Gartner

Top 9 Trends in Cybersecurity for 2024

Optimizing for Resilience

Disclaimer: The trends are not ranked in order of importance.

1. Continuous Threat Exposure Management (CTEM)

Organizational attack surfaces have expanded enormously in recent years. This growth has been driven notably by accelerated adoption of SaaS, expanding digital supply chains, increased corporate presence on social media, custom application development, remote working and internet-based customer interaction.

2. Extending IAM's Cybersecurity Value

Identity and access management's (IAM's) role in cybersecurity has been increasing steadily. As of 2023, IAM is the second-most-popular topic of discussion by security and risk management (SRM) leaders who use Gartner's client inquiry service.

3. Third-Party Cybersecurity Risk Management

The inevitability of third parties experiencing cybersecurity incidents is pressuring SRM leaders to focus more on resilience-oriented investments and move away from front-loaded due-diligence activities.

4. Privacy-Driven Application and Data Decoupling

Multinational companies that have relied on single-tenant applications for decades face rising compliance demands and business disruption risks. This is due to increasing nationalistic privacy and data protection and localization requirements that result in enforced fragmentation of enterprise application architectures and data localization practices.

Optimizing for Performance

5. Generative AI

SRM leaders can improve the security function's reputation and performance by using generative AI (GenAI) in proactive collaboration with business stakeholders. This will help lay the foundations for ethical, safe and secure use of this disruptive technology.

6. Security Behavior and Culture Programs

Security behavior and culture programs (SBCPs) encapsulate an enterprisewide approach to minimizing cybersecurity incidents associated with employee behavior. Increased focus on the human elements of SBCPs continues to show promise in the mission to minimize the impact of employees' unsecure behavior.

7. Cybersecurity Outcome-Driven Metrics

Cybersecurity outcome-driven metrics (ODMs) are operational metrics with special properties — that enable cybersecurity's stakeholders to draw a straight line between cybersecurity investment and the delivered protection levels that investment generates.

8. Evolving Cybersecurity Operating Models

The acquisition, creation and delivery of technology continues to move from central IT functions to lines of business. This breaks traditional cybersecurity operating models. SRM leaders are adapting their operating models to meet their business needs.

9. Cybersecurity Reskilling

The skills that cybersecurity teams need are changing drastically, yet cybersecurity leaders continue to hire for legacy roles and skills. SRM leaders must reskill their teams by retraining existing talent and hiring new talent with new profiles.

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

eBook

2024 Leadership Vision for Security and Risk Management Leaders

Uncover the top 3 strategic priorities for 2024.

Download Now

Webinar

The Gartner Emerging Technologies and Trends in Security for 2024

Identify the emerging technologies set to revolutionize the security landscape.

Watch Now

How We Help

How Gartner Works With CISOs

Find out how we provide the insight, guidance and tools needed to deliver on your mission-critical priorities.

Learn More

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

Already a client?
Get access to even more resources in your client portal. Log In

Learn more about Gartner for Cybersecurity Leaders | Follow Us on LinkedIn | Become a Client

Source: Gartner