# Using more complex IT security strategies does not necessarily increase security, survey finds

*Hornetsecurity's survey reveals that organizations activated more M365 security features as they were increasingly targeted by cyber attacks in the last year.*

Overall, the survey results indicate that while the use of additional security features is essential, it is more practical to use tried and tested, user-friendly solutions - preferably executed by dedicated security professionals.

LONDON, UNITED KINGDOM, June 21, 2022 /EINPresswire.com/ -- A global IT security and compliance survey of 800+ IT professionals found that the rate of IT security incidents increases the more Microsoft 365 security features are used. Organizations using Microsoft 365 and that use 1 or 2 of its stock security features reported attacks 24.4% and 28.2% of the time respectively, while those that use 6 or 7 features reported attacks 55.6% and 40.8% of the time respectively. Overall, it was found that 3 in 10 organizations (29.2%) using Microsoft 365 reported a known security incident in the last 12 months.

Overall, the survey results indicate that while the use of additional security features is essential, it is more practical to use tried and tested, user-friendly solutions - preferably executed by dedicated security professionals.

What do IT security professionals say?

Experts at Hornetsecurity, a leading security and backup solution provider for Microsoft 365, say that this could be due to a number of factors. They point to the likelihood that organizations with a high number of implemented security features have done so as a result of sustained cyber attacks over a period of time, in an attempt to mitigate security threats.

They also suggest that the more security features that IT teams attempt to implement, the more complex the security system becomes. Features may be misconfigured, leaving vulnerabilities.

This is corroborated by the fact that 62.6% of respondents indicated that the main roadblock to implementing security features within their organization is 'not enough time or resources'.

Another theory is that making use of more features may contribute to a false sense of security within the organization. This could lead it to stop paying close attention to potential security threats, believing that all these features will keep them safe without having to make additional active effort.

"It's a game of cat and mouse. As you grow, you add security features, but you also become more susceptible to attack because you are a more lucrative target. Yet, you have to stay ahead of the criminals trying to harm your organization. The results of our survey made clear that relying on stock security features for digital safety is insufficient," said Daniel Hofmann, CEO at Hornetsecurity. "Organizations must proactively find ways of identifying unseen vulnerabilities and should take a diligent, holistic approach to cybersecurity, rather than relying on what is available out of the box and only reacting once it is too late."

What are the roadblocks faced by IT Pros to implement security features in their organizations?

Surprisingly, a quarter of respondents (25.7%) that employ over 50 people and have compliance requirements neither employ a dedicated compliance officer nor a dedicated IT security officer. Several factors contribute to a lack of attention to IT security and compliance in medium to large organizations.

Nearly 2 in 3 IT professionals (62.6%) surveyed indicate that 'not enough time or resources' is the main roadblock to implementing security features within their organization. Following this, respondents cite a 'lack of budget' (44.6%), 'skilling issues and/or a lack of knowledge' (36.2%) and a 'lack of interest from management' (23.1%).

All of the above results indicate a general lack of urgency surrounding security within organizations. Only 2% of respondents indicated that they have no roadblocks with regards to security, and over half of respondents (55.5%) said that their organization does not have a change tracking and review process in place - a vital tool for the identification of security threats.

What are the most commonly used security features within organizations?

Of the 11 security features listed in the survey, 'spam filtration' was the most popular, with 84.4% of respondents reporting its use within their organization. 'Multi-factor authentication' (82.7% of respondents) follows closely behind. 'Web traffic filtration', 'permissions management', and 'IT security awareness training for users' are used by 68.8%, 66.4%, and 61.2% respectively.

The least common security measure was 'SIEM Solution', with only 14.1% of respondents implementing such a measure. However, 'SIEM Solutions' corresponded with the highest rate of

incidents at 42.1%, which corroborates the idea that more advanced security is needed as organizations become a bigger target.

About Hornetsecurity Group

Hornetsecurity is the leading security and backup solution provider for Microsoft 365. Its flagship product is the most extensive cloud security solution for Microsoft 365 on the market, providing robust, comprehensive, award-winning protection: Spam and virus filtering, protection against phishing and ransomware, legally compliant archiving and encryption, advanced threat protection, email continuity, signatures and disclaimers. It’s an all-in-one security package that even includes backup and recovery for all data in Microsoft 365 and users’ endpoints.

Hornetsecurity Inc. is based in Pittsburgh, PA with other North America offices in Washington D.C. and Montreal, Canada. Globally, Hornetsecurity operates in more than 30 countries through its international distribution network. Its premium services are used by approximately 50,000 customers including Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, and CLAAS.

Media enquiries

Please contact us on press@hornetsecurity.com.

Angelica Micallef Trigona
Hornetsecurity
press@hornetsecurity.com
Visit us on social media:
Facebook
Twitter
LinkedIn

---