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.