Gartner
Peer Insights™

The Future of Cybersecurity: Tools and Strategies

The cyberthreat landscape is becoming increasingly complex and attackers are eager to take advantage of any digital vulnerability. How are decision makers using emergent strategies and tools to maintain effective cybersecurity?

One-Minutes Insights:

- Leaders are researching new cybersecurity solutions every week through online communities and peer conversations
- Emerging technologies like SOAR, CNAPPs and mobile MFA are seen as promising solutions in network, cloud, and IAM security respectively
- Leaders are interested in new approaches to cybersecurity like zero trust and proactive security through AI
- Most want to see more innovation in cloud and endpoint security
- Leaders expect attacks to become more sophisticated but are optimistic that cybersecurity will adapt

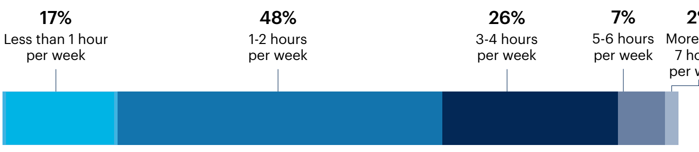
One-Minute Insights on timely topics are available to Gartner Peer Insights members. Sign up for access to over 100 more, and new insights each week.

Data collection: Feb 21 - Aug 18, 2022

Respondents: 300 IT/Eng/Infosec leaders

Most spend at least an hour a week researching emerging cybersecurity trends and technology, mainly through online communities and their peers

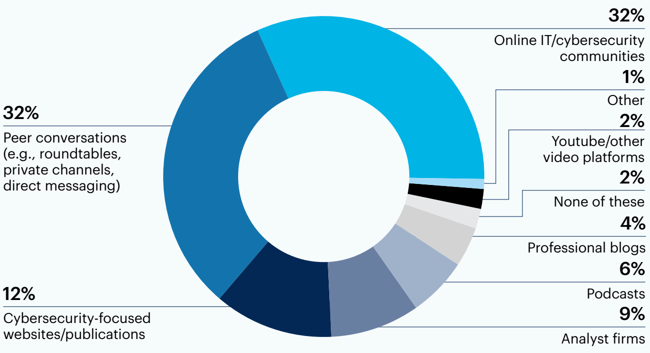
Most leaders (48%) spend **1-2 hours** each week **researching cybersecurity trends and emerging technologies**. About a **quarter (26%)** spend **3-4 hours** on this research each week.



How much time per week do you spend researching cybersecurity trends and emerging technologies?

n = 300

32% of respondents find **online IT and cybersecurity communities** the **most valuable** resource when conducting their research on cybersecurity trends and emerging technologies. Another **32%** identified **peer conversations** as their most valuable resource.



What is your most valuable resource for researching cybersecurity trends and emerging technologies?

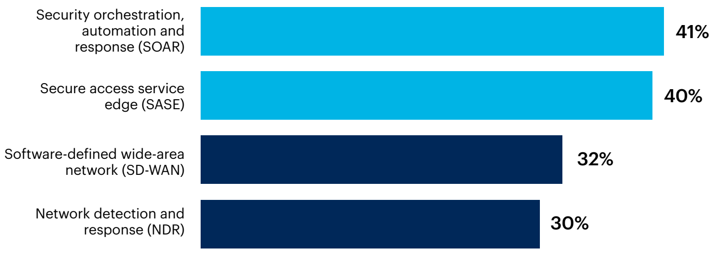
n = 300

> “[Cybersecurity] is getting more complicated.”
>
> -Director, finance industry, 10,000+ employees

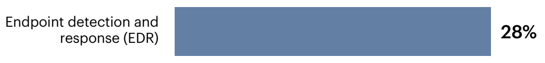
> “Cybersecurity is essential for any organization to survive tomorrow.”
>
> - C-suite, manufacturing industry, 10,000+ employees

Leaders are excited about a variety of emerging technologies in network security, cloud security and IAM

The **top three emerging network security tools** causing excitement among leaders include network **access control (41%), secure access service edge (40%)** and **software-defined wide-area network (32%).**



What emerging network security tools are you most excited about?

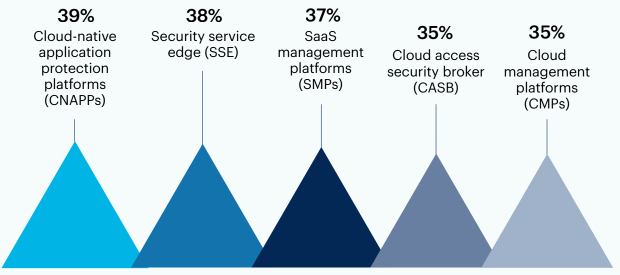


User and entity behavior analytics (UEBA) **24%**, Intrusions prevention system (IPS) **23%**, Network access control (NAC) **21%**, Remote browser isolation (RBI) **19%**, Zero trust network access (ZTNA) **19%**, Extended detection and response (XDR) **15%**, Desktop as a service (DaaS) **6%**, None of these **2%**, Other **1%**

n = 300

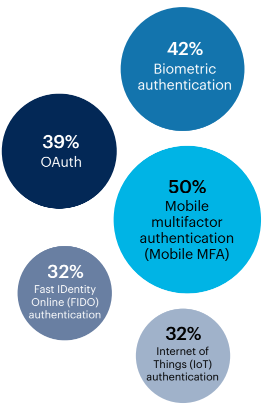
In the area of **emerging cloud security tools**, most leaders are excited about **cloud-native application protection platforms (39%), security service edge (38%)** and **SaaS management platforms (37%).**

What emerging cloud security tools are you most excited about?



Cloud data protection gateways (CDPGs) **31%**, Cloud security posture management (CSPM) **24%**, None of these **7%**, Other **0%**

n = 300



Half of respondents (50%) identified **mobile multifactor authentication** as one of the emerging identity and access management tools they are most excited about. Many are also interested in **biometric authentication (42%)** and **OAuth (39%).**

What emerging identity and access management (IAM) tools are you most excited about?

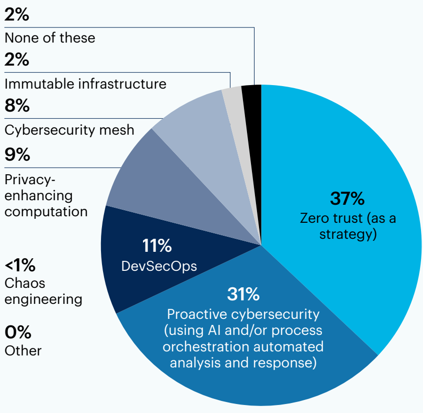
Decentralized identity **26%**, Cloud infrastructure entitlement management (CIEM) **24%**, Zero-knowledge proofs (ZKPs) **14%**, None of these **3%**, Other **0%**

n = 300

> "There are several interesting cybersecurity technologies I'm interested in."
>
> - C-suite, finance industry, 5,000 - 10,000 employees

> "[Cybersecurity is] moving from infancy to the awkward teenage years where we will see a lot of consolidation in the industry, fallout, and unexpected new solutions."
>
> - C-suite, healthcare industry, 1,000 - 5,000 employees

Emerging cybersecurity approaches like zero trust cause excitement, but cloud security and endpoint security need innovation



Leaders are most excited about **emerging cybersecurity approaches like zero trust (37%)** and **proactive cybersecurity (31%).**

Which emerging approach to cybersecurity do you find most exciting?

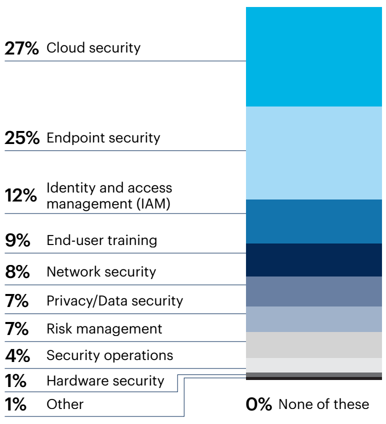
n = 300

27%

of respondents believe that **cloud security** is the area of cybersecurity in most need of innovation, while **25%** point to **endpoint security**.

Which area of cybersecurity is most in need of innovation?

n = 300



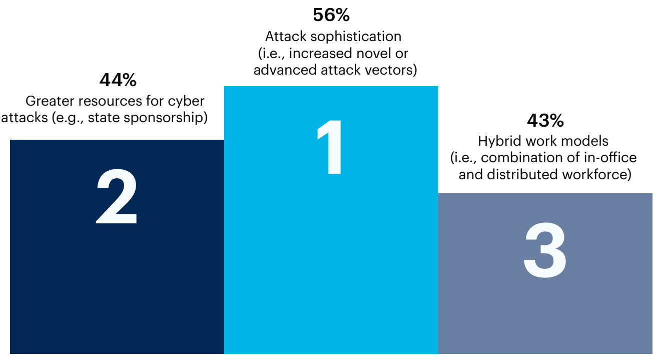
> "Zero Trust Network Architecture is a game changer and needs to be implemented across all enterprises."
>
> - Director, finance industry, 5,000 - 10,000 employees

> "I believe AI and ML are important because users will continue to be the weakest link."
>
> - C-suite, other services industry, 10,000+ employees

In the future, cybersecurity will need to contend with increasingly resourced and sophisticated attacks, but most feel optimistic about its adaptability

The **top 3 identified challenges** for the future of cybersecurity include **attack sophistication (56%), greater resources for cyber attacks (44%)** and **hybrid work models (43%).**

What are the top challenges for the future of cybersecurity?

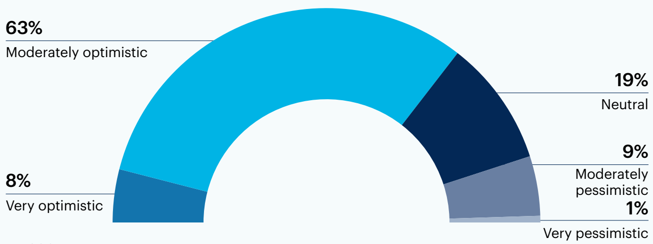


Blockchain technology (e.g., cryptocurrencies enabling anonymity/lack of traceability) **33%**, Hiring (i.e., lack of qualified personnel) **29%**, Increase in number of devices on the network (e.g., personal laptops, Internet of Things (IoT) devices) **17%**, End-user security hygiene (e.g., poor password or data management) **15%**, Talent management (e.g., skills development, talent retention) **15%**, Cybersecurity framework limitations (i.e., frameworks out of date) **14%**, Business support (i.e., cybersecurity still seen as an IT cost rather than a business continuity issue) **12%**, Executive burnout (e.g., CISOs leaving the workforce due to stress) 10%, Lack of business skills in security leadership (e.g., inability to "sell" cybersecurity to the business) 9%, Punitive government measures (e.g., fines for cybersecurity breaches) **5%**, None of these **<1%**, Other **0%**

n = 300

Most leaders (71%) are **optimistic** that cybersecurity will be able to adapt and protect against future threats.

Do you feel optimistic or pessimistic about the ability of cybersecurity to adapt to and protect against future threats?



n = 300

> "[Cybersecurity] is going to be a challenge well into the future."
>
> - VP, healthcare industry, 10,000+ employees

> "End-user cybersecurity training is still lacking but important as ever. I believe that there is an increase in attack reports due to ignorance and callous computing practices. Also, the law just has not been effective in indicting nation-state sponsors of attackers. The international governments and community have to do more to deter cyber-criminals."
>
> - Director, education industry, 5,000 - 10,000 employees

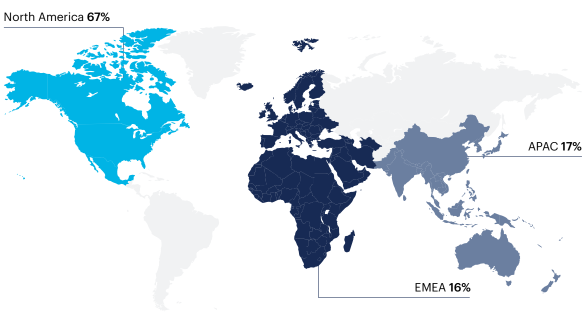
> "The future of cybersecurity will be reliant on the training of future security analysts and the passing of information from our veterans."
>
> - Director, education industry, 1,000 - 5,000 employees

Want more insights like this from IT leaders like you?

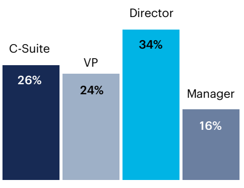
Click here to explore the revamped, retooled and reimagined Gartner Peer Insights. You'll get unprecedented access to verified reviews, synthesized insights and engaging discussions from a community of your peers.

Respondent Breakdown

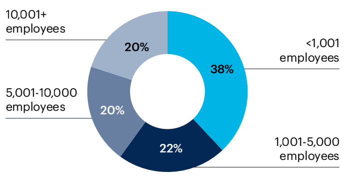
Region



Title



Company Size



This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Source: Gartner Peer Insights, The Future of Cybersecurity: Tools and Strategies survey

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved.