netwrix

2024

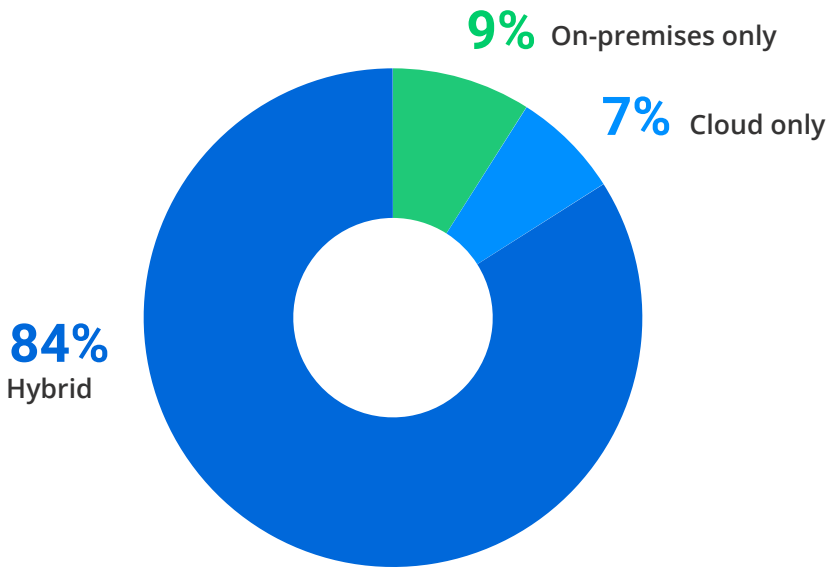
Hybrid Security Trends Report

Additional Findings for the Enterprise Sector

CLOUD ADOPTION

Enterprises (over 1,000 employees) are moving to the cloud faster than smaller organizations. While on average, 74% of respondents say they have a hybrid infrastructure, this number is higher for the enterprise sector (84%). Subsequently, only 9% of large organizations are on premises only compared to 15% for the market average.

IT Architecture: Enterprises



IT PRIORITIES

The two main IT priorities are the same for organizations of all sizes: data security and network security. Automation of manual IT processes ranked third for the enterprise sector–almost half (49%) of respondents named it among their top priorities for 2024 compared to just fifth place for respondents overall.

Top IT priorities for the enterprise sector

Fully automated security solutions are often seen as a desirable goal. But what if that automation becomes compromised? Enterprises have to include these considerations in their risk management programs. While automation-related risks may require new mitigations, current controls like just-in-time access or access review process in place can help address these new risks.

Ilia Sotnikov

Security Strategist at Netwrix

For the IT and security departments, automation can offer benefits for a full range of tasks. First, it can help establish self-service for users without jeopardizing security, such as when users are granted local admin rights for their endpoints. Next, IT teams can seek to increase the automation of cloud and container management and improve log event analysis so that responses to detected incidents can be automated.

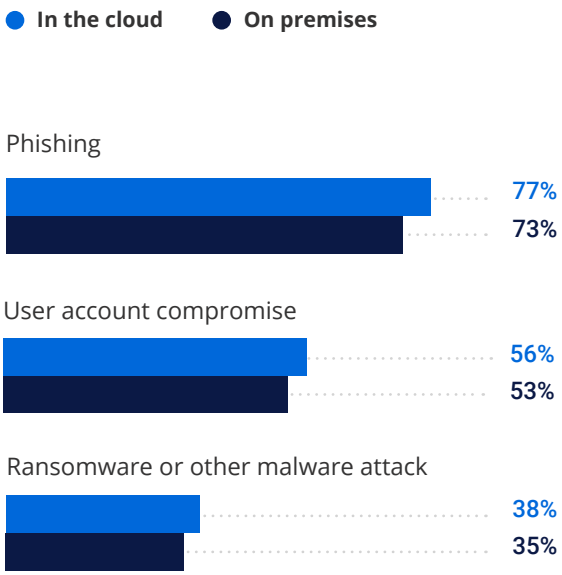
Dirk Schrader

VP of Security Research at Netwrix

SECURITY INCIDENTS

84% of organizations in the enterprise sector spotted a cyberattack within the last 12 months, compared to only 65% in 2023. Moreover, this rate is higher than the results among companies of all sizes in 2024: 79% of respondents say they detected an attack in their IT infrastructure.

Most common security incidents in the enterprise sector



The surge in the attack rates across organizations of all sizes, including the enterprise sector, may indicate that threat actors found AI automation extremely beneficial. With the introduction of AI, sending a massive number of phishing emails and probing systems and services for vulnerabilities is only a matter of orchestration on those platforms operated by cybercriminals. Constant pressure stresses the security teams and might lead to reduced and worn-out protection levels. To ease this burden, organizations should consider involving third-party investigators as a part of their incident response plan. It will help offload the internal security team when dealing with an ongoing attack.

Dirk Schrader

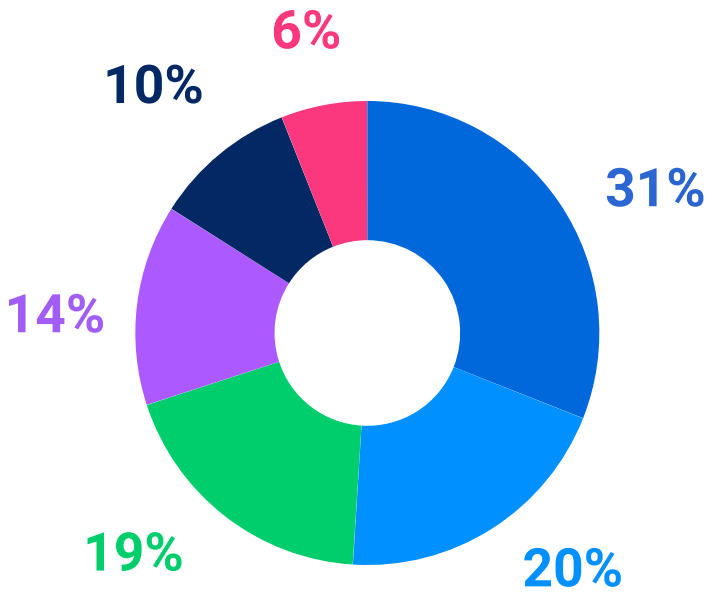
VP of Security Research at Netwrix

COST OF CYBERATTACKS

For 53% of large organizations, a cyberattack resulted in additional unexpected expenses to fix security gaps, compared to 45% among organizations overall. Each fifth enterprise faced compliance fines (22%) and a reduced competitive edge (21%). Moreover, 30% of enterprises estimated their financial damage from cyber threats to be at least $50,000, compared to just 17% among organizations overall.

Estimated financial damage due to cyber threats for large enterprises

- 0$
- $1 – $10,000
- $10,001 – $50,000
- $50,001 – $200,000
- $50,001 – $200,000
- $500,001 or more

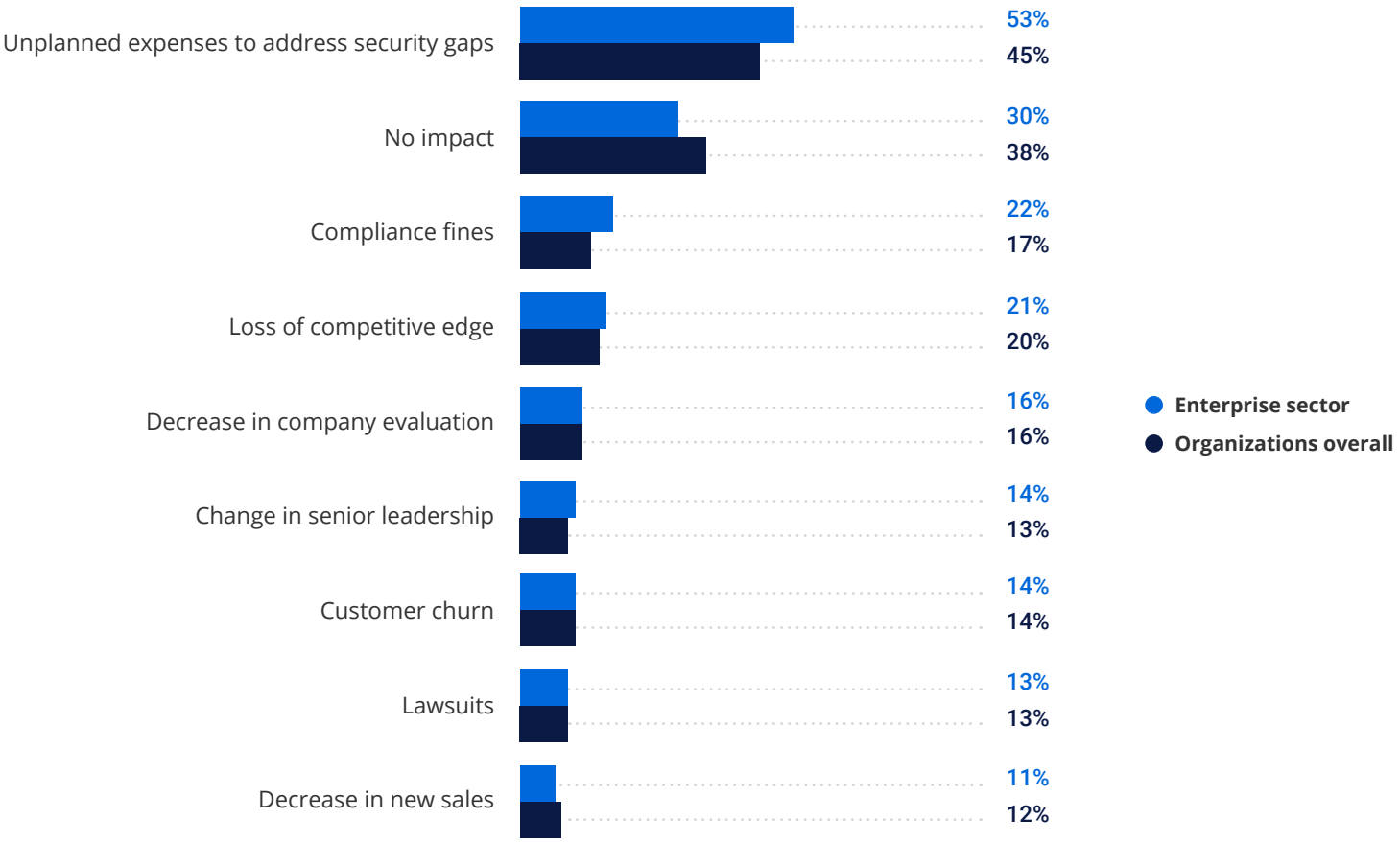


Mature security teams do not solely rely on preventative controls. They are investing in detection and remediation solutions as part of the defense-in-depth strategy, contributing to the growth in incident reports. Moreover, both the industry and the governments' expectations about security transparency are changing, increasing visibility into the real scale of the problem.

Ilia Sotnikov

Security Strategist at Netwrix

Cyberattack consequences for large enterprises



Typically, large enterprises have already implemented the basic security controls and thus must address more complex and costly issues in the aftermath of an attack. Where a smaller organization may have a quick fix available and can accept certain risks, enterprises must invest in the security team, process changes, and tooling to close even the smallest gaps exploited by the attacker.

Ilia Sotnikov

Security Strategist at Netwrix

ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover important changes and trends. For more reports, please visit www.netwrix.com/research

ABOUT NETWRIX

Netwrix champions cybersecurity to ensure a brighter digital future for any organization. Netwrix's innovative solutions safeguard data, identities, and infrastructure reducing both the risk and impact of a breach for more than 13,500 organizations across 100+ countries. Netwrix empowers security professionals to face digital threats with confidence by enabling them to identify and protect sensitive data as well as to detect, respond to, and recover from attacks.

For more information, visit www.netwrix.com

Corporate Headquarters:
6160 Warren Parkway, Suite 100, Frisco, TX, US 75034
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

www.netwrix.com/social