# 43% of businesses don’t protect their full IoT suite

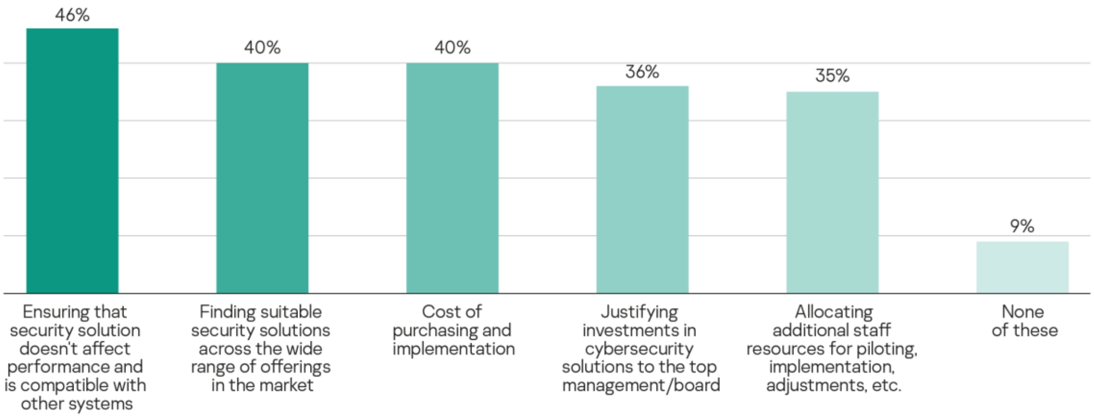
1 March 2022

**A recent Kaspersky report, “Pushing the limits: How to address specific cybersecurity demands and protect IoT”, revealed that in two-in-five businesses (43%), some parts of their IoT infrastructure are yet to have any protection. Meanwhile, the main barrier for implementation of many businesses’ IoT projects is the risk of cybersecurity breaches and data compromises.**

According to IoT Analytics, the global number of connected IoT devices is expected to grow 9%, reaching 27 billion IoT connections by 2025. With that dramatic rise in connected devices also comes an increased need for security. In fact, Gartner highlights that, in the past three years, nearly 20% of organizations have already observed cyberattacks on IoT devices in their network.

While two thirds of organizations (64%) globally use IoT solutions, 43% don’t protect them completely. This means that for some of their IoT projects – which may be anything from an EV charging station to connected medical equipment – businesses don’t use any protection tools.

The reasons behind this may be due to the great diversity of IoT devices and systems, which are not always compatible with security solutions. Almost half of businesses fear that cybersecurity products can affect the performance of IoT (46%) or that it can be too hard to find a suitable solution (40%). Other common issues businesses face when implementing cybersecurity tools are high costs (40%), being unable to justify investment to the board (36%) and lack of staff or specific IoT security expertise (35%).



Top issues with cybersecurity solutions organizations face

Furthermore, cybersecurity risks are seen by more than half of organizations (57%) as the main barrier to implementing IoT. This can occur when companies struggle to address cyber-risks at the design stage and then have to carefully weigh up all pros and cons before implementation.

“*Cybersecurity must be front and center for IoT. Managing risk is a major concern as life, limb and the environment are at stake. An IT error can be embarrassing and expensive; an IoT error can be fatal. But cybersecurity is only one part of making a system trustworthy. We also need physical security, privacy, resilience, reliability and safety. And these need to be reconciled: what can make a building secure, (locked doors for example), could make it unsafe if you cannot get out quickly,*” comments Stephen Mellor, Chief Technology Officer at Industry IoT Consortium.

“*IoT projects are very fragmented, loosely-coupled, domain-specific and integration-heavy in nature. In comparison, IT projects such as messaging/communication, analytics, CRM, etc., have around 80% of common requirements. In the case of IoT implementation, however, we have to deal with all kinds of legacy systems, physical constraints, domain protocols, multiple vendor solutions, etc., and maintain a reasonable balance in availability, scalability and security. In pursuit of higher availability and scalability, certain cloud infrastructure has to be leveraged, the system has to be open to some extent, then security becomes an enormous challenge*,” comments Eric Kao, Director, WISE-Edge+ of Advantech, a global vendor of industrial IoT solutions.

“*Despite all these challenges, IoT brings fantastic opportunities not just to businesses but to all of us, enabling comfortable living, transport, faster delivery and communications. IoT is widely used in smart cities (62%), retail (62%) and industry (60%). These include projects such as energy and water management, smart lighting, alarm systems, video surveillance and many more. Experts around the world are working on the task of effective protection for such projects but efforts should be made at every level – from equipment manufacturers and software developers to service providers and companies that implement and use these solutions,” adds* Andrey Suvorov, CEO at Adaptive Production Technology (Aprotech, Kaspersky’s subsidiary IIoT company).

To help organizations fill the gaps in their IoT security, Kaspersky suggests the following approaches:

- Assess the status of a device’s security before implementing it. Preferences should be given to devices with cybersecurity certificates and products from manufacturers who pay more attention to information security.
- Use a strict access policy, network segmentation and a zero-trust model. This will help minimize the spread of an attack and protect the most sensitive parts of the infrastructure.
- Adopt a vulnerability management program to regularly receive the most relevant data about vulnerabilities in programmable logic controllers (PLCs), equipment and firmware, and patch them or use any protection workarounds.
- Check the “IoT Security Maturity Model” – an approach that helps companies evaluate all steps and levels they need to pass to achieve a sufficient level of IoT protection.
- Use a dedicated IoT gateway that ensures the inbuilt security and reliability of data transferring from edge to business applications such as Kaspersky IoT Secure Gateway 100. It is Cyber Immune, which means almost no attack can affect the gateway’s functions.

The full report, “Pushing the limits: How to address specific cybersecurity demands and protect IoT”, is available to download here.

## About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky’s deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company’s comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.