Bitdefender

Cybersecurity Assessment Report

2024

Bitdefender

Summary

This year's cybersecurity landscape continues to evolve, with cloud technologies and AI becoming increasingly central to corporate infrastructure and the threats they face. As these technologies drastically accelerate, the complexity of managing and securing them has intensified.

This year's research focuses on the prevalence of cloud adoption and organizations' significant concerns regarding protecting this infrastructure. A staggering number of enterprises are grappling with how to defend against sophisticated threats that now include AI-driven tactics, which pose new challenges and risks.

Moreover, the financial stakes of cybersecurity breaches remain high, with the costs associated with data breaches continuing to climb. Organizations cannot afford to falter on security and need solutions that effectively prevent problems before they escalate to a breach.

As we delve deeper into integrating AI into cybersecurity strategies, we raise a crucial question: are organizations truly prepared to face a growing attack surface that is increasingly dominated by intelligent, adaptive threats?

To help answer this, Bitdefender commissioned Censuswide, a third-party research firm, to survey 1,200 IT professionals ranging in title from IT managers to CISOs in various industry sectors who work in organizations with 1,000+ employees. The survey and analysis took place from March 2024 through May 2024. The respondents were geographically split equally between France, Germany, Italy, Singapore, U.K. and the U.S.

IAM and maintaining compliance are the leading security concerns when managing cloud environments.

96%
of respondents are concerned about AI's impact on the threat landscape.

64%
of respondents are planning on looking for a new job in the next 12 months.

57%
More than half of organizations experienced a data breach or leak in the last 12 months (up 6% from previous year).

Bitdefender

2024 Cybersecurity Forecast: Navigating New Frontiers

Managing cloud infrastructure is becoming increasingly complex and challenging. Today's businesses have embraced the cloud, with environments sprawling across multiple cloud and hybrid platforms. By adopting the cloud, they have realized enormous gains in efficiency and agility, but at a cost. Their attack surfaces have expanded dramatically, creating more areas to manage and protect.

While the core cloud platforms of AWS, Azure, and Google Cloud behave somewhat similarly, no two are identical. They all come with differences in configuration and operations, making identity and access management (IAM), data security, network configurations, and compliance a unique challenge. Any setup or operations failures may have wide-reaching consequences, exposing sensitive data and infrastructure to attackers.

A shortage of qualified cloud cybersecurity talent makes this all the more challenging. Many IT professionals may possess deep expertise in one specific cloud platform, such as Azure, yet find themselves less familiar with others, like Google Cloud or AWS. This skill disparity can lead to gaps in an organization's overall cloud security posture.

Organizations want to "use the cloud with confidence" but are concerned about security challenges offsetting the benefits they get from the cloud. This survey was conducted to help organizations understand the different security pain points felt across the industry. By understanding the vulnerabilities and risks associated with cloud infrastructure, we aim to equip our readers with the knowledge and strategies to navigate these challenges effectively.

Question

What types of threats, if any, are you most concerned about?

Respondents selected up to three of their top choices.