

# What's in store for MSPs: Trends for 2023

DUBAI, UNITED ARAB EMIRATES, April 7, 2023 /EINPresswire.com/ -- Alžbeta Kovaľová and Márk Szabó, security writers at [ESET](#) discuss what happened in 2022 and what is to be expected for MSPs in 2023

2022 was a strong year for MSPs, but 2023 looks to be even stronger. ESET experts claim that the number one priority for MSPs in 2023 is cybersecurity, and they are here to talk about the trends and challenges awaiting MSPs this year.

Michal Jankech, ESET's VP of the SMB and MSP segment, together with Jake Moore, ESET's global security advisor, have no doubt that cybersecurity will remain a top priority. With SMBs being early adopters of technology, MSPs helping drive digital transformation, and cybercrime changing in response, all (legitimate) parties must work to respond to evolving cybersecurity threats.

2022 saw MSPs change their approach, with more internal risk assessment, beefing up their security with instant response policies. Since cyberattacks demand high-quality solutions, new economic factors need to be considered. Trends suggest more business email compromises, zero-day attacks, and supply chain attacks. And with more users being targeted than ever, human error unfortunately remains the biggest security threat.

"Likewise, the threat landscape is unpredictable, with threats always evolving and becoming more sophisticated," says Jankech. All new technology can be and will be misused by cybercriminals. New emerging threats are quite complex and often rely on the above-mentioned human factor; therefore, more methods to eliminate and minimize the chance of a compromise are required.

However, Moore provided a few tips MSPs can implement to improve their security:

1. Automatic patch processes: Often, attacks rely on human error, so eliminating the opportunity for error is the best bet. Plus, with automated updates, every security update is applied in a timely manner.



2. Shrink the attack surface: Nowadays businesses are moving to the cloud, with many more devices accessing business networks, hence practical ways to monitor them are required, such as a “single pane of glass” approach.
3. Enhance data protection: Make sure business data is as safe as possible across all data locations by adding an additional layer of protection, for example, multifactor authentication.
4. Do not fall to alert fatigue: People (including security admins) often get desensitized by tasks and responses, leading to missed or ignored alerts. A solution for small businesses is to employ an MSP who could focus on these challenges, with expertise in automated solutions. Similarly, MSP admins can suffer from alert fatigue...
5. Employee awareness: Social engineering is a very successful tactic, and making sure employees are aware of the threats and know how to act and report threats in case they face one brings the company one step closer to a cyber secure 2023.

What can ESET offer MSPs?

Overall, the number one thing any business can do to improve its protection is to opt for a trustworthy cybersecurity solution. ESET is here to provide that protection to all businesses, big or small.

“It is not just products and features; our partnership places the MSP at the center. It is the platform and portfolio of solutions; it is also the level of support we give, regardless of geography or language. Flexibility is there too, with zero commitment, daily billing, and monthly invoicing through a completely self-serviced platform MSP model with integrations. We are in it together. And all of those pieces enable what is at the core of any partnership, and that is trust,” says Jankech.

The ESET MSP Program puts a strong emphasis on balance to provide the most carefree cybersecurity experience possible. It offers integration, automation, a unified ecosystem, and flexibility. ESET uses a combination of long-standing experience with machine learning and AI-based technologies, ESET LiveGrid, and the human expertise of digital security leaders to deliver cutting-edge MSP solutions. ESET products are known for their small system footprint, which boosts energy efficiency and enables further optimization for a company. All of this fuels ESET PROTECT, the most powerful multi-layered platform in the world for preventing, detecting, and responding to cyber threats.

ESET PROTECT also has an integrated XDR module, providing enterprise-grade security and risk management tools, such as advanced threat hunting, incident response, and complete network visibility. Additionally, it makes it possible for the ESET PROTECT platform to provide the user total control over the response. This also includes ESET Inspect Cloud, which collects data in real time on endpoint devices. The data is matched against a set of rules to detect suspicious activities automatically and permits security professionals at MSPs to efficiently search for unusual and suspicious activities while also enabling accurate incident response, management, and reporting. ESET Inspect Cloud also provides Managed Detection and Response (MDR)—outsourced cybersecurity services protecting customers’ data and assets, even if a cyber

threat avoids detection by standard security solutions.

In combination, the customizable products provide formidable protection for business as well as a rich service offer for the clients.

Sanjeev Kant

Vistar Communications

+971 55 972 4623

[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/626631794>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.