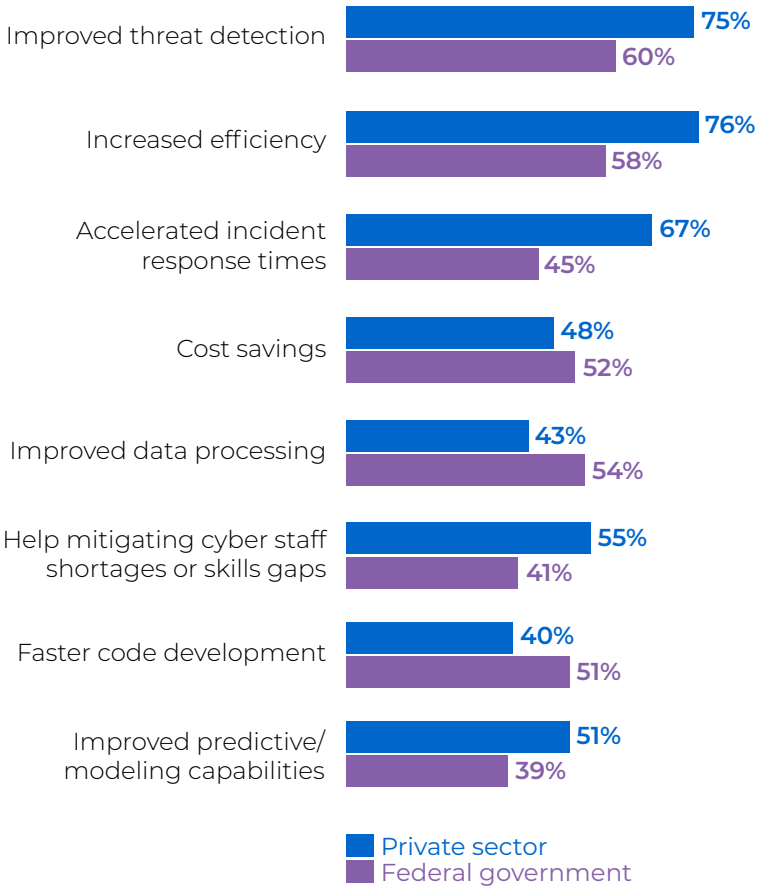
AI has the potential to revolutionize cybersecurity, supercharging defenses and transforming threat detection and response capabilities. While nearly **one in three** public and private sector cybersecurity professionals **(31%)** say their organization is using AI today, another **50%** are actively working toward adoption.

How would you describe your organization's adoption of AI for cybersecurity?

4%	15%	19%	31%	31%
Not considering	Discovering	Planning	Implementing	Utilizing

80% of cyber leaders say **accelerating AI adoption** is **critical** to their organization's resilience against evolving threats

What benefits do you see for incorporating AI into cybersecurity practices?[1]



> "With any organization [you only] have a certain amount of resources … so anything we can do with AI to **improve our ability to deliver on our mission** – either by doing it better, faster, or being able to scale more to meet the need – those are the areas we're looking at."
>
> – Public sector cyber leader

[1] Respondents asked to select all that apply

Proven Applications and Early Wins

Cybersecurity leaders implementing or utilizing at least one AI solution for cybersecurity **confirm improvements** in incident response times, vulnerability detection, and risk mitigation.

Those implementing or utilizing AI for cybersecurity: What has been your most effective application to date?

"Using **behavioral analytics** to find compromised accounts and insider threats."
– Public sector cyber leader

"**Threat detection**. It's been extremely helpful in reducing false readings and quickly catching errors that need to be handled immediately."
– Public sector cyber leader

"**Generative AI**. The ability to grab code without being an expert in syntax has reduced our time to implementation."
– Private sector cyber leader

"Systems for **analyzing network traffic** that use AI to find anomalies and intrusions."
– Public sector cyber leader

"**Firewall systems** powered by AI that modify rules in response to current threat information."
– Public sector cyber leader

"AI for **endpoint protection** using real time threat intelligence."
– Private sector cyber leader

"Building cybersecurity controls that run in **milliseconds** – based on pattern matching and deviation scores – is well within our thresholds and our capabilities."

– Public sector cyber leader

Initial achievements:[2]


Accelerated incident response times
54%


Successfully detected a vulnerability
52%


Improved cyber risk prioritization and mitigation
52%


Gained information on the threat landscape
50%


Proactively responded to a threat
50%


Boosted operational efficiency
44%


Accelerated code development and/or review times
41%

[2] According to those implementing or utilizing at least one AI solution for cybersecurity

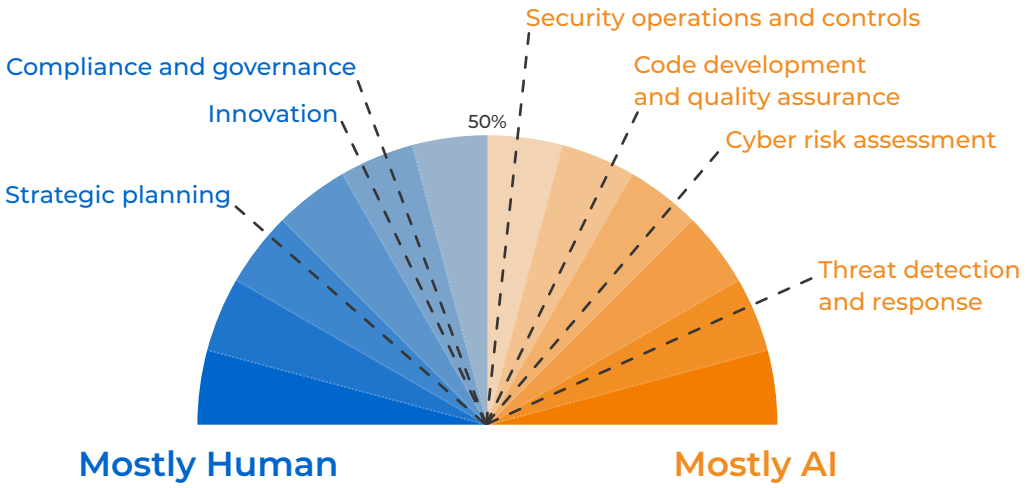
The Case for Collective Intelligence

The consensus is clear – public and private sector cybersecurity professionals see **human-AI teaming** as the future of effective cyber operations.

86% agree that human-AI collaboration will become the **cornerstone** of effective cybersecurity strategies.

However, fewer are comfortable giving up full control. **While two thirds (67%)** agree that they trust AI to automate cybersecurity decisions, just **21%** strongly agree.

As AI advances within cybersecurity, what do you see as the ideal division of work between cyber professionals and AI?

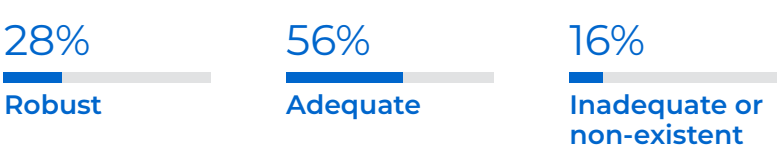


> Divide the labor into who's better at doing what: Big math problems – that's probably going to be computers. When you get into these more **complex, nuanced conversations** and strategic plans – that's probably going to be the humans."
>
> – Private sector cyber leader

Governance and Guardrails

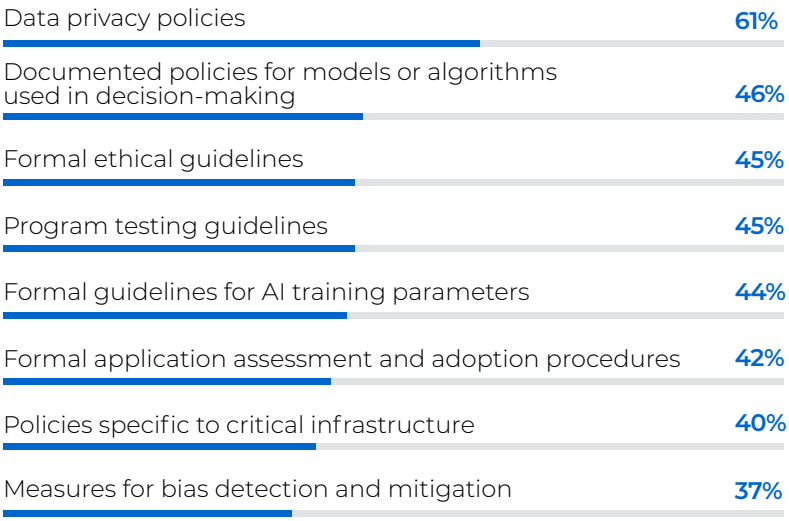
While most organizations view their current AI governance as adequate, **critical policy gaps exist** – especially for smaller organizations – raising the risk of unintended consequences from AI applications. Less than half of organizations planning, implementing, or using AI have documented policies for decision-making models or formal ethical or program testing guidelines. Just **40%** report policies specific to critical infrastructure.

Those planning, implementing, or using AI: How would you describe your organization's AI governance (including policies, processes, and best practices for managing cyber AI systems)?[3]



Smaller organizations[4] are significantly more likely to say their governance is inadequate or non-existent **(40% to 12%)**

What specific measures or policies, if any, does your organization have in place to govern the use of AI (including generative AI) in your cybersecurity practices?[3]



51% of private sector leaders and **77%** of Federal leaders feel government AI regulations are **generally good** for the United States' cybersecurity posture

> "Cybersecurity practitioners have come a **long way** in integrating their skills, their capabilities, and their contributions into organizations, and AI practitioners are sort of at the beginning of this. So, there's an opportunity for cybersecurity to show [AI practitioners] a model of how you integrate into the organization, how you talk to other parts of the business, how you mature your governance, oversight, and risk management – because we've been through it over the last 20 years."
>
> – Public sector cyber leader

[3] Those planning for, implementing, or using AI
[4] Organization with fewer than 500 employees

Remaining Roadblocks

Despite momentum, **nine out of ten** cybersecurity leaders are experiencing challenges that impact their organization's ability to adopt AI. While top challenges vary, cyber leaders agree fears of increased attacks, limited workforce skills, and data quality issues are the most prevalent.

What challenges, if any, are having the biggest impact on your organization's adoption of AI for cybersecurity?[5]

#1 Fears of increased attacks on new AI models, data, or services

> We have to teach our CEOs and CIOs to change their language. Instead of saying, 'Is it ready yet?' or 'Is it running?' ... the question needs to be, '**Is it resilient?**'"
>
> – Private sector cyber leader

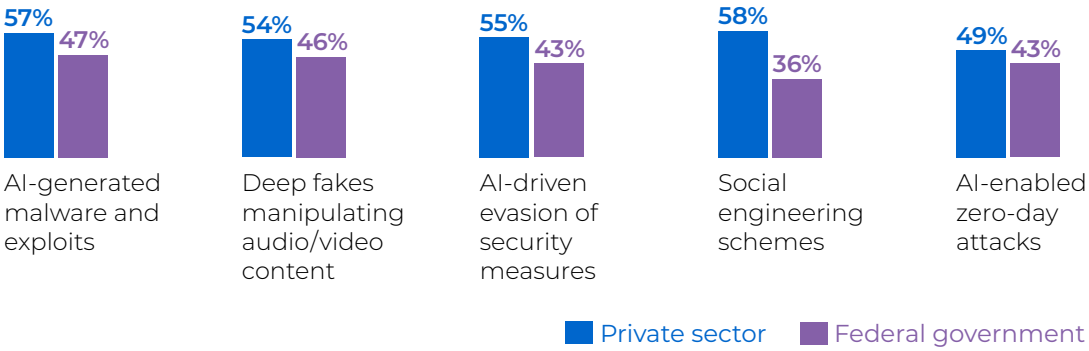
#2 Lack of skilled workforce to implement

> The number of people that are skilled in both cybersecurity and machine learning is **extremely small** right now."
>
> – Private sector cyber leader

#3 Data quality, integrity, or availability challenges

> Never fully trust the data lakes you are getting information from; always complete a **thorough review** process."
>
> – Private sector cyber leader

Which of the following AI-driven attack strategies do you think pose the greatest threats to your organization?[5]



[5] Respondents asked to select up to five

Taking the Next Step

Looking ahead, **few cybersecurity leaders feel well-prepared** to address new AI-driven threats. To expand their cyber AI capabilities, leaders recommend improving their understanding of cyber AI use cases, expanding their workforce's AI education and training, and improving their collaboration with external AI security experts and partners.

Looking ahead, how prepared is your organization to combat AI-driven cybersecurity threats?

4%	25%	38%	30%	3%
Not at all prepared	Slightly prepared	Somewhat prepared	Well prepared	Unsure

In the next 12 months, what steps would you like to see your organization take to advance its cyber AI capabilities?[1]

Research additional AI use cases	55%
Expand workforce education and training	48%
Improve collaboration with external AI security experts and partners	48%
Improve communication on AI usage and limitations	45%
Develop or expand ethical guidelines and governance frameworks	43%
Develop or expand cross-functional AI teams	40%

> We have to figure out a way to put **governance and containment** around the use of this disruptive technology, but at the same time support innovation. Innovation is 'implementation, failure, adjustment,' … and the faster we do that, the more innovative we can be."
>
> – Private sector cyber leader

> It's understanding the platforms themselves and that whole digital supply chain … We talked about software bill of materials (SBOMs), then cloud BOMs, now it's going to be **AI BOMs** – talking about what AI models make up your systems. That's something that we should really understand more."
>
> – Private sector cyber leader

> I really believe in building security in and **secure by design** … We need to start putting all that wonderful security goodness that we brought into the development lifecycle as DevSecOps and have a similar approach with MLSecOps."
>
> – Private sector cyber leader

[1] Respondents asked to select all that apply

Future Perspectives

When asked to envision the future of human-AI collaboration, cyber professionals relayed a **mix of optimism and caution**. While many see immense potential for innovation, efficiency, and improved security, concerns around safety, ethics, and responsible development remain.

When you think about the future of human-AI collaboration for cybersecurity, what ONE word comes to mind?

Responsible Use; Realistic Expectations

What is **one piece of advice** you would give fellow cybersecurity professionals on embracing the benefits of AI for cybersecurity while managing risks?

"We have a very important, upfront role to play here to make sure that we're deploying ML capabilities and the ML pipeline in a way that we're not going to come to regret. That means **knowing the right questions to ask**. What are the permissions? How are we maintaining system boundaries?"

– Public sector cyber leader

"Read the **NIST AI Risk Management Framework**; it's just a fantastic foundational piece."

– Private sector cyber leader

"**Start with principles** … [for example], 'we will never deploy the output of a generative AI LLM without a human checking it' … Policies take a little bit longer to create and are a little bit more prescriptive, and controls morph from the enforcement policies."

– Private sector cyber leader

"**Invest in your team's upskilling** and training so they can use AI tools and technology efficiently."

– Public sector cyber leader

"Be open-minded and try to find your use case. There are many different ideas and small models that you can use almost right away … **Don't be afraid to break a few things** at this stage rather than waiting for the perfect solution."

– Private sector cyber leader

"Look for **force-multiplier opportunities**, both to your attacker, but also to your defense. Counter one with the other."

– Private sector cyber leader

"Aim for human-AI cooperation. **AI complements human knowledge**, not the other way around. Make use of their combined abilities."

– Public sector cyber leader

"It is irresponsible to blindly trust AI solutions with inflated expectations, and **AI is not the best solution for everything** at this time. We are prioritizing use cases by business value and feasibility/maturity. "

– Private sector cyber leader

"For things that are **highly predictable**, don't have a lot of complexity, and are of great benefit – those are the kinds of tasks that we want to look at automating."

– Private sector cyber leader

"As great as it is, AI is still a program. It never will totally replace human judgment and innovation. But it is a **great tool** to assist us in doing our jobs better."

– Private sector cyber leader

Recommendations

The following recommendations build on key insight from the qualitative interviews and quantitative survey responses. To optimize AI's cybersecurity impact, organizations should:

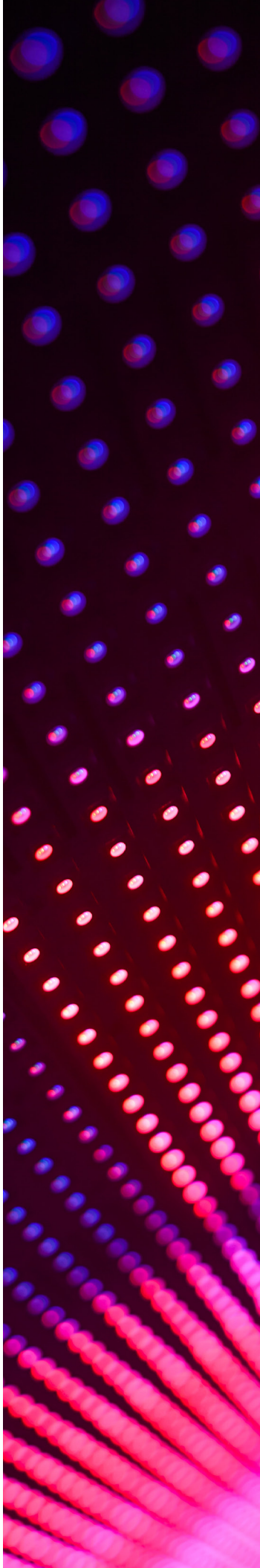
- **Start with increased human communication and collaboration:** In periods of rapid change, internal communication is paramount. Start with an AI Cyber Council to collect and disperse information on potential applications, best practices, and lessons learned. Establish interdisciplinary teams that blend AI/ML expertise with traditional cybersecurity knowledge, to bridge knowledge gaps, foster a shared language, and design core AI principles that can evolve into policies and controls. Build trust and understanding with regularly scheduled meetings on AI governance and successful integrations throughout the organization.

- **Emphasize a culture of continuous learning:** Staying abreast of the latest AI development, tools, and techniques is a constant challenge. Look for specialized training programs or certifications to offer your team. Follow cyber AI thought leaders on social media. Encourage participation in conferences, webinars, and workshops. Set the expectation that no one is an expert and constant practice, curiosity, and experimentation is the fastest way forward.

- **Evaluate AI use cases by tech maturity, mission value, and risk:** When considering new AI solutions, prioritize applications with low risks and high rewards. Start with the stability of the technology – are there mature and reliable solutions available? Next, consider factors like mission enablement, data preparedness, system integration capabilities, and the availability of skilled personnel. Finally, conduct comprehensive risk assessments to identify and mitigate potential vulnerabilities and ensure the solution aligns with your organization's overall risk management strategy.

- **Build in AI security from inception:** To minimize cyber threats, AI systems themselves must be secure by design. This involves implementing robust data protection measures, secure coding practices, regular vulnerability assessments, and threat modeling throughout the AI development lifecycle. Pay special attention to the supply chain – understanding what models you are using and where. Incorporating security by design principles can help prevent exploitation by malicious actors and ensure the integrity of AI-driven processes.

- **Be realistic about expectations:** While AI offers transformative potential for cybersecurity, it is crucial to maintain realistic expectations about its capabilities and limitations. AI systems excel at processing large volumes of data and identifying patterns that may elude human analysts, but they are not infallible and can be susceptible to biases and errors. It's important to view AI as a complementary tool that augments human expertise, rather than a singular answer for all cybersecurity challenges.



- **Focus on thorough testing and evaluations:** As you expand AI solutions in your cybersecurity operations, it is vital to perform thorough testing and evaluations. Conduct regular performance reviews, stimulate real-world attack scenarios, run penetration tests, and fine-tune algorithms to improve their accuracy and effectiveness over time. Involve diverse stakeholders in the testing process (including security professionals and data scientists) and share lessons learned throughout the organization.

- **Embrace change:** The evolution of AI in cybersecurity will bring about a significant shift in how organizations categorize, identify, and mitigate threats. Embracing this change requires an open-minded approach and a willingness to experiment with new technologies and methodologies. Encourage innovation and creative problem-solving within your team, allowing them to learn from inevitable failures and rapidly iterate improvements.

Methodology and Demographics

MeriTalk, in collaboration with RSA Conference™, compiled qualitative data from five in-depth interviews with senior cybersecurity leaders, as well as quantitative data from 100 Federal and 100 private sector cybersecurity decision-makers in January and February 2024. The quantitative research has a margin of error of ±6.93% at a 95% confidence level.

Organization type:

- **50%** Industry or private sector business
- **22%** Federal government – Civilian agency
- **28%** Federal government – DoD or Intelligence agency

Industries represented include IT, Finance, Healthcare, Manufacturing, and others

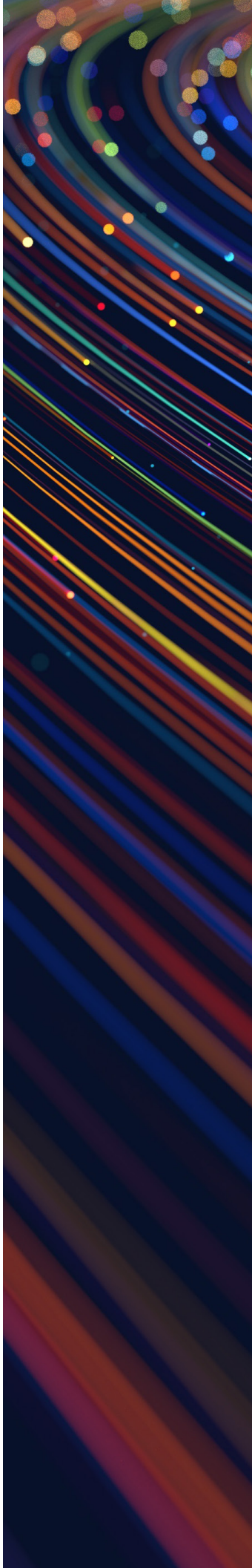
Organization size:

- **21%** Fewer than 500 employees
- **17%** 500-999 employees
- **32%** 1,000-4,999 employees
- **30%** 5,000 employees or more

Job title:

- **39%** C-suite (CIO, CTO, CISO, or other executive-level IT/IS decision-maker)
- **35%** Information Technology (IT), Information Security (IS), or Cybersecurity Director/Supervisor
- **9%** IT/IS or Cybersecurity Program Manager/Officer
- **6%** IT/IS or Cybersecurity Analyst/Engineer
- **4%** IT/IS or Cybersecurity Specialist
- **3%** Software/Applications Developer or Development Manager
- **2%** Data Center or Network Manager
- **2%** Other IT/IS or Cybersecurity Manager

100% of respondents make, contribute, or otherwise influence their organization's purchasing decisions for cybersecurity solutions



MeriTalk
Improving the Outcomes of Government IT

RSAConference™
Where the World Talks Security™

Underwritten by:

FORTINET FEDERAL