Responding to your current and future IT security needs

A stage-by-stage cybersecurity approach

kaspersky

Building a security foundation for your organization by choosing the right product or service is just the first step. Developing a forward-thinking corporate cybersecurity strategy is key to long-term success.

Kaspersky's Enterprise Portfolio reflects the security demands of today's businesses, responding to the needs of organizations at different levels of maturity with a stage-by-stage approach. This approach combines different layers of protection against all types of cyberthreat to detect the most complex attacks, respond quickly and appropriately to any incident, and prevent future threats.

Threat types and the expertise required to counteract them

As IT environments grow in size and complexity, businesses face increasingly sophisticated threats that require them to constantly advance their cybersecurity expertise to enable effective defenses.

Our experience and continuous threat research allows us to divide all of the available threats into categories. The majority of the threats are at the bottom of the pyramid. These are generic threats that require only basic defensive mechanisms and IT security hygiene to be in place. If you move up the pyramid, you start seeing more advanced threats that evade preventive protection by using known Tactics, Techniques and Procedures (TTPs). Threat actors in this category, for example, could get hold of and reuse the more sophisticated tools that their better-resourced 'colleagues' have already developed. Most breaches are from this category. And, finally, at the very top there are complex APT-like threats and attacks that use unknown TTPs. Threat actors on this level have unlimited resources to develop highly sophisticated tools and methods with very specific targets in mind.

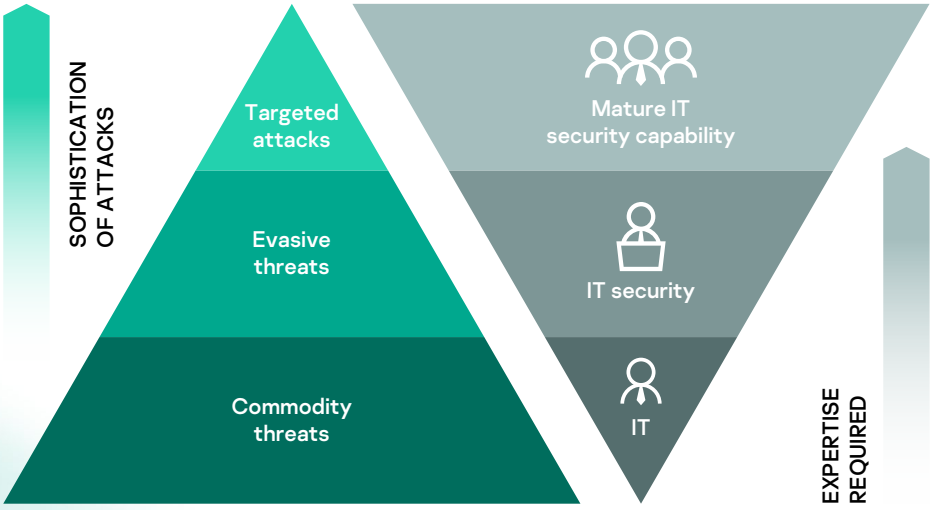

Figure 1. Threat types and the expertise required to counteract them

To drive successful business growth and maintain competitiveness, businesses continuously increase their reliance on information technologies. Ongoing digital transformation expands the potential attack surface through more and more interconnected systems. With IT environments growing in size and complexity, companies face the increasing sophistication of threats requiring them to continuously advance their cybersecurity expertise in order to enable effective defenses.

A stage-by-stage cybersecurity approach

In alignment with the threats and the varying degree of our customers' cybersecurity capabilities we've employed a strategy of going to market with our products and services to help organizations prevent 90% of threats automatically - and then systematically, and methodically empower them to add new and advanced capabilities to counter more sophisticated threats as their business develops.

Taking into account growth in the number and complexity of threats, IT security maturity, cybersecurity skills and existing budgets, there is a clear need to start building a comprehensive and adaptive security strategy.

At Stage 1 we provide all our leading preventive products along with premium support and professional services to ensure that customers extract maximum benefit from our technologies. At Stage 2 as you move up the pyramid there is a growing need to counter threats that circumvent existing preventive mechanisms. To support resource-conscious protection from advanced and evasive threats, we provide a cloud-enabled solution which complements the customer's own basic cybersecurity skills with managed detection, prioritization, and guided response, together with an automated toolset that helps security personnel to identify, analyze and respond to the more dangerous evasive threats more effectively. Organizations at Step 3 have higher chances of facing an actual APT and they need effective defenses against unknown TTPs. To fulfill the needs of mature IT security teams, Kaspersky delivers an innovative and balanced combination of technologies and services to address the challenges of today's most sophisticated threats and targeted attacks.

Kaspersky Managed Detection and Response enables an instantly matured IT security function without the need to invest in additional staff or expertise. At the same time it allows incident triage processes to be offloaded to Kaspersky, so that mature IT security teams can focus on responding to the critical outcomes delivered.

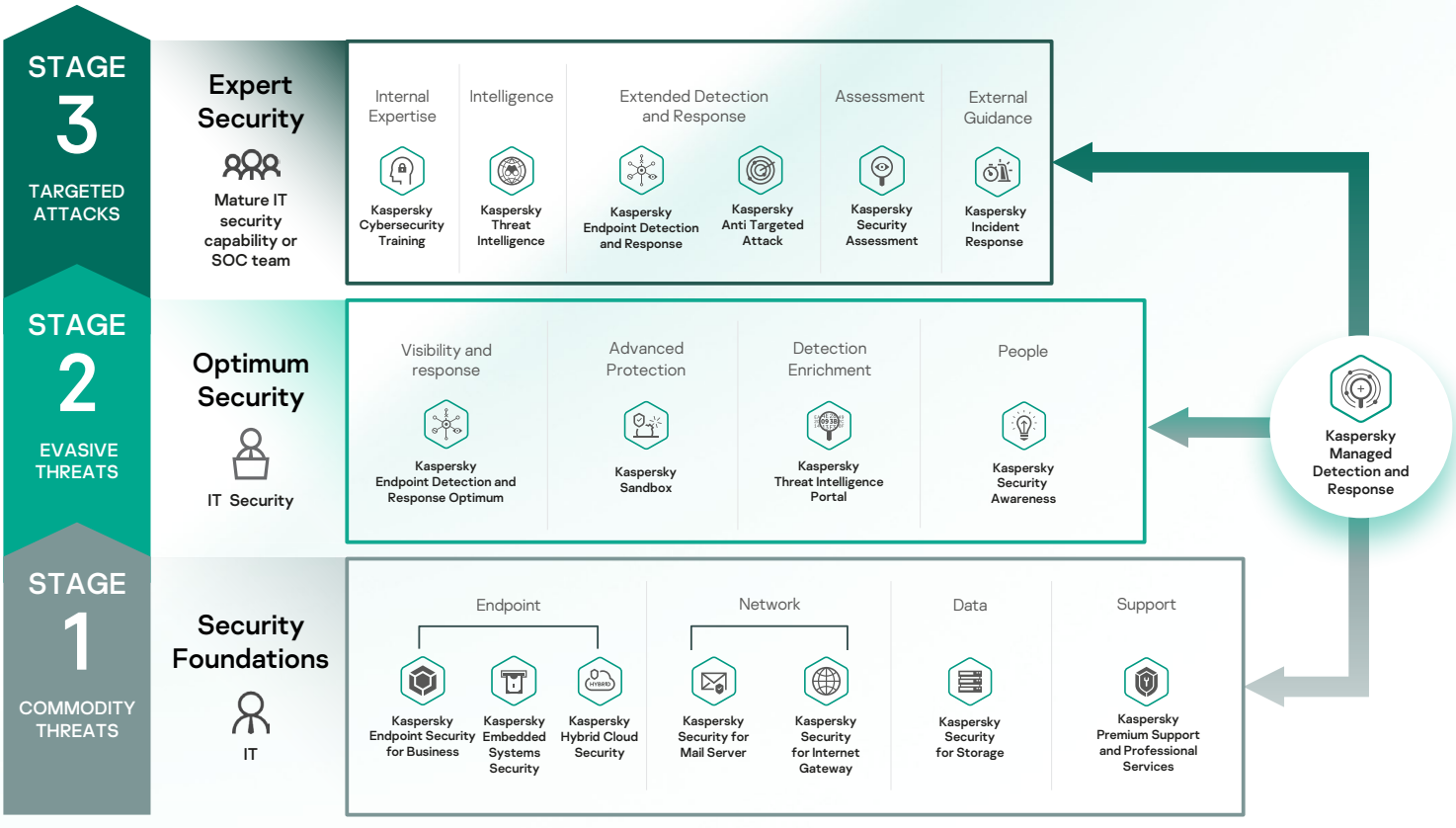

Figure 2. A stage-by-stage cybersecurity approach

Security Foundations

Block the maximum number of threats — automatically.

Security Foundations is a fundamental stage for organizations of any size and infrastructure complexity when building an integrated defense strategy against complex threats. It provides multi-vector automated prevention of a large number of possible incidents caused by commodity threats. This stage is usually sufficient for smaller enterprises with IT teams only.

Companies can't skip this stage and move directly to implementing advanced detection and response technologies. This is because most of those technologies require human involvement which is, of course, expensive and requires expertise. So expensive IT security staff get overwhelmed with alerts, without most threats even being prevented. And instead of proactively hunting for hidden threats and responding to incidents, IT security staff waste time sorting through and prioritizing thousands of alerts, leaving most of them untouched.

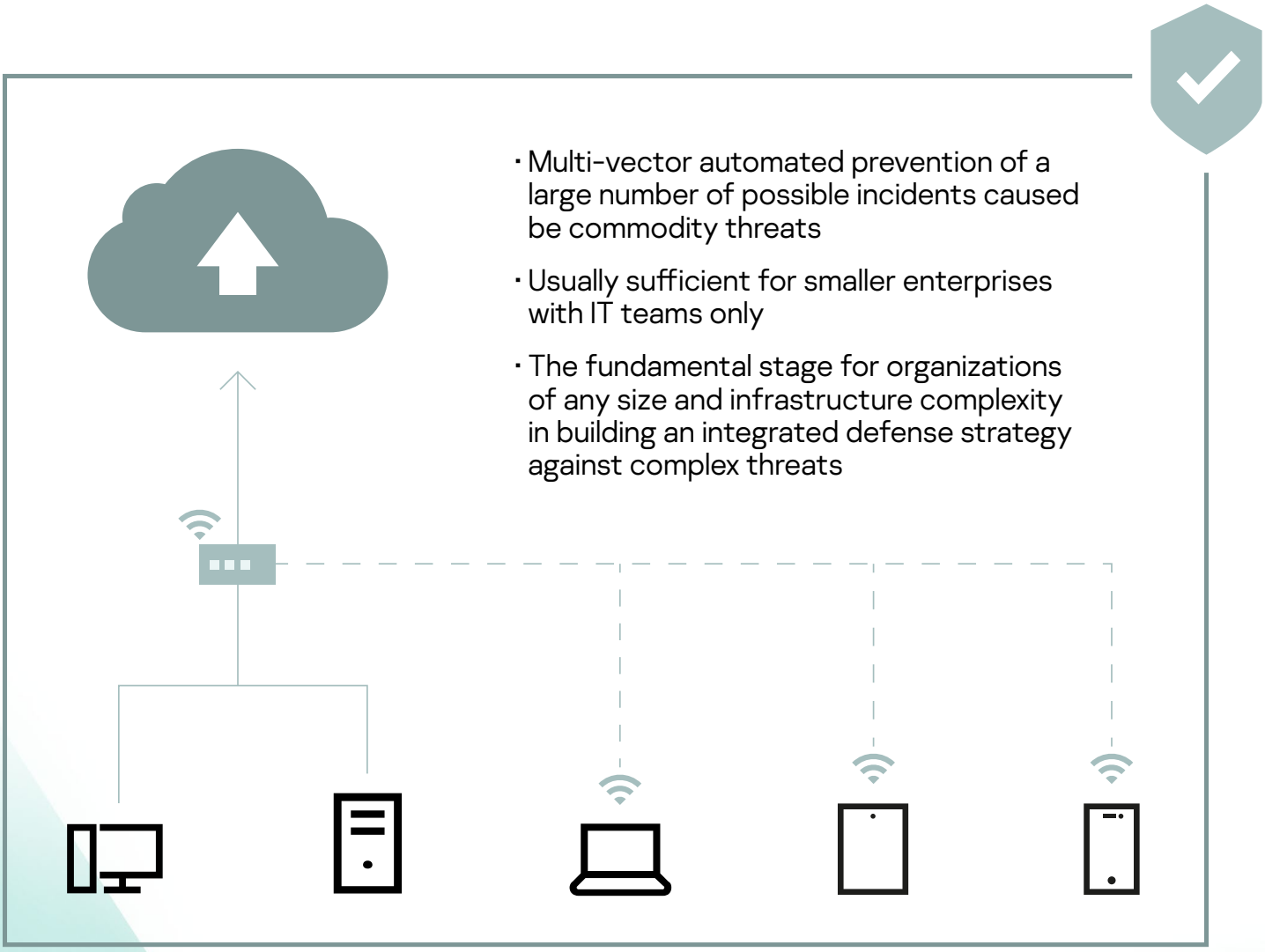

Figure 3. The key characteristics of Stage 1

Optimum Security

Focus on advanced detection and a fast response to threats evading preventive protection.

With the growing size and complexity of IT environments supporting business development and growth, organizations increase their potential attack surface too. They become more attractive targets for cybercriminals and are at higher risk of facing advanced threats that evade automatic prevention mechanisms.

As the potential attack surface grows, the importance of establishing at least basic incident response practices cannot be underestimated. These companies usually begin developing an IT security function inside their IT department, but its maturity is still low. Small IT security teams require instruments for automated detection of advanced threats and centralized response as the foundation for further maturing its function. Staff training also becomes essential to raise security awareness across the organization and motivating all employees to pay attention to cyberthreats and how to handle them – even if this is not considered to be a specific part of their job responsibilities.

Building on from Security Foundations, Optimum Security enables organizations with IT environments that are growing in size and complexity to counter commodity threats and threats that circumvent existing preventive mechanisms. A resource-conscious solution is ideal for small IT security teams with basic expertise. This stage enables customers to enhance their own detection and response capabilities, while benefiting from 24/7 managed protection. At the same time, a portfolio of computer-based gamified training products helps to shape employees' cyber-hygiene skills and motivate them to maintain safe practices.

- Security Foundations successfully inplemented
- IT environment is growing in size and complexity, creating an increased attack surface
- A small IT security team is in place, with some expertise
- Incident response capability is important to you

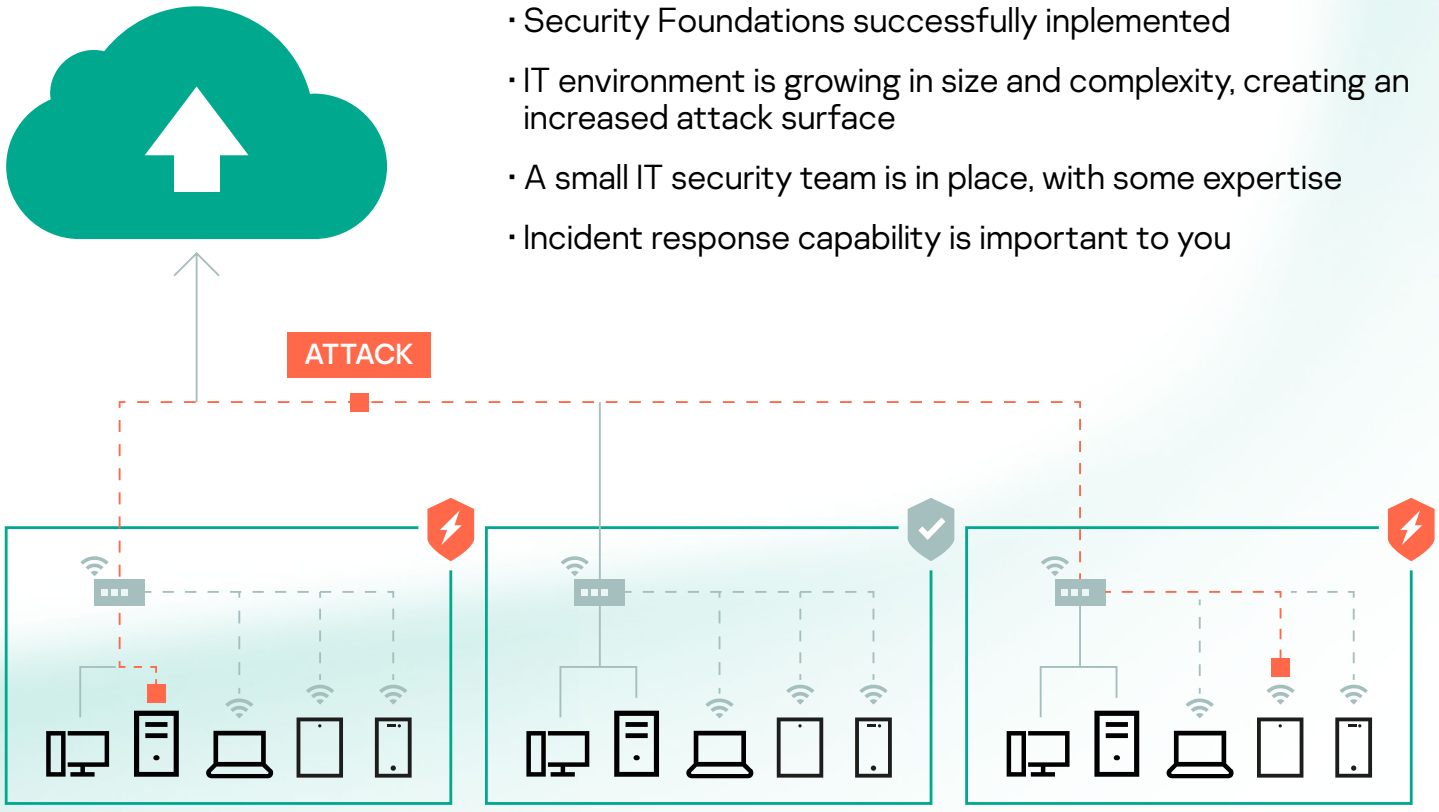

Figure 4. The key characteristics of Stage 2

Expert Security

Readiness for complex and APT-like attacks.

Adopting manual threat hunting practices and advanced use cases for threat intelligence while having a fully-equipped team with deep knowledge in specific topics like digital forensics and malware analysis will be vital for organizations at Stage 3. They will benefit from establishing trusted relationships with a highly qualified partner to quickly complement their existing capabilities with more specific skill sets when required. Kaspersky Expert Security delivers an Extended Detection and Response platform together with unequalled expert guidance, assessment, threat intelligence and skills training, which combine to cover the end-to-end security needs of any enterprise with a mature IT security function to face down today's complex threats, APT-like and targeted attacks.

- IT environments are becoming complex and distributed
- IT security team is mature or a Security Operations Center is established
- Risk appetite is low due to higher costs of security incidents and data breaches
- Regulatory compliance is a concern

Figure 5. The key characteristics of Stage 3

Why Kaspersky

Our mission is to build a safer world. We believe in a tomorrow where technology improves all of our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings.

We are a global company, with a global vision and a focus on international markets. We operate in 200 countries and territories and have 34 offices in more than 30 countries. Our team consists of more than 4,000 highly-qualified specialists.

We are constantly innovating, delivering protection that's effective, usable and accessible. Our 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. Our comprehensive security portfolio includes leading protection, detection and response solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 250,000 corporate clients protect what matters most to them.

www.kaspersky.com