KASPERSKY lab

Advanced Threat Defense and Targeted Attack Risk Mitigation

Kaspersky Anti Targeted Attack solution

www.kaspersky.com
#truecybersecurity

The growing risk of advanced threats and targeted attacks

200% growth of the recovery initiated at the same day and after week of discovering a security breach for Enterprises*.

*Results from Kaspersky Lab's Corporate IT Security Risks Survey 2016, conducted worldwide by Kaspersky Lab

15% of enterprises have experienced a targeted attack, more than 53% losing sensitive data as a result*.

*Kaspersky Global IT Security Risks Report 2015

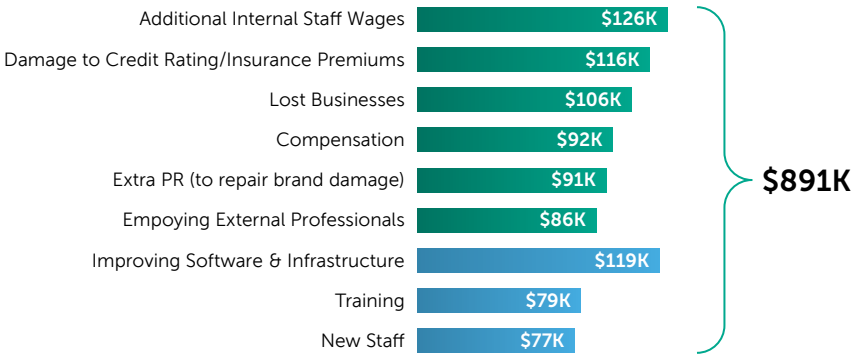
Every corporation big enough to occupy a significant place in its market is a potential target. This doesn't mean smaller businesses are immune – in many cases, criminals view them as an easy-to-breach stepping stone from which to reach the bigger target. But when it comes to market leaders, the odds in favor of becoming a victim of such an attack increase substantially. It's not a case of 'if' but 'when'...

Enterprise Threats Landscape

Targeted attacks and advanced threats – including Advanced Persistent Threats (APTs) – are some of the most dangerous risks to enterprise systems. However, while the threats and techniques that cybercriminals use are constantly evolving, too many organizations are relying on yesterday's security technologies and an outmoded mindset to protect against today's and tomorrow's threats.

Advanced, specially targeted threats can go undetected for weeks, months, or even years, while their actors slowly and silently gather information and work incrementally to exploit the unique vulnerabilities in their chosen targets' systems. Unlike regular malware, advanced, targeted threats are actively controlled and managed by the perpetrators. The goal isn't limited to malware delivery: the objective is to persist inside the enterprise perimeter. These attacks are the result of patient, often painstaking research by actors who are prepared to play a waiting game in the quest for their prize.

Average loss from a single targeted attack:



Who's doing the attacking?

Cybercriminals – who sell data to the highest bidder or simply steal money. They usually develop their cyber tools themselves or buy them on the dark web.

Competitor businesses – looking for confidential data or even committing sabotage. They will usually 'buy in' the services of cyber-mercenaries.

Cyber-mercenaries – masters of cyber-espionage, they develop their own tools and sell their 'services' to the highest bidder.

Hacktivists – claim to be working for a 'greater good', they're inventive, use complex toolsets and present a serious problem for any organization that attracts their attention

Government agencies – they may deny it, but it's generally accepted that governments the world over routinely track individuals, groups and businesses. Their toolsets can be extremely sophisticated, expensive and hard to detect.

Internal and External factors which leads to successful breach

Key factors contributing to the successful development of targeted attacks on IT infrastructures include:

- Lack of preventive capabilities and an over-optimistic view of current perimeter security
- Low employees awareness of information security risks
- Lack of visibility over the IT environment and particularly network routing
- Proprietary and outdated software and operating systems
- Lack of security team qualification regarding malware research, digital forensics, incident response and threat intelligence

What's the risk?

Risks to all organisations:

- Unauthorized transactions
- Critical data theft or corruption
- Stealth process manipulation
- Undermining by Competitors
- Blackmail extortion
- Identity theft

Risks to key industry sectors:

Financial Services

- Unauthorized transactions
- ATM attacks with physical cash theft
- Identity theft

Government

- Data manipulation
- Espionage
- Restricted availability of online services
- Identity theft
- Hacktivism acts

Manufacturing and High Technology

- Espionage (know how)
- Compromized critical technological processes

Telecommunication

- Attack on corporate clients using telecoms infrastructure
- Manipulation of mail servers for social engineering
- Billing control
- Manipulation of web resources for phishing purposes
- Using compromised infrastructure (devices/IoTs) for DDoS attacks

Energy and Utilities

- Manipulating with calculations data
- Attacks on technological networks with physical damage

Mass media

- Hacktivism
- Compromized web site (deface, phishing) and spreading attacks on mass audience

Healthcare

- Theft of patient information
- Attacks on telemedicine equipment

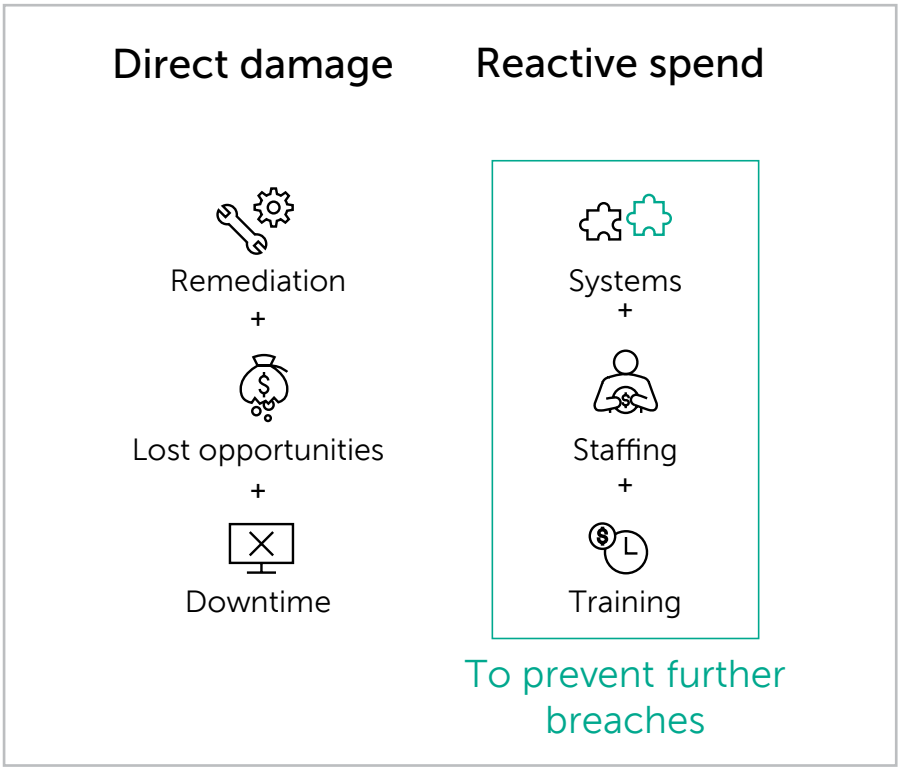
Targeted Attacks - Cybercrime as a Business Profession

Most targeted attacks are overseen by highly experienced cybercriminals and hackers who know how to adapt each phase of their attack to slip past traditional defenses, exploit weaknesses and maximize the amount of valuables they can steal, including money, confidential data and more.

The security geek attackers of the past have metamorphosed into professional for whom cybercrime is a business. Their sole motivation in targeting and attacking any enterprise is optimum profit – calculated even before launching the attack, on the basis of the associated costs and potential rewards. The objective is, of course, to minimize up-front costs by attacking as cheaply as possible, with maximum financial outcomes.

Most targeted attacks use a combination of social engineering and a customized toolset. The cost of launching an effective targeted attack has fallen significantly, with a commensurate increase in the total number of attacks globally.

So what's at stake when an organization like yours falls victim to a targeted attack?



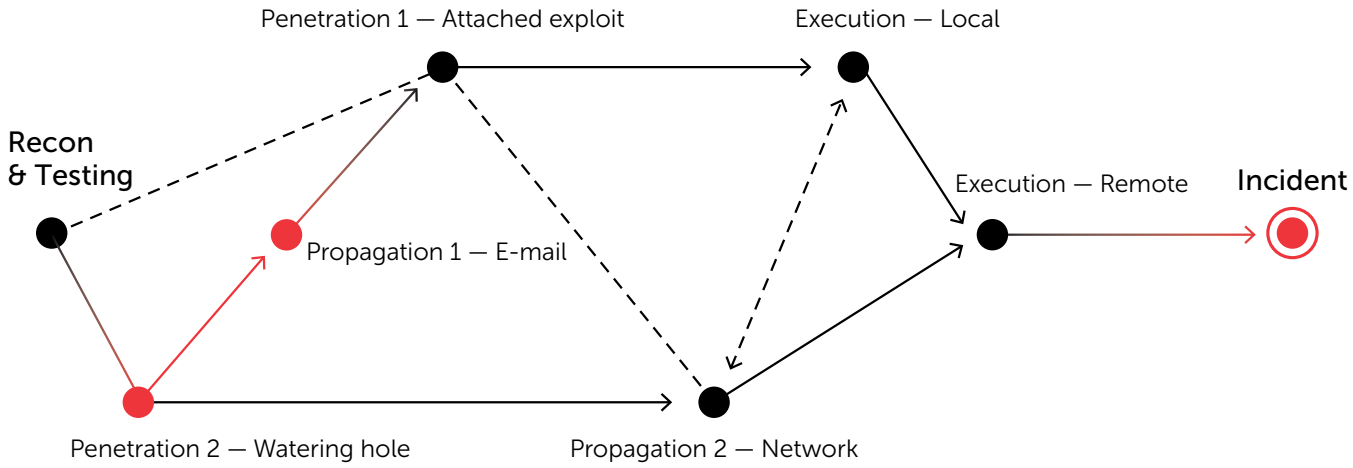
Direct financial losses. Attackers may try to commit cyber-fraud by stealing banking credentials in order to access corporate accounts and conduct fraudulent transactions.

Disruption of key business processes. While some attacks may – merely as a by-product – impair or slow down critical business processes, others may deliberately set out to sabotage them. Even if an attack is discovered, there's likely to be a further period of disruption while the targeted business conducts investigations and recovers its operations, during which further business opportunities may be lost.

Clean-up costs. After an attack, you can be faced with having to cover a whole host of expenses that haven't been budgeted for. Recovering systems and processes is likely to involve both capital expenditure and operational expenses – like hiring security and systems consultants.

Anatomy of a Targeted Attack

In theory, the targeted attack kill chain seems pretty straightforward: Reconnaissance & Testing, Penetration, Propagation, Execution, Outcome. This might suggest that by automatically blocking the first steps of a multi-stage attack, the attack itself can be thwarted.



But in reality, targeted attacks are highly sophisticated and nonlinear in terms of their progression and execution. So automated detection capabilities, continuous monitoring and threat hunting should all be in place as part of a multi-stage defense strategy.

Targeted attacks are long-term processes that compromise security and give the attacker unauthorized control over the victim's IT – helping the attacker to avoid detection by traditional security technologies.

Although some attacks may use Advanced Persistent Threats (APTs) – which can be very effective, but expensive to implement – others may use a single technique, such as advanced malware or a zero-day exploit.

A targeted attack is a lengthy process that violates security and allows a cybercriminal bypassing authorization procedures and interacting with the IT infrastructure, so avoiding detection by traditional means.

So first of all, itirst process – an ongoing activity, a project, rather than a one-off malicious action. According to our experience in monitoring global attacks, such operations tend to last at least 100 days, and for government agencies, large market players and critical infrastructures, the time can be calculated in years.

Secondly, the process is aimed at a specific infrastructure, designed to overcome specific security mechanisms, and may well initially involve targeting named employees through email or social media . This is a very different approach from the mass mailings of standard malicious software based attackers, who are pursuing completely different goals. In the case of a targeted attack, the methodology and kill chain stages are built around the specific victim.

Thirdly, this operation is usually managed by an organized group or team of professionals, sometimes international, armed with sophisticated technical tools. Their activities could be said to be not just a project: more of a multi-combat operation. For example, attackers might typically compile a list of employees who can potentially become the 'gateway' to the target organization, networks, and study their online profiles and social media activity. After that, the task of gaining control over the victim's working computer is virtually solved. On the employees computer is infected, and intruders go on to seize control of the network from where they can direct their criminal activities.

Enterprise Security challenges

With the risk of sophisticated threats growing exponentially, many enterprises already implement technologies and services in the hope of achieving the next level of visibility and protection against current threats. But without a multi-faceted approach and strategic planning, these efforts can fall short of expectations.

Disappointing outcomes of 'patchy' or unstructured security investment can include:

1. Major investment in a sandbox, in standalone technologies, or in the construction of a SOC, any of which then fail to generate commensurate improvements in security outcome.

Perimeter security techniques like firewalls and anti-malware software can hold their own against some of the more opportunistic attacks. But targeted attacks are a different matter.

Some vendors have sought to address APTs using a variety of standalone, discrete products: sandboxes, network anomaly analysis or even endpoint-focused monitoring. While these individual elements all can – and do – offer some protection and blocking of the cybercriminal's toolset, they're not enough in themselves to uncover a targeted, coordinated attack.

To achieve this requires the detection of multiple events occurring across all levels of the enterprise infrastructure. The information gained can then be processed using a multi- layered analysis system, followed by interpretation applying real-time security intelligence from a trusted source. In other words, your best investment is an approach that integrates the best of many technologies, including sandboxing with network anomalies analysis and endpoint events analysis into an overall, end-to-end process.

2. Current solutions generate too many security events for your SOC team to process, analyze, triage, and respond to within a reasonable timeframe.

3. Lack of security skills appropriate to current levels of threat sophistication. Security experts may be skilled in incident detection and fast remediation (golden image, blacklisting URLs/files, building some rules) but not fully qualified to implement a full circle response process (qualifying risk levels, performing initial analyses, investigation, containment, forensics)

4. Lack of operational visibility. During a targeted attack, cybercriminals can easily evade traditional security solutions by using stolen credentials and legitimate software, so that they are not apparently creating any systems violations.

Because attackers do their utmost to hide their malicious activities, it can be very difficult for an in-house IT security team to spot an attack – and that means the attackers can continue to cause damage over an extended period.

The reality is that malware is responsible for only 40% of breaches – as we've seen, threat actors use a variety of techniques to access company systems.
Even when malware is used, 70-90% of it is is unique to the organization it's found in (Verizon: Data Breach Investigation Report).

5. Difficulty in knowing what expertise to employ and grow in-house, what security tasks to outsource, and what can safely be left to automated systems.

With the growing severity of security incidents and their potential impact on overall business effectiveness, one of the main security department challenges is that of fielding a sufficient number and range of appropriately qualified experts. A fully effective security strategy requires not just continuous monitoring and detection capabilities but a fast response and qualified remediation, with appropriate forensic processes in place.

Conventional SOC teams tend to focus on only part of this task - detection and response. The implementation of automated solutions helps free up experts to undertake the next steps in the incident management process, but few enterprises are ready to perform every high level task in-house. So the challenge is in identifying which elements of the overall process (management, qualifying the risk, prioritization, fast recovery) should be undertaken by the in-house team and which (malware research, digital forensic, incident response, threat hunting) may be more effectively outsourced to specialists.

A word on sandboxes

Many 'targeted attack detection solutions' on the market simply comprise a standalone sandbox. Even vendors with no track record in new, advanced threat discovery claim to offer sandboxes that are often little more than an extension of their anti-malware engines – and have no significant threat intelligence behind them.

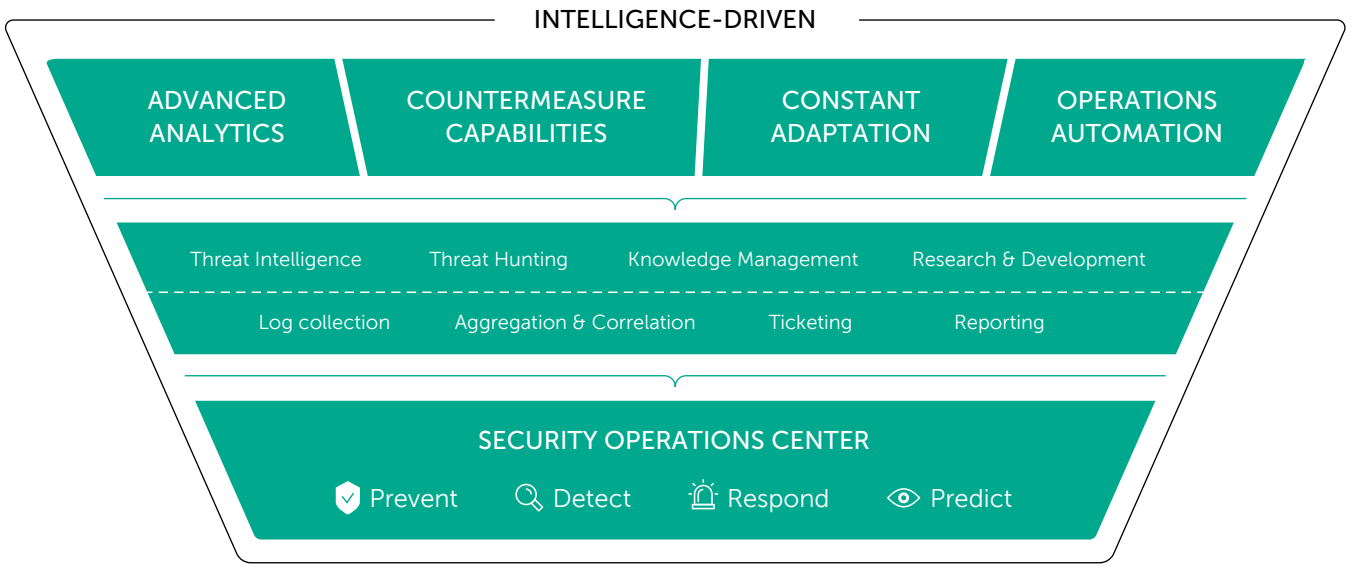
Kaspersky Lab's advanced sandbox is just another part of our integrated detection capabilities. It's been developed directly out of our in-lab sandbox complex, the technology we've been using for more than a decade. Its capabilities have been honed on statistics gathered from ten years of threat analysis, making it more mature and more focused on targeted threats than the silver bullet' sandbox solutions currently of offer.

The Intelligence-driven Enterprise SOC

Cybercriminals have adapted their techniques to sidestep traditional defenses and lurk undetected in systems for months, or even years. It's time for enterprise security to adapt in its turn, by taking an intelligence-driven, multi-layered approach to IT security.

Until recently, it was enough to defend the corporate perimeter using commonly available security technologies that prevented malware infections or unauthorized access to the corporate network. However, today, with the rise of targeted attacks, this simple approach is no longer adequate.

If your security department is going to guard against new dangers, you'll need a multi-faceted, highly adaptable approach to security, based around a conventional SOC empowered with threat intelligence and multi-layered security solutions.



Improving enterprise security processes

The Information Security Department is responsible for the organizational and technical protection of critical information and business processes in often complex IT environments. This includes, for example, the increasing adoption of automated solutions and software components, and the transition to electronic document management.

The avalanche-like growth in the number of advanced threats and targeted attacks has generated increasing numbers of solutions. In order to collect, store and process the unstructured data generated, in order to identify and prioritize complex multi-level attacks, existing processes must be upgraded. These include:

- the manual prioritization of threats and the evaluation of factors potentially indicative of a possible targeted attack
- Information collecting about targeted attacks and advanced statistics threats;
- identification of and response to incidents;
- analysis of suspicious objects in network traffic and email attachments
- detection of abnormal / unusual activity within the protected infrastructure

Large enterprises are responding to today's advanced threats by moving to centralized information security management, consolidating data from disparate Security solutions (through automating data collection and correlation of events - SIEM) and unifying its presentation through the construction of security monitoring centers (SOC, Security Operations Center) . But for this approach to be effective against targeted attacks and advanced threats, a comprehensive understanding of security problems and the deep knowledge of cyberthreat analysis is required.

Our Solution

Kaspersky Lab was the first technology company to establish a dedicated advanced threat lab, back in 2008.

That's how we have uncovered more advanced, targeted threats than any other security vendor. When you hear in the news about the latest advanced persistent threat, the chances that it was detected by Kaspersky Lab's elite Global Research and Analysis Team (GReAT).

With an enviable track record in detecting targeted attacks and APTs, Our GReAT team is renowned for its threat intelligence. The team has played a major role in discovering many of the most sophisticated attacks, like:

- Stuxnet
- RedOctober
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

... and many more.

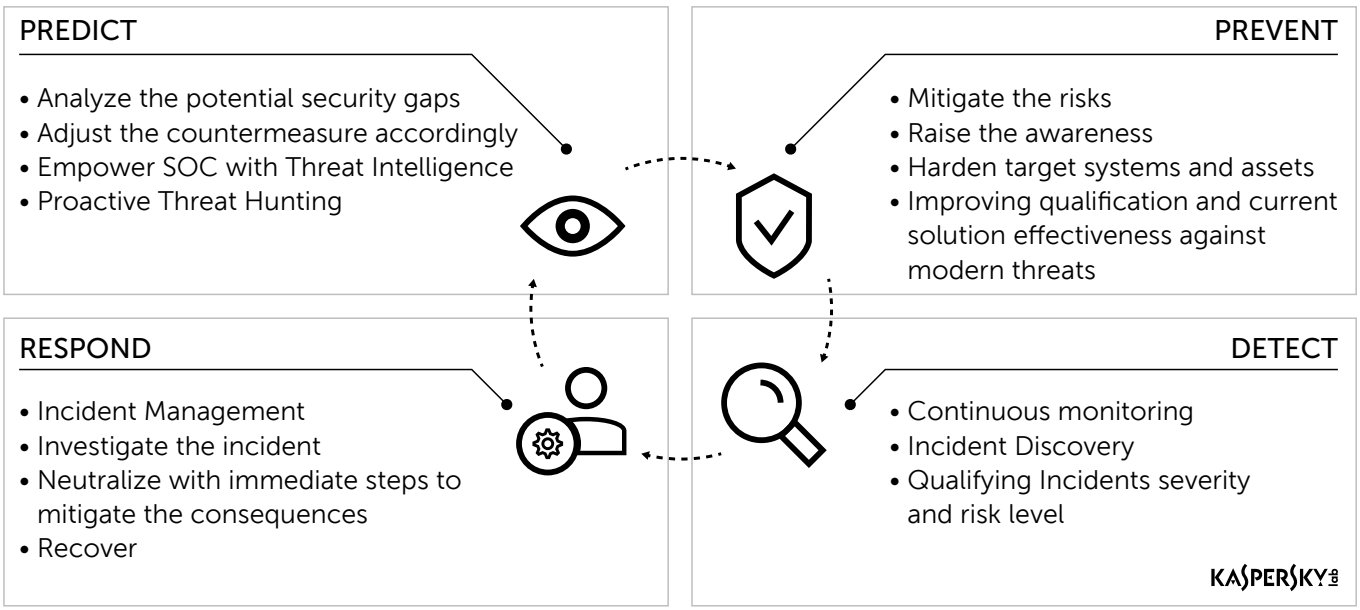
Kaspersky Lab's understanding of the inner workings of some of the world's most sophisticated threats has enabled us to develop a strategic portfolio of technologies and services capable of delivering a fully integrated, adaptive security approach. Our expertise has seen Kaspersky Lab achieve more first place rankings in independent threat detection and mitigation tests than any other IT security company. Now, we've brought this targeted attack detection expertise together into one standalone solution – the culmination of a two decade' s worth of threat research and analysis, generating mature, proven technologies.

While the majority of simple cyberthreats can be blocked by traditional, signature-based and heuristics-enhanced security products, today's cybercriminals and hackers are using increasingly sophisticated attacks – to target specific organizations. Targeted attacks – including Advanced Persistent Threats (APTs) – are now one of the most dangerous risks that enterprises have to deal with. However, while the threats – and the techniques that cybercriminals and hackers employ – are constantly evolving, many businesses are failing to adapt their security strategies .

Harder to detect and - often - even harder to eliminate, targeted attacks and advanced threats call for a comprehensive, adaptive security strategy. Kaspersky Lab's Adaptive Security Strategy is founded on the most viable security architecture as described by Gartner. Our approach is to provide a cycle of activities in four key areas: Prevent, Detect, Respond, and Predict.

- Prevent – reduce the risk of advanced threats and targeted attacks
- Detect – identify activities that could signal a targeted attack
- Respond – close security gaps and investigate attacks
- Predict – where and how new targeted attacks could appear

Essentially, this assumes that traditional prevention systems should function in coordination with detection technologies, threat analytics, response capabilities and predictive security techniques. This helps to create a cybersecurity system that continuously adapts and responds to emerging enterprise challenges.



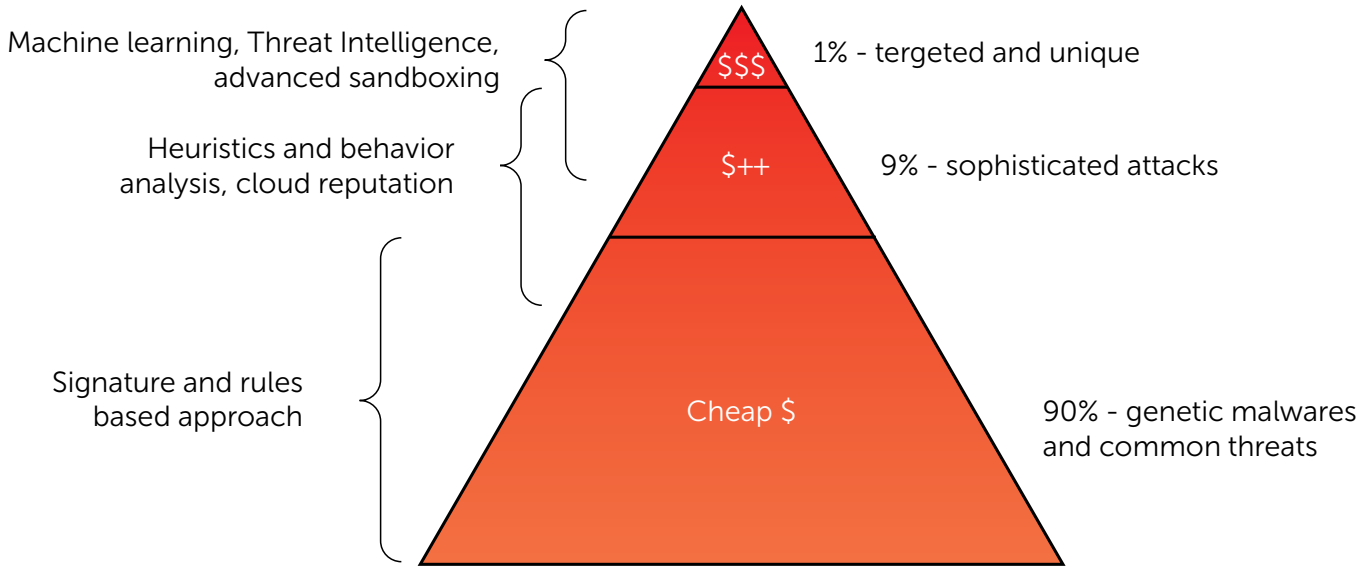
Prevention - using award-winning security technologies to decrease the risk of targeted attacks

For targeted attacks, prevention technologies are valuable in filtering out unnecessary incidents, common malicious objects and irrelevant communications.

But comprehensive system hardening with targeted security solutions, security education and by raising awareness is also of value - increasing the amount of time and investment necessary for attackers to invest in penetrating your controlled perimeter, and rendering you no longer cost-effective to attack.

Prevention-based security products can be very effective in protecting against common threats – including malware, network attacks, data leakage and more. But even these technologies are not sufficient to protect a business against the targeted attacks. During a targeted attack, conventional, prevention-based security technologies may spot some incidents but will usually fail to determine that t individual incidents are part of a much more dangerous and complex attack that could be causing severe damage to your business... and will continue to inflict damage over the long term.

However, multi-layered, prevention-based technologies are still a key element in the new, proactive approach to guarding against targeted attacks.



Addressing different threats with security technologies

80% of targeted attacks start with a malicious email containing an attachment or link.

Preferred penetration targets for cybercriminals include HR, call centers, personal assistants to senior management and outsourced areas of the business. These are seen as the least prepared areas of the organization.

It's essential for enterprise organizations to continue using 'traditional' security technologies to:

1. Automate the filtering and blocking of events and incidents not related to Targeted attacks. which will help to avoid unnecessary distractions to relevant incident discovery

2. Harden IT infrastructure against cheap and easy-to-perform techniques (social engineering, removable devices, mobile devices, malware and malicious email delivery etc.). In fact all past spending to perimeter and endpoint security, along with controls implemented, helps to increase amount of effort and investment required by cybercriminals in order to penetrate your network.

But if the attacker is sufficiently highly motivated, and perhaps even hired by a third party to conduct a successful attack, a prevention-only approach will not be enough.

Detection — multi-vector advanced threat discovery before the damage occurs

The Kaspersky Anti Targeted Attack platform includes:

- Multi-layered sensor architecture – to give 'all round' visibility. Through a combination of network, web & email, and endpoint sensors, KATA provides advanced detection at every level of your corporate IT infrastructure
- Advanced Sandbox – to assess new threats. The result of over a decade of continuous development, our Advanced Sandbox offers an isolated, virtualized environment where suspicious objects can be safely executed so their behavior can be observed
- Powerful analytical engines – for rapid verdicts and fewer false positives. Our Targeted Attack Analyzer assesses data from network and endpoint sensors and rapidly generates threat detection verdicts for the security team.

The earlier you detect an attack, the lower your financial losses and the less disruption your organization will suffer. So the quality and effectiveness of detection is paramount.

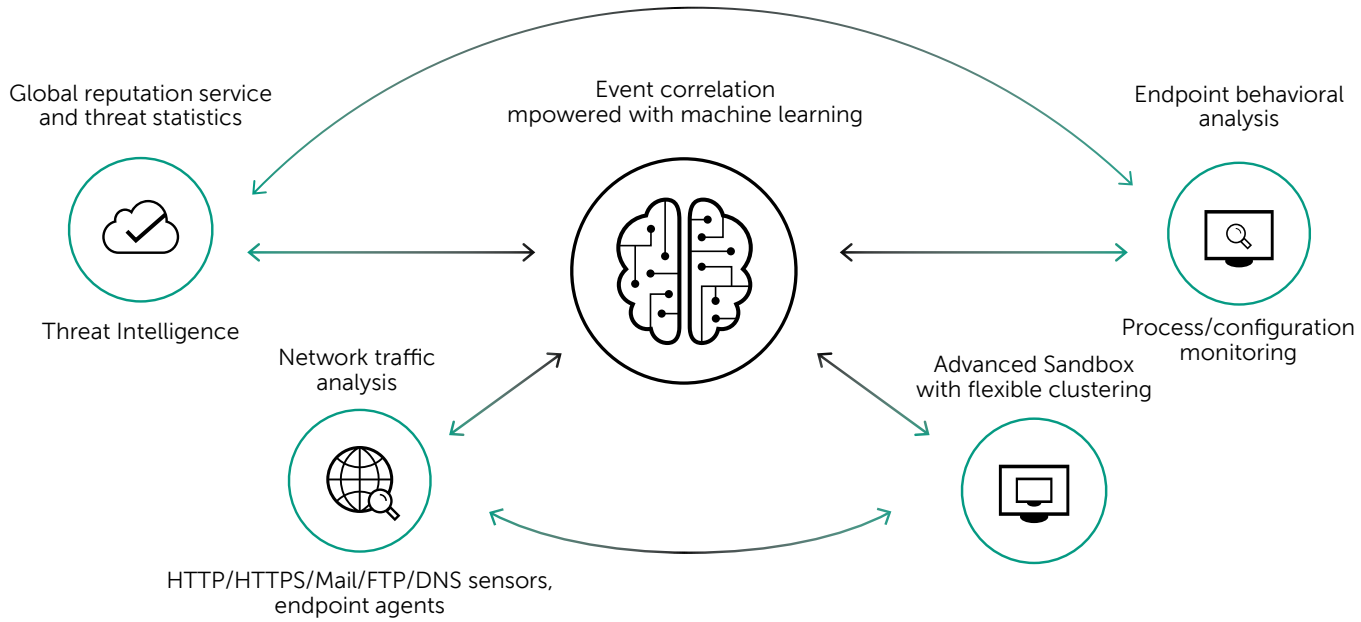
Because targeted attacks are both compound and complex, detecting them calls for a deep practical knowledge about how advanced and targeted attacks work. Simple anti-malware solutions are not able to defend against these types of attack. Instead, you'll need detection technologies that can access up-to-the-minute threat intelligence data – and can perform detailed analyses of suspicious behavior that may be occurring at different levels of your corporate network.

The ability to detect targeted attacks consists of connected solutions and services able to deliver:

- Training
- Targeted Attack Discovery expertise - one-time audit of infrastructure in order to find traces of compromise
- Specialized solution - Kaspersky Anti Targeted Attack platform
- Threat Data Feeds for real-time threat exchange and updates about new threats
- Custom and APT reports for better understanding of threat sources and methods

The Kaspersky Anti Targeted Attack Platform (KATA) is an innovative solution that provides detection capabilities going far beyond conventional, prevention-focused security technologies.

KATA is part of an adaptive, integrated approach to enterprise security. Real time monitoring of network traffic, combined with object sandboxing and endpoint behavior analysis, delivers a detailed insight into what's happening across a business's IT infrastructure. By correlating events from multiple layers including network, endpoints and the global threat landscape, KATA achieves the 'near real-time' detection of complex threats and helps to enable retrospective investigations.

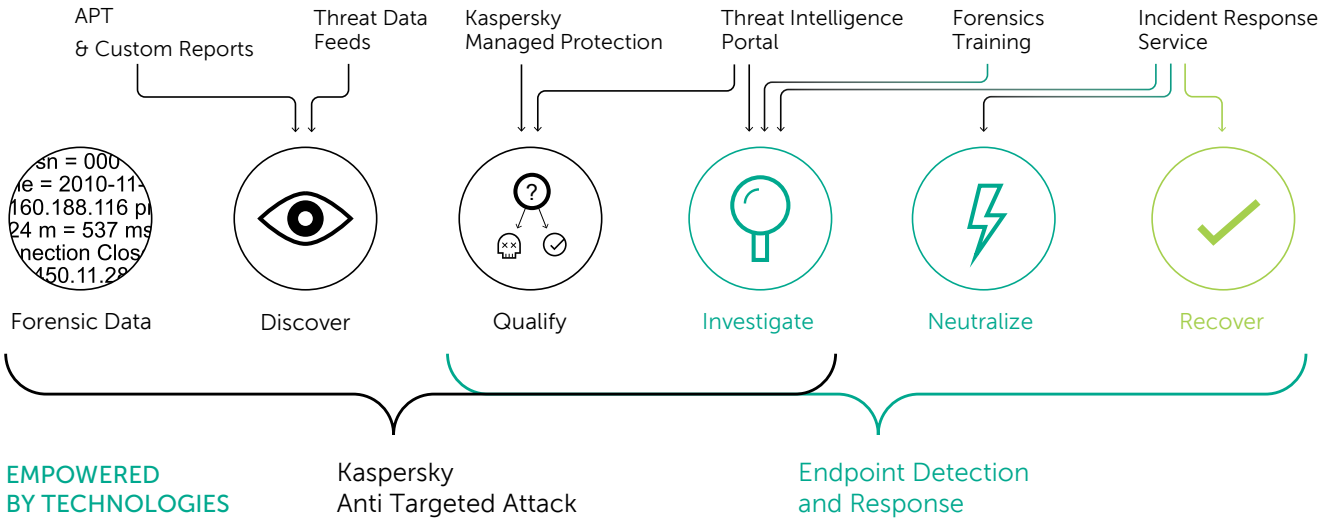


Response — helping businesses to recover from attacks

Of course, achieving a higher rate of detection is only part of the battle. The best detection technologies are not much use if you don't have the tools and expertise needed to respond rapidly to the 'live' threat that's potentially damaging your organization

After detecting an attack, it's important to have access to recognized security experts with the skills and experience to help:

- Assess and rectify the damage
- Rapidly recover your operations
- Receive actionabale intelligence after Incident Investigation process
- Plan actions to prevent further repeat of the same attack scenarious



Once Kaspersky Anti Targeted Attack Platform identifies that your business is being attacked, our experts can also help you analyze the attack. Our Incident Response Service includes:

- Incident assessment. Initial analysis of an incident – rapidly delivered to help you minimize the damage to your business (the analysis can be performed on-site or remotely)
- Evidence collection. For example, gathering hard disk drive images, memory dumps, network traces and other information that's relevant to the incident
- Forensic analysis. Detailed analysis to help establish information about:
  - What was attacked
  - Who carried out the attack
  - The period during which your business was attacked
  - Where the attack originated
  - Why your business was attacked
  - How the attack was implemented
- Malware analysis. Detailed analysis of malware that was used as part of the attack.
- Remediation plan. A detailed plan that will help your business to prevent the malware propagating across more of your network – plus help you create an uninstallation plan.
- Investigation report. A detailed report that includes information about the incident investigation and remediation.
  If your own security team is able to carry out many of the incident response tasks, you may wish to use one of our other services:
- Malware Analysis Service – subjects the malware your team has isolated to detailed analysis.
- Digital Forensics Service – analyzes digital evidence & incident effects gathered by your team.

Prediction - doing more to guard against future threats

With the threat landscape constantly changing, your security strategy must continually evolve to meet new challenges.

Security isn't a 'one-off activity' – it's an ongoing process that calls for continuous assessment of:

- The latest threats
- The effectiveness of your IT security

... so your business can adapt to new risks and changing demands.

Having access to experts that can keep you updated on the global threat landscape – and help you to test your systems and your existing defenses – is a vital element in helping your organization to adapt and keep pace with new security threats.

Over the years, our global security experts have amassed a vast amount of knowledge about how advanced and targeted attacks work – and we're constantly analyzing new attack techniques. This hard-won expertise means we're uniquely placed to predict new attack methods and help you to be ready to combat them.

In addition, we can offer specialized services to help you 'harden' your IT infrastructure:

- Penetration Testing Services – to help you assess the effectiveness of your current security provisions
- Application Security Assessment Services – to help you find software vulnerabilities... before the cybercriminals do
- Advanced Cybersecurity Training – to help train your own experts and build your own Security Operations Center
- Intelligence Reporting and Customized Threat Reporting – to help keep you updated on today's constantly changing threat landscape
- Threat Lookup portal – access to Kaspersky Lab intelligence global database to help Empower your malware researches

Kaspersky Adaptive Security Strategy founded on the most viable security architecture described by Gartner. Kaspersky Lab approach providing cycle of activities in four key areas: Prevent, Detect, Respond, and Predict. Essentially, it assumes that traditional prevention systems should function in connection with detection technologies, threat analytics, response capabilities and predictive security techniques. This helps to create a cybersecurity system that continuously adapts and responds to the emerging enterprise challenges.

Adopting Kaspersky Lab's Advanced Security Strategy means:

1. Moving from from a reactive security model to a proactive model based on risk management, continuous monitoring, more informed incident response and threat hunting capabilities

2. Your operational framework streamlines day-to-day security processes and boosts security effectiveness through a multi-layered defense model that prevents and detects advanced threats at each stage of the attack.

3. One integrated platform reduces the security alerts that overwhelm most security teams by providing threat intelligence-based context and prioritization to alerts as well as improving tactical responses by sharing threats knowledge, deep expertise and providing security intelligence services.

4. This environment provides security analysts with visibility of all attack stages in a unified way, enabling seamless threat analysis and confident investigation of both known and unknown threats before they impact the business.

5. Global Threat Intelligence sharing through APT and threat intelligence portals provides unique proactive insights into the motives and intentions of your adversaries , so you can prioritize policies and security investment planning accordingly.

A world of expertise in Kaspersky Lab Technologies

The effectiveness of Kaspersky Lab products is proven on a regular basis by the results of independent testing. In 2016, the company headed the Top 3 rating of security solution manufacturers. According to the results of 78 different tests performed by respected test organizations in several countries, Kaspersky Lab solutions fnished in the Top 3 in 90% of tests and topped the rating on 55 occasions. This is undeniable proof that Kaspersky Lab provides the industry's best protection.

Proven solution against advanced threats

During 2017, our Kaspersky Anti-Targeted Attack Platform has continued participate in ICSA Lab tests.

The latest tests lasted for 37 days and consisted of 585 attacks and 519 clean files. KATA demonstrated excellent results:

- Perfect detection rate – 100% (ZERO missed samples)
- Lowest possible false positive rate – 0%
- Achieved 'Certified' status

Here are a few quotes from the resulting report issued by ICSA on 7th July:

- 'Kaspersky's solution did remarkably well during this test cycle'
- 'The Kaspersky Lab KATA platform detected 100.0% of the threats it encountered during testing, considerably better than the percentage required for certification.'
- 'Kaspersky Labs' KATA demonstrated excellent threat detection effectiveness against nearly 600 new and little-known threats.'
- 'Regardless of how new or how old the threat, the Kaspersky KATA platform detected all new and little-known malicious threats.'
- 'The Kaspersky KATA platform had zero false positives during this test cycle, which is excellent.'
- 'Kaspersky Labs' KATA advanced threat defense solution passed all the test cases to retain ICSA Labs Advanced Threat Defense Certification. Successful completion of this test cycle marks Kaspersky Labs' 3rd consecutive quarter having met the ICSA Labs ATD certification testing criteria.'

NOTE: ICSA testing methodology is dynamic and changes from quarter to quarter. The test itself is a continuously evolving simulation of a real environment and attack methods. The level of security is not measured at one given moment but over an extensive period (more than 30 days) of continuous operation under numerous attacks. In this way, the test aims to showcase the efficiency and effectiveness of a solution from a user standpoint.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Visionaire and comprehensive approach

For several years Radicati Group doing an independent analysis of the Market for APT Protection Solutions Revealing Top Players, Trail Blazers, Specialists and Mature Players. In the result of the market analysis, which just released, Kaspersky Lab's approach of countering targeted attacks and advanced threats were evaluated with an excellent side.

In 2017 KATA significantly improved its position with a major move from Specialists to Trail Blazering leader.

Trail Blazing vendors offer advanced, best of breed technology, in some areas of their solutions, but don't necessarily have all the features and functionality that would position them as Top Players. Trail Blazers, however, have the potential for "disrupting" the market with new technology or new delivery models. In time, these vendors are most likely to grow into Top Players.

«The Kaspersky Anti Targeted Attack Platform provides advanced threat and targeted attack detection across all layers of a targeted attack – initial infection, command and control communications, and lateral movements and data exfiltration».

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com