KASPERSKY lab

KASPERSKY ANTI TARGETED ATTACK PLATFORM

Detects advanced threats...
in real time

www.kaspersky.com

The number of targeted attacks against enterprises is growing – and the techniques and skills of the attackers are more sophisticated than ever. Today's targeted attacks and advanced threats are harder to detect – and often harder to contain and eliminate – so enterprises need a comprehensive, adaptive security strategy.

Security weak points and modern threats

Most enterprises have already made large investments in traditional IT security solutions – mostly located at the gateway level. However, although these preventive security technologies can be very effective in protecting against common threats – including malware, data leakage, network attacks and more – the overall number of business security incidents and breaches has not decreased.

Advanced, targeted threats can go undetected for weeks, months or years – while the cybercriminals silently gather valuable information and / or impact vital business processes. During such an attack, prevention-based security technologies may detect some incidents but will usually fail to determine that individual issues are part of a much more dangerous and complex attack that could be causing severe damage to the business... and will continue to inflict damage over the long term.

Targeted attacks are long-term processes that compromise security and give the attacker unauthorized control over the victim's IT – plus help 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 – other attacks may use a single technique, such as advanced malware or a zero-day.

To improve the security levels that traditional solutions can provide, many businesses are automating processes – via Security Information and Event Management (SIEM) systems. Some businesses then go on to develop their own dedicated Security Operations Center – for correlating events and data, centralizing security management and responding to incidents. However, to be fully effective, this approach requires a global vision of security and in-depth expertise in cyberthreat analysis. Even multinational corporations are rarely able to recruit, train and retain the necessary experts within their in-house security teams.

Overcoming the limitations of preventive security technologies

Because yesterday's preventive-only approaches are not effective against targeted attacks, businesses need to reconsider their security – or risk being unable to detect when cybercriminals have gained access to their systems.

As an internationally recognized researcher of cyberthreats, Kaspersky Lab supports the use of a strategy whereby businesses implement a continuous, multilayered process for defending against targeted attacks.

Identifying the presence of a targeted attack requires more than just finding malicious samples or unauthorized connections. Advanced detection depends on an understanding of normal system behavior and normal user behavior – plus constant analysis of all activities – to ensure adequate visibility across all IT infrastructure. To ensure the latest threats can be detected, businesses also need to receive proactive threat updates and global Intelligence about new attack methods.

The more effort a business devotes to protection – the more it costs cybercriminals to breach that business's systems. As a first stage, it's essential that the business identifies weak points within its current systems – and proactively eliminates those issues. It's also important to ensure employees are aware of security risks – especially as cybercriminals recognize the potential for 'human error' and often deliberately target employees during an attack. In addition, the business's security officers should be trained in the identification – and prioritization – of incidents that are related to targeted attacks.

An adaptive security strategy

Kaspersky Lab has an enviable track record as an industry leader in the discovery of targeted attacks and APTs. Almost a third of the company's employees are security research experts. In addition, the cloud-based Kaspersky Security Network (KSN) is continually receiving data about new threats – from all points on the globe. This valuable data 'from the field' helps the company to discover over 310,000 new malicious programs and threats every day.

Kaspersky Lab is a pioneer in helping businesses to change their security strategies – in order to defend against advanced threats and targeted attacks. We offer a unique combination of technologies and services – all underpinned by world-leading security intelligence – to help businesses to detect targeted attacks and mitigate risks... at an earlier stage, before severe damage is caused.

We believe that every business needs to establish an adaptive security strategy that is based on four vital elements:

- **PREDICT** – to help businesses to evaluate their current security and identify how future targeted attacks could strike at their infrastructure
- **RESPOND** – by helping businesses to perform investigations and to close their security gaps

- **PREVENT** – to help block advanced threats and reduce the risk of targeted attacks
- **DETECT** – using continuous monitoring to identify activities that may signal a targeted attack

Kaspersky Anti Targeted Attack Platform achieves extremely high detection rates because it receives real-time feeds from Kaspersky Security Network – based on the latest Global Security and Threat Intelligence.

Delivering a multi-layered, adaptive security strategy

Kaspersky Anti Targeted Attack Platform 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. The adaptive security approach protects businesses against most sophisticated threats, targeted attacks, new malware – including ransomware and crimeware – and Advanced Persistent Threats.

By correlating events from multiple layers – including network, endpoints and the global threats landscape – Kaspersky Anti Targeted Attack Platform delivers 'near real-time' detection of complex threats and helps to enable retrospective investigations.

ANALYSIS OF SUSPICIOUS OBJECT PAYLOADS – AND APT DISCOVERY

To perform multi-layered analysis of objects, Kaspersky Anti Targeted Attack Platform includes:

- Network Sensors that monitor network traffic – to enable detection of cyberattack indicators
- Email Sensors that exfiltrate potentially harmful objects from email attachments
- Web Sensors that exfitrate objects from Web traffic using ICAP protocol
- Advanced Sandbox technology that provides an isolated, virtualized environment where suspicious objects from Network, Email and Web sensors - as well as the artifacts they produce - can be dynamically studied
- The data from Network and Endpoint Sensors are then combined and compared with the 'baseline picture' by the Targeted Attack Analyzer – in order to discover suspicious activities and help provide your security team with timely and accurate alarms.

The Advanced Sandbox is equipped with several technologies that prevent malware from detecting that it is running in a sandbox – so the malware can't automatically shut itself down and avoid revealing data about its activities.

MONITORING ABNORMAL AND SUSPICIOUS BEHAVIOR

To perform advanced network behavior analysis, Kaspersky Anti Targeted Attack Platform includes:

- Endpoint Sensors (lightweight agents) that collect information about network-active processes that are running on the business's endpoints
- Network Sensors that intercept raw IP traffic and Internet activities – to exfiltrate metadata
- A Targeted Attack Analyzer that builds an understanding of normal behavior patterns and then – by monitoring network sensor metadata and data received from the endpoint sensors – can detect anomalies and deviations on the business's network

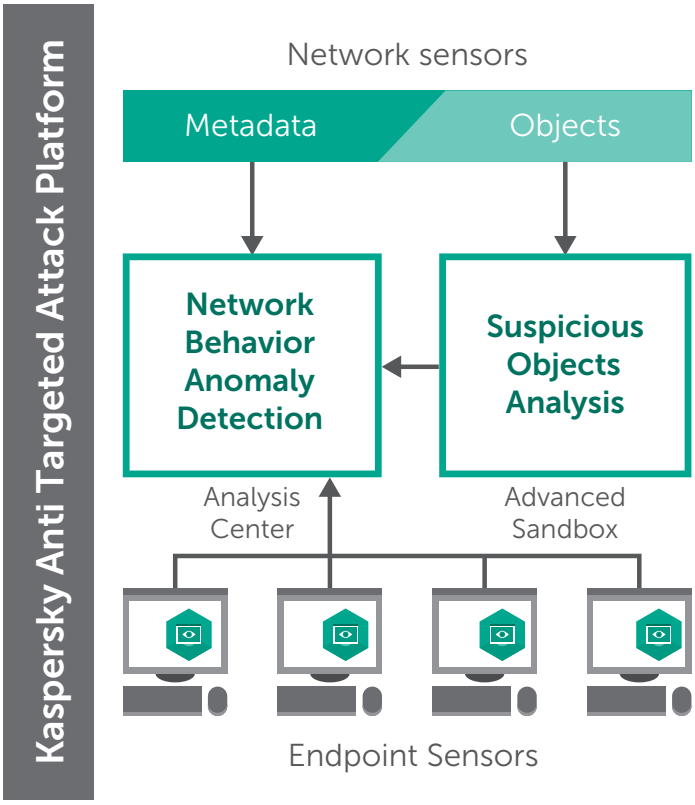
EASY TO USE... AND TO MANAGE

The Targeted Attack Analyzer receives data from Network and Endpoint Sensors – to perform in-depth analysis and provide detection verdicts. All detection verdicts are stored – for use during post-attack investigations.

A dashboard – featuring convenient output filtering – gives 'at-a-glance', detailed information on activities and potential issues... to help businesses achieve earlier discovery of security incidents. Furthermore, to assist with incident response and post-attack investigations, detailed logs of alerts are recorded for analysis within Kaspersky Anti Targeted Attack Platform. Incident logs Logs can also be forwarded to the customer's SIEM system.

TARGETED ATTACK INCIDENT RESPONSE SERVICE

When Kaspersky Anti Targeted Attack Platform identifies that a business is under attack, Kaspersky Lab security experts can offer a full Incident Response Service – to analyze the attack and help with remediation. The Incident Response Service can cover everything from initial assessment of the incident... through to evidence collection, forensic analysis and the submission of a detailed investigation report and a remediation plan.



TARGETED ATTACK DISCOVERY SERVICE

Because Kaspersky Lab understands that small businesses can sometimes be subjected to attacks that can stay active for a very long time – and remain relatively undetectable – the company also offers a dedicated Targeted Attack Discovery Service. This service delivers a single audit – without any requirement to buy any targeted attack detection products.

In addition, Kaspersky Lab security experts offer Penetration Testing Services, Application Security Assessment Services and Cybersecurity Training Services – to help ensure businesses are better placed to deal with future attacks.

Kaspersky Anti Targeted Attack Platform/Jan 2016/Global