KASPERSKY lab

ENTERPRISE SECURITY GETS ADAPTIVE

Today's threat landscape was unimaginable a decade ago. Cybercriminals have adapted their techniques to sidestep traditional defenses and lurk undetected on systems for months or even years. It's time for enterprise security to adapt with an intelligence-driven, multi-layered approach to IT security.

"Intelligence is the ability to adapt to change."
– Stephen Hawking.

ENTERPRISE SECURITY GETS ADAPTIVE

Advanced Persistent Threats (APTs), sophisticated malware and targeted attacks are just some of the new, constantly evolving threats the enterprise faces. Cybercriminals are only too aware of the limitations of traditional, perimeter-based security – it's their first port of call when they're looking for chinks in the enterprise armor.

If the attackers are constantly shape-shifting, it's fair to say that multiple enterprise technologies provide a convenient support network of attack vectors: mobile devices, web applications, portable storage, virtualization, cloud-based technologies all present a window of opportunity to cybercriminals that traditional 'prevent and block' security alone cannot answer.

A new, more adaptive, integrated approach built on the pillars of prediction, prevention, detection and response is needed.

THE FOUR PILLARS OF ADAPTIVE ENTERPRISE SECURITY

Prediction: No one has a crystal ball, but enterprises with access to the latest threat intelligence and trends are better placed to anticipate – and avoid – incidents. Training employees to recognize the tactics used in attacks augments predictive analysis, as does the ability to learn from mistakes by forensically analyzing breaches; penetration testing, meanwhile, can help expose the weak spots.

Prevention: A key goal here is to reduce attack surface – be it traditional, signature-based anti-malware, device controls or patching application vulnerabilities – hardening systems and placing as many obstacles in the way of attackers as possible are just two components of an over-arching approach that includes limiting the ability of attacks to spread and reduce their impact.

Detection: As Kaspersky Lab research into high-profile APTs shows, sophisticated attacks can go undetected for years. It's estimated that the average enterprise attack goes undetected for over 200 days[1]; the sooner any incident is discovered, the better. Detection technologies underscored by the best threat analysis augments discovery: as threats evolve at pace, the best detection strategy is often built on the ability to spot behaviors and sequences of events that suggest a breach has taken place.

Response: Effective enterprise security has the capacity to respond to and mitigate the effects of a breach. At one level, this can involve "If/then" policy for procedures that can be automated, such as patching. At another level, this could include post-breach analysis or the use of specialized incident-response teams to stop, mitigate and investigate attacks, breaches and other security incidents.

To be truly effective, each of these capabilities must work together as a multi-layered system. Intelligence-driven, threat focused, integrated, holistic and strategy-driven: these are the key characteristics of a comprehensive, adaptive enterprise security architecture. Kaspersky Lab is uniquely placed to deliver an adaptive enterprise security platform, let's take a look at some of the elements.

[1] https://www.siliconrepublic.com/enterprise/2014/04/11/advanced-cyberattacks-can-go-undetected-for-typically-229-days

ENTERPRISE SECURITY. POWERED BY INTELLIGENCE.

Kaspersky Lab has a long track record in making some of the highest profile, most relevant threat discoveries, including:

- Carbanak: the world's biggest cyber bank heist
- Dark Hotel: which specifically targets senior-level business travelers
- The Mask/Careto: which targeted enterprises, governments and private equity firms, among others
- Wild Neutron: targeting global enterprises and other businesses
- Icefog: attacked the supply chain for businesses
- Red October: exploited enterprise systems to conduct mass surveillance operations

More than a third of our employees work in research and development, focusing solely on developing technologies to counteract and anticipate the constantly evolving threats Kaspersky Lab's dedicated teams of Intelligence and Analysis Researchers investigate every day.

Kaspersky Lab's understanding of the inner workings of some of the world's most sophisticated threats has enabled us to develop a multi-layered, strategic portfolio of security 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.

PREDICTION

Prediction capabilities – and the mitigation strategies that are built around them – are central to everything Kaspersky Lab does, from our dedicated Global Research and Analysis Team (GReAT) to Kaspersky Security Network (KSN) and our Security Intelligence Services (SIS) portfolio:

Kaspersky Security Network: One of the most important components of Kaspersky Lab's multi-layered platform, Kaspersky Security Network is a cloud-based, complex distributed architecture dedicated to gathering and analyzing security threat intelligence from millions of systems worldwide.

Effectively a global, cloud-based threat laboratory, KSN detects, analyzes and manages unknown or advanced threats and online attack sources in seconds – and delivers that intelligence straight to customer systems. For enterprises with very specific data privacy concerns, Kaspersky Lab has developed a Kaspersky Private Security Network option.

Security Intelligence Services: Few organizations have the resources to develop the high levels of strategic security intelligence required to keep pace with constantly evolving, sophisticated threats. That's why Kaspersky Lab has developed an extensive portfolio of Intelligence Services:

Education and training: From more generalized cybersecurity fundamentals to advanced digital forensics, malware analysis and reverse engineering training, Kaspersky Lab provides comprehensive training and awareness programs to enterprises – both on-site and online. In addition to interactive games, skills assessments and general cyber safety promotion, courses of 2-5 days duration are also available, including some of the following topics:

- **Cybersecurity Fundamentals:** Understanding the threats, using technology safely.
- **General Digital Forensics:** Building a digital forensics lab, incident reconstruction, tools.
- **General Malware Analysis & Reverse Engineering:** Build a secure malware analysis environment, conduct express analysis.
- **Advanced Digital Forensics:** Deep file system analysis, recover deleted files, incident timeline reconstruction.
- **Advanced Malware Analysis & Reverse Engineering:** Analyze exploit shellcode, non-Windows malware, use global best practices.

Security Assessment:

- **Penetration testing:** Understanding infrastructure security from an attacker's perspective, while achieving compliance with security standards such as PCI DSS.
- **Application security testing:** Analysis of web applications (including online banking and ones with WAF enabled), mobile applications, fat clients

Threat Intelligence:

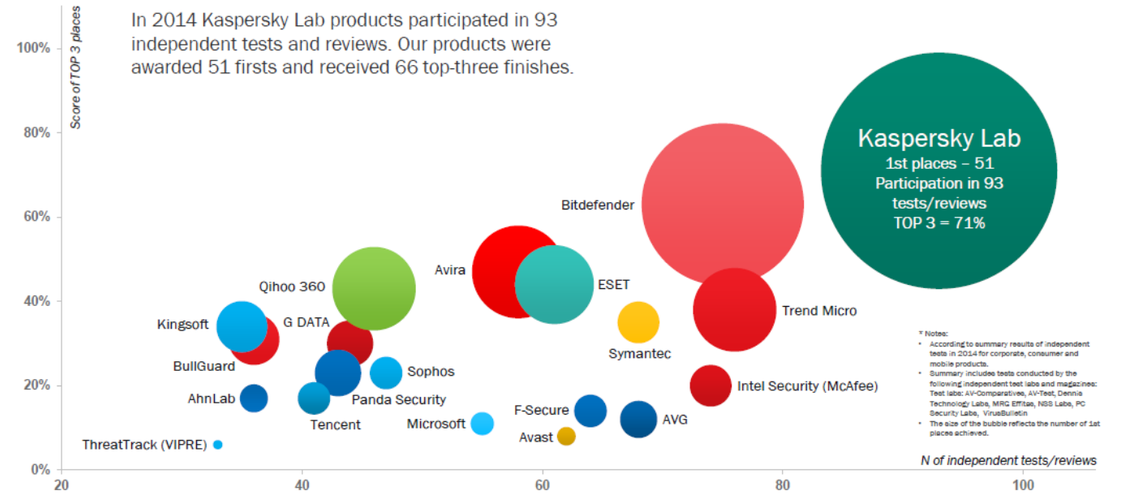
- An early warning system, driven by GReAT's expertise and supported by KSN, this includes threat data feeds, botnet tracking and intelligence reporting. Early access to APT-related configuration files and malware samples, along with integration with SIEM (HP Arcsight) help enterprises develop comprehensive intelligence insight.

PREVENTION

Kaspersky Lab detects 325 000 new pieces of malware *every single day*. Even a single additional percentage point in detection rate can translate into hundreds of thousands of pieces of malware being caught. Independent test results consistently demonstrate that Kaspersky Lab provides the best protection in the industry. In 2014 alone, we participated in 93 independent tests and reviews, ranking first 51 times and finishing in the top three a record 71% of the time.[2] That's just one of the reasons why OEMs – including Microsoft, Cisco Meraki, Juniper Networks and Alcatel Lucent -trust Kaspersky Lab to provide the security they ship within their own products.

[2] For more detail on the tests and the metrics, visit: http://media.kaspersky.com/en/business-security/TOP3_2013.pdf
New link for updated report is: http://media.kaspersky.com/en/business-security/TOP3_2014.pdf.

KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION*



Our Enterprise Security portfolio combines industry-leading anti-malware with multiple technologies to reduce attack surfaces in a unique combination of intelligence-led technologies.

Known, unknown and advanced threats are prevented using multiple protection layers, including:

Network Attack Blocker: Scans all network traffic using known signatures to detect and block network-based attacks, including port scanning and Denial of Service (DoS) attacks. For a further layer of protection, Kaspersky DDoS Protection (KDP) is available as a solution to protect against Distributed Denial of Service (DDoS) attacks. It's a comprehensive, integrated DDoS prevention and mitigation solution, that includes 24/7 analysis and post-attack reports.

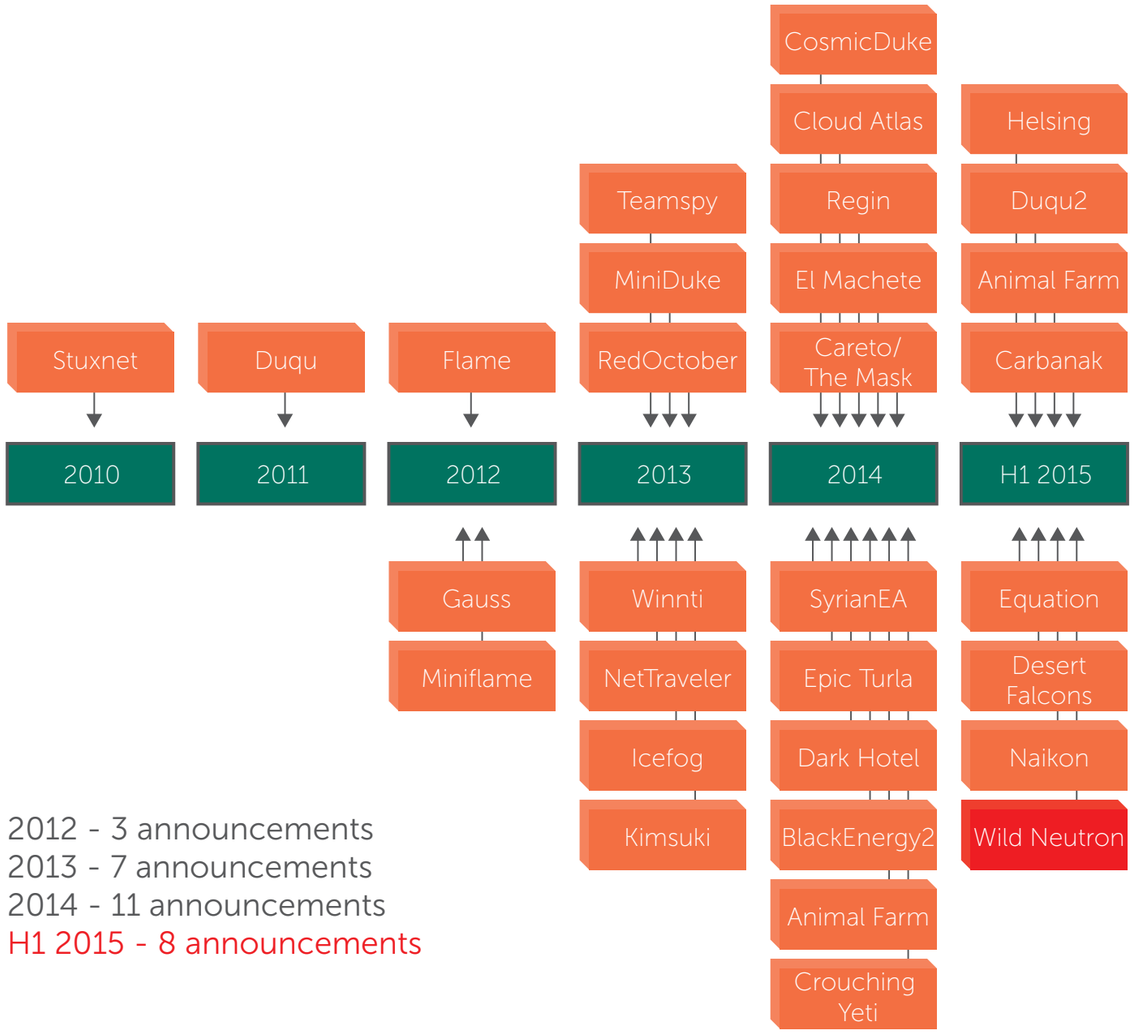
Heuristic anti-phishing: Capable of preventing some of the very latest phishing attack techniques by looking for additional evidence of suspicious activity, over and above traditional phishing database-led approaches. Application control and Dynamic Whitelisting: Application control blocks or allows administrator-specified applications. It's built on dynamic whitelisting, Kaspersky Lab's continuously updated lists of trusted applications and software categories.

Host Intrusion Prevention System (HIPS): Helps control how applications behave and restricts the execution of potentially dangerous programs without affecting the performance of authorized, safe applications.

DETECTION

Kaspersky Lab's unparalleled expertise in detecting some of the world's most sophisticated threats feeds directly into our enterprise threat detection capabilities. Since 2008, our researchers have uncovered some of the most sophisticated, multi-component attacks the world has ever seen. This insight and intelligence directly informs our product development; in addition to our capacity to detect sophisticated enterprise-focused attacks, Kaspersky Lab has used the insights gained from discovering significant financial threat actors such as Carbanak to develop solutions geared entirely towards detecting financial fraud.

APT ANNOUNCEMENTS KASPERSKY LAB



2012 - 3 announcements
2013 - 7 announcements
2014 - 11 announcements
H1 2015 - 8 announcements

RESPONSE

In an adaptive security architecture, the ability to respond to threats is as important as the capacity to predict and prevent them – saving the enterprise both time and money. It's also worth acknowledging the reality that a direct consequence of enhanced detection will be enhanced response capability. Kaspersky Lab addresses this at both the technology and services levels:

System Watcher: Kaspersky Lab's unique and proactive monitor is capable of reacting to complex system events, such as installation of drivers and detecting suspicious behaviour.

Investigation Services: Resolve live security incidents with Kaspersky Lab's help. From malware analysis to digital forensics, reporting and incident response, customers are empowered to learn from incidents while mitigating the impact of an attack and restoring damaged systems.

PROACTIVE, REACTIVE, INTELLIGENCE-DRIVEN ENTERPRISE SECURITY

To say malware has metastasized is something of an understatement: advanced threats evade traditional blocking techniques, ready-made malware kits can be bought for spare change online and tools capable of automatically creating multiple, tailored variants of a single piece of malware are just the tip of a massive malware iceberg.

An increasingly sophisticated and complex threat landscape calls for a multi-layered, adaptive security approach, in which a combination of integrated technologies provides comprehensive detection and protection against known, unknown and advanced malware and other enterprise-focused threats.

Kaspersky Lab's unparalleled track record in discovering the most sophisticated, relevant threats, combined with its industry-leading technologies and services mean it's uniquely placed to deliver the comprehensive, adaptive security enterprises need. While Kaspersky Security Network builds on the real-time intelligence generated by over 60 million nodes worldwide, our elite Global Research and Analysis Team contributes a unique set of skills and expertise to our threat research, developing solutions capable of combating increasingly complex and sophisticated threats.

TRUSTED PARTNER OF ENTERPRISES, GOVERNMENTS AND REGULATORS

Because it's privately owned, Kaspersky Lab is free to invest heavily in Research and Development outside short-term market constraints. Almost half of our 3000 employees globally work in our research and development labs, focusing on developing innovative technologies, investigating cyber-warfare, cyber-espionage and all types of threats and techniques.

This focus on high-quality, internal R&D has led to Kaspersky Lab being recognized as an industry leader in IT security technologies. That's just one of the reasons why over 100 leading OEMs – including Microsoft, Cisco Meraki, IBM, Juniper Networks and Alcatel Lucent – trust Kaspersky Lab to provide the security they ship within their own products.

It's also why we're a trusted partner of governments, law-enforcement agencies and large businesses all over the world. Respected international organizations, including INTERPOL, Europol and numerous CERTS have all invited Kaspersky Lab to collaborate and consult with them on an ongoing basis; in addition to holding regular training courses for INTERPOL and police officers of many countries, we supported the launch of INTERPOL's Digital Forensics Laboratory.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab