**Kaspersky®
Anti Targeted
Attack Platform**

Cybersecurity risk mitigation in an era of digital transformation

Corporate security should act as a catalyst for accelerated innovation, a cornerstone of your digital business strategy, proactively identifying and mitigating risk and reducing the impact of digital disruption in alignment with your overall business vision. Where cybersecurity is still viewed as a necessary burden and a potential progress inhibitor rather than a nurturer of corporate growth, Kaspersky Lab can help transform expectations.
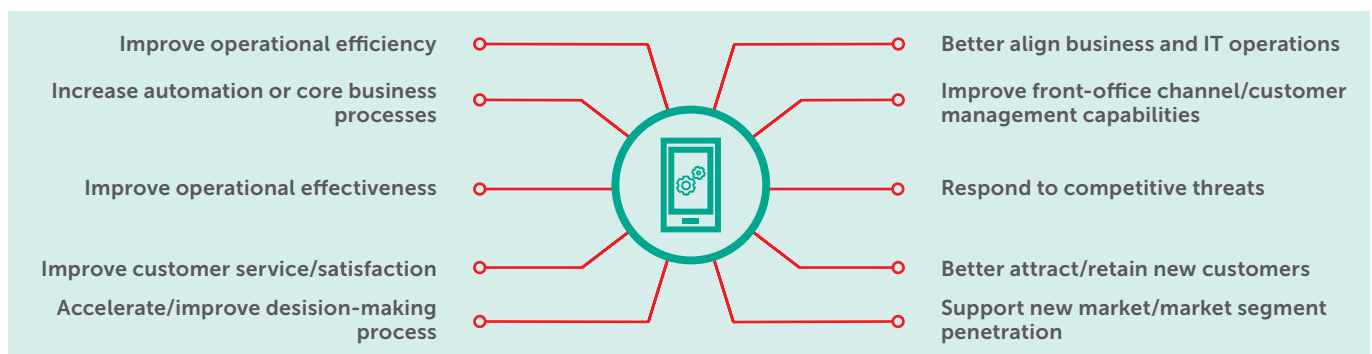
A strategic approach to advanced enterprise security

Kaspersky Anti Targeted Attack Platform delivers a new, strategic approach to detecting targeted attacks. Complemented by our multi-layered prevention technologies and solutions, as well as an extensive portfolio of Security Intelligence Services for response and prediction, Kaspersky Lab delivers a truly integrated, strategic approach to targeted attacks and to threat detection and response.

A corporate cybersecurity strategy to meet digital disruption challenges

With the increasing adoption, throughout business and society at large, of digital technologies such as the cloud, big data, mobile, IoT and artificial intelligence, the growing connectivity of everything brings challenges as never before in terms of security, compliance and data protection.

Business goals of Digitalisation

Improve operational efficiency

Increase automation or core business processes

Improve operational effectiveness

Improve customer service/satisfaction

Accelerate/improve desision-making process

Better align business and IT operations

Improve front-office channel/customer management capabilities

Respond to competitive threats

Better attract/retain new customers

Support new market/market segment penetration

Digital transformation – a new role for cybersecurity

Cybersecurity, along with compliance and data usage, has become a key strategic priority for digital business. Organisations are looking for security approaches that facilitate a clear focus on business needs.

A trusted security solution delivering complete privacy

All object analysis is performed on-site, with no outbound data flow, and the Kaspersky Private Security Network delivers real-time inbound reputation updates while preserving the full isolation of corporate data.

A unified solution to accelerate innovation in digital transformation

- **Integral business continuity**, achieved through building security and compliance into new processes right from inception
- **Visibility** over shadow IT and hidden threats
- **Maximum flexibility** enabling deployment across both physical and virtual environments, wherever visibility and control is needed
- **The automation of investigation and response tasks**, optimising the cost-effectiveness of your security, incident response and SOC teams
- **Tight, straightforward integration** with existing security products, enhancing overall security levels and protecting legacy security investment

Proven to be the industry's most effective solution


ICSAlabs CERTIFIED ADVANCED THREAT DEFENSE

In independent tests, Kaspersky Anti Targeted Attack platform has been found to deliver 100% detection rates, with a 0% false positive rate, eliminating the need to waste time responding to false alarms. ICSA, q3 2017

How it works

«The Kaspersky Anti Targeted Attack Platform provides advanced threat detection across all layers of a targeted attack – initial infection, command and control communications, and lateral movements and data exfiltration» – a competitive analysis of Advanced Persistent Threats (APT) protection by Radicati Group 2017.

Automated aggregation of essential telemetry and data across the entire network
The platform leverages network and endpoint data to deliver complete visibility across distributed enterprise networks for early threat detection and comprehensive response. Objects can be collected through SPAN, ICAP, POP3S or SMTP. Suspicious objects can also be extracted from third party systems' custom connectors.
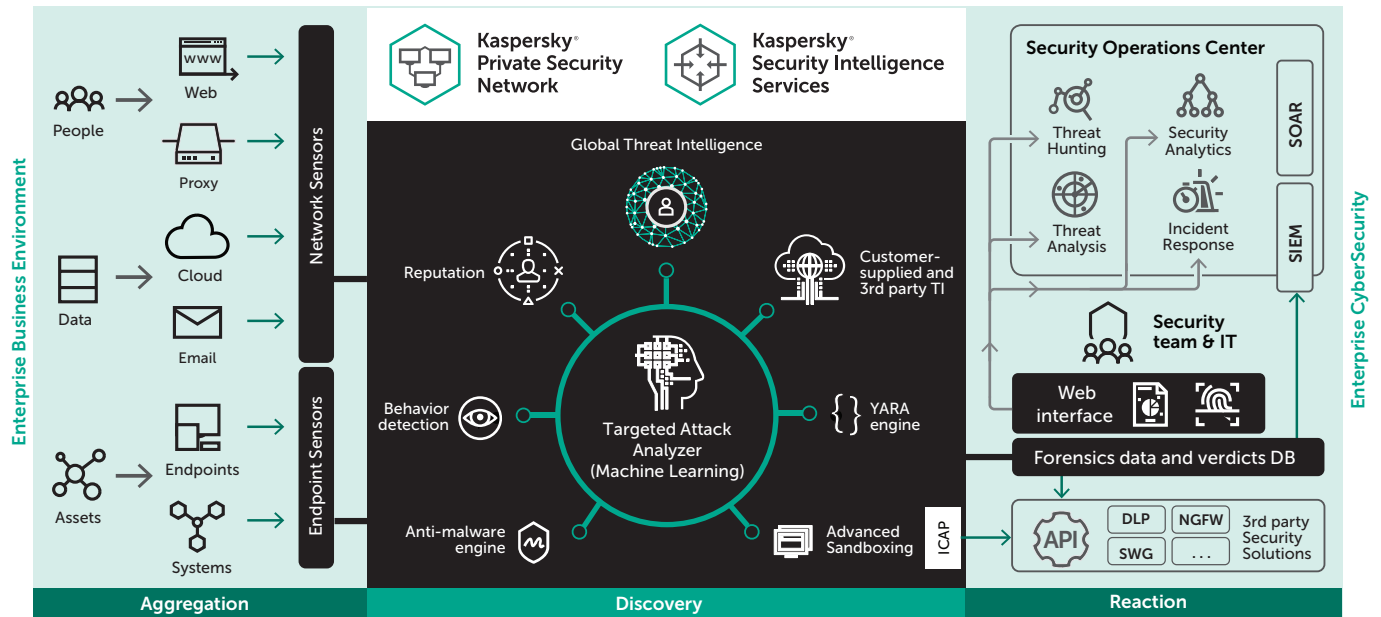
## Integrates with existing enterprise security

Existing security solutions can be fed with new context and verdicts for blocking. Blocking rules can be sent to Next-Generation Firewalls (NGFWs), breach event data sent to your Security Information Event Management system (SIEM) and unique URL and Domain insights added to Secure Web Gateways (SWGs).

Multi-dimensional advanced detection
Based on leading security intelligence and advanced machine learning technologies, the Kaspersky Anti Targeted Attack Platform combines network and endpoint data, sandbox and intelligent analysis to correlate incidents, search for Indicators of Compromise and help uncover the most complex targeted attacks. Connecting up the various pieces of an incident provides a comprehensive view of the entire attack chain, increasing confidence in assigned threat scores and reducing false positives to zero.

Automated prevention of advanced threats and comprehensive response
The Kaspersky Anti Targeted Attack platform can automatically share verdicts with traditional security Kaspersky Lab solutions via an on-premise intelligence sharing layer – Kaspersky Private Security Network. This tight integration from global to network to endpoint level, between Kaspersky Anti Targeted Attack Platform, Kaspersky Security for Mail Gateway, Kaspersky Endpoint Security, Kaspersky Security for Virtualization and Kaspersky Endpoint Detection and Response, means immediate, informed action can be taken when an incident emerges.
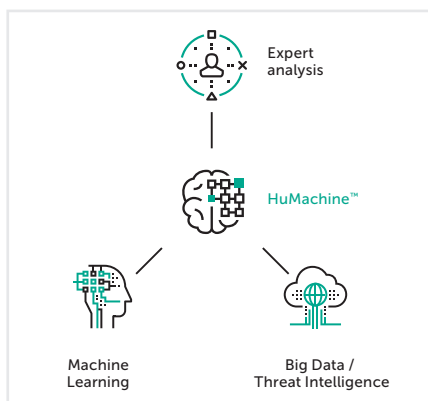
Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com

Proven. Transparent. Independent.