# Going beyond Next Gen Security

Is your business getting the protection it deserves?

www.kaspersky.com
#truecybersecurity

# Enterprises are under attack

Because there's so much money to be made from attacks against businesses, today's cybercriminals are highly skilled and very well-funded… and that makes them an even bigger threat to enterprises.

Cybercriminals are running efficient organizations that have the resources to develop increasingly sophisticated threats that can:

- Defraud enterprises
- Steal valuable intellectual property
- Disrupt day-to-day business operations
- Steal confidential information about customers
- Hold businesses to ransom – by encrypting and 'locking up' essential data

**Data security is a major concern for enterprises – and it's also a focus for regulators.**

The average financial impact of a single data breach at an enterprise is

**$992,000**

Source: Kaspersky Lab survey

## The scale of the problem

Every day, we identify an average of 360,000 new items of malware.

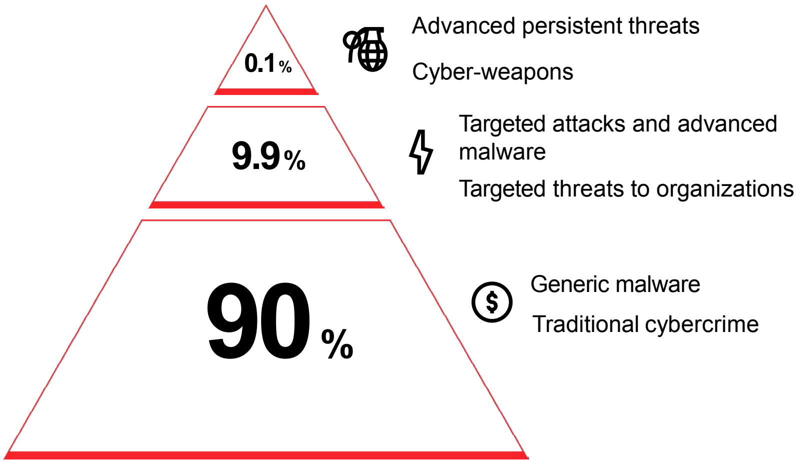
That's a massive 131,400,000 new threats per year… and any one of those threats could be the attack that slips through an enterprise's defenses, resulting in:

- Direct financial losses – from the actions of the attack itself
- Damaging publicity and loss of business reputation – that could take years to recover from
- Financial and legal penalties – imposed by regulatory bodies
- Indirect financial losses – owing to the costs to recover systems and data to their pre-attack state

The volume of the threats is enough to cause headaches for IT and security teams… but, if we add in the possible financial and reputational damage – from just one successful attack – it's clear that cybersecurity has become a much bigger priority for all businesses.

## The range of today's threats

Within this vast volume of threats, there's a variety of types of attack that can strike at the heart of the corporate network.



## Common Threats

The most common threats are classed as Mass Malware – which accounts for 90% of all cyberthreats. These may not be the most sophisticated threats, but the sheer volume of Mass Malware brings its own risks for the enterprise.

Security measures have to be capable of dealing with both volume and variety. Effective defense depends on the ability to detect as many of these threats as possible – and then block them.

## Sophisticated Threats and Targeted Attacks

Whereas Mass Malware often uses a 'scatter gun approach' – indiscriminately attacking any business or individual – some 9.9% of all threats will deliberately target a specific victim.

These attacks are usually much more difficult to deal with. The cybercriminal will have carefully chosen their target. Attackers will have specific objectives in mind… and they may use several different techniques – coupled with human ingenuity – to try to achieve their malicious goals.

**Modern IT environments bring additional risks**

The growing complexity of most corporate IT networks can create 'visibility gaps'. Unfortunately, threats can often hide inside these gaps.

On average, a Targeted Attack can continue to lurk within the target business's systems – totally undetected – for 214 days.

During that 214-day period, the threat could be continuing to perform a range of malicious activities… such as stealing sensitive corporate data or confidential information about customers. So, it's vitally important that businesses use efficient tools that can rapidly **detect, remove and remediate**.

Source: Kaspersky Lab survey

## Advanced Persistent Threats

At the top of the pile are Advanced Persistent Threats (APTs). Accounting for just 0.1% of all threats, APTs are obviously only a small fraction of the total number of attacks. However, they're the threats that can inflict the most damage on an enterprise.

A successful APT attack can lead to very significant financial losses – both from the attack itself and the subsequent 'clean up' operations.

In general, advanced threats call for advanced defenses – and that's one of the reasons why more enterprises are re-evaluating their current security provisions.

# Cybercrime-as-a-Service

Cybercriminals are also acting as 'guns for hire' – selling cybercrime services to unscrupulous businesses that are keen to damage their competitors' operations.

In recent years, the cost of launching an attack has fallen – so Cybercrime-as-a-Service attacks are on the increase… and they're easier to arrange than you might think.

Just as a business might get quotations from three or four suppliers, whenever it's buying a typical business-to-business service – such as office cleaning or the outsourcing of catering operations in the staff canteen – it's now easy for devious businesses to obtain quotes for a range of disruptive activities… that their chosen cybercrime supplier will use to attack a specific target, over a specified period.

**Early detection of a security incident helps to cut the cost of recovery**

A recent survey of security breaches within enterprises measured how recovery costs can grow if threat detection is delayed.

Source: Kaspersky Lab survey

# Is there a simple solution?

Sadly, despite some vendors' grandiose claims, there is no Silver Bullet security solution that can guarantee 100% protection against every threat. Because there's such a wide range of threats, there isn't one single protection technology that will protect against all types of risk.

Similarly, security isn't one of those issues that has a 'one-time fix'. For all businesses, IT security is a constant process of evaluating how the dangers have evolved and then:

- Adapting & updating security policies and
- Rolling out new security technologies
  … to deal with new risks.

The cybercriminals are constantly innovating… so your business needs to make sure its defenses are keeping pace with the evolving threat landscape.

**Early detection of a security incident helps to cut the cost of recovery**

A recent survey of security breaches within enterprises measured how recovery costs can grow if threat detection is delayed.

| Time to detect incident | Cost of recovery<br>(from a single incident) |
|---|---|
| Almost Instant Detection<br>(Using automated detection solution) | $392,984 |
| Detection within a few hours | $555,274 |
| Detection delayed by over a week | $1,092,303 |

Source: Kaspersky Lab survey

**Vulnerability dangers**

In 2017, WannaCry ransomware caused havoc for both businesses and public-sector organizations – including parts of the UK's National Health Service (NHS).

On the first day of the attack, WannaCry was found in 74 countries.

Wannacry exploited a known vulnerability within some Microsoft software. It encrypted the victim's data and the attacker then demanded payment of a ransom.

**If the victims had applied the latest patches to their Microsoft software – prior to the attack – Wannacry would have had no 'entry point'… and the victim would not have been attacked.**

# How the attacks strike

The majority of attacks have four distinct stages:

- **DISCOVERY** – to identify entry points for the attack
- **INTRUSION** – into an endpoint on the corporate network
- **INFECTION** – often spreading to many locations on the corporate network
- **IMPLEMENTATION** – of the cybercriminal's malicious actions

## Stage 1

During the DISCOVERY stage, the attacker may use a variety of techniques, including:

- Phishing emails
- Infected email attachments
- Social engineering

However, one of the most common methods is to exploit unpatched vulnerabilities within the operating systems – or any of the applications – that the enterprise is running.

Whichever method the attacker uses, the cybercriminal's objective is to gain entry into the enterprise's corporate network.

## Stage 2

Now the attacker will deliver malicious code onto one or more of the enterprise's endpoints. These could be any of the enterprise's:

- Servers
- Desktops
- Laptops
- Mobile devices – including tablets and smartphones

Laptops and mobile devices – that are used both inside and outside the corporate network – can add to the enterprise's security challenges… because simply defining and defending a perimeter around the enterprise's corporate systems is no longer a valid form of defense.

Today's perimeters are more 'fluid' – so the security solutions have to be more flexible in their approach.

## Stage 3

The malicious code infects the selected endpoint – and often tries to spread to other systems on the corporate network.

## Stage 4

The infection now performs the malicious actions intended by the attacker. These could include:

- Stealing data
- Overloading Web servers – to ensure the enterprise's website crashes… so customers can't access information, order goods & services or process payments
- Encrypting corporate data – so the attacker can demand the payment of a ransom, in exchange for unlocking the enterprise's data.

# Stage-by-stage defense

One of the keys to dealing with an attack is to have defenses that are capable of providing protection at each of the four stages of the attack.

| Attack Stage | Defense Stage |
|---|---|
| DISCOVERY | EXPOSURE PREVENTION<br>To block access to potential entry points |
| INTRUSION | PRE-EXECUTION PROTECTION<br>To detect threats before they can cause infections |
| INFECTION | POST-EXECUTION PROCESSES<br>To detect suspicious behavior – and help prevent the infection performing malicious actions |
| IMPLEMENTATION | AUTOMATED RESPONSE<br>To help the victim business to recover systems and data – plus identify how to avoid similar attacks in the future |

Some security solutions build further on this concept – by including multiple defense technologies within each of the four defense stages – so, in effect, there are multiple layers of defense for each stage of the attack.

## How many layers of security do you need?

With budgets under pressure, it's always worth considering whether there are very low-cost solutions for any IT or security issue. This can lead businesses to consider very simple security that has very few layers of defense… and with one of the layers being provided by free or 'bundled' software:

**One layer** may be an antivirus application that is already included as part of another software package that's being used by the business – or could be a free antivirus product. The aim is to use this layer to defend against Mass Malware.

**Another layer** will require investment in specialist technology that can defend against Targeted Attacks and APTs.

Unfortunately, this approach will usually have major flaws:

- Free or bundled antivirus software will protect against some Mass Malware. However, it's unlikely to achieve the industry's highest levels of threat detection – so it's likely that more threats will slip through the business's defenses. The quality of the technologies within each layer will have a major effect on the number of threats that are successfully blocked.
- In addition, free or bundled software may include little or no automation for recovering data and systems after an infection. Instead, following an attack, the business may be left facing delays and substantial costs associated with manual recovery processes.
- There's likely to be no interaction between the layers – so there'll be no opportunity for the security to perform complex behavior analysis that's based on monitoring events acrossdifferent layers. Again, this limitation will hamper the solution's ability to identify some threats.

So, a simple model that has very few layers – and uses bundled or free software – may save a small amount on the IT and security budget. However, it won't offer the most effective security… so it's likely to be a 'false economy' – as the cost of attacks against the business can far outweigh any budget savings.

## Quality really counts… within each layer of protection

Even for the least sophisticated threats – Mass Malware – it pays to select the most efficient protection technologies.

Despite what some vendors may claim, anti-malware is not a commodity item. Yes, anti-malware is an established technology – but it's not a case of '*any vendor's anti-malware is as good as any other vendor's anti-malware*'.

For example…

At first sight, the difference between a product that stops 99.1% of malware and one that stops 99.7% of malware may seem very small. After all, that's only a 0.6% difference. However, if there are 360,000 new items of malware being found every day… that 0.6% difference in malware detection & blocking means that the product that is only 99.1% effective is potentially letting 2,160 more malicious software programs slip through onto the business's systems… **every day**.

Over a period of one year, that's an extra 707,370 malware items that the business could be subjected to… and all for the sake of a 0.6% difference in anti-malware performance. Faced with that unnecessary level of additional risk, it could be just a matter of time before one of those malware items causes serious damage to the business.

That's a compelling reason for taking care over the selection of every layer of defense… even the layer that protects against relatively simple Mass Malware.

## Look for true integration

It's worth noting that some vendors may provide products that include multiple layers of security – but not as part of a fully integrated solution. This can cause security management issues.

Some vendors add new technologies by acquisition. Instead of developing the technologies in-house, they'll simply buy other security vendors, in order to access new protection technologies.

In these cases, a lack of proper integration within the vendor's product is likely to mean that your IT security team will be faced with having to use multiple security management consoles. Furthermore, there may be operability issues.

Always try to look beyond a vendor's claims about integration – to check whether the true level of integration is just superficial. It's a question of making sure that management and operability issues have been fully thought out by the vendor.

By definition, any security solution that delivers multiple protection technologies that are all built into a single agent… is likely to offer much higher levels of integration – and higher levels of interoperability across each protection technology. This helps enterprises to save time, save money and avoid security errors.

## The limits of multi-layered security solutions

We've seen that:

The more layers of security technologies that your security solution delivers…
… the more effective your defenses.

Plus, we've established that each layer should contain best-of-breed versions of each technology.

However, there's yet another factor that can help you to defend against a greater number of threats.

### Correlation… to help boost detection

The best security solutions don't just give you multiple layers of protection. They also have the ability to assess what's happening within each of those defense layers – and to correlate findings from the various different layers. This can help solutions to identify Targeted Attacks and APTs that other security products may totally miss.

Many threats can evade one or two types of protection technologies. In those cases, you hope that another of your defense layers will be successful in stopping the threat.

But what about those particularly cunning threats that can slip through every individual layer of defense? For those threats, their activities may appear to be perfectly innocent – when each individual layer assesses them. In these cases, a pattern of suspicious behavior is only identified if your security solution has some way of 'adding together' the seemingly innocent activities that have been noted by various layers of defense… and then automatically working out that these individual events add up to something sinister.

### Adding a Meta-Layer… that 'sees' all other layers of security

These security solutions will generally use a Meta-Layer of protection that's capable of assessing the outputs of multiple individual layers of defense. By correlating events from the various security layers, the Meta-Layer will do more to spot threats that could have slipped through all of the individual defense layers.

Not all multi-layered security solutions have this ability.

# Enterprise-grade security... from Kaspersky Lab

To help enterprises defend their operations against today's:

- Mass Malware
- Targeted Attacks
- Advanced Persistent Threats
  ... Kaspersky Lab delivers one of the industry's most comprehensive portfolios of technologies and services.

We can help enterprises to protect every endpoint, including:

- Windows Servers
- Linux Servers
- Virtual machines, including:
  - Virtual Servers
  - Virtual Desktop Infrastructure (VDI)
- Desktops & laptops, including:
  - Windows PCs
  - Mac computers
- Tablets and smartphones, including:
  - Android devices
  - iOS devices (iPad and iPhone)

Plus we offer specialist security for:

- Internet gateways
- Mail servers
- Microsoft SharePoint collaboration environments
- Network attached storage (NAS)
- Protection against DDoS attacks
  ... and more.

## Integrated technologies deliver better security

All of our core security technologies have been developed by our own, in-house security experts – and those technologies are part of a single agent.

This helps to eliminate technology integration issues, so our customers benefit from more efficient protection.

## Smoother & faster security management

Because the vast majority of our security technologies can be managed via a single management console – Kaspersky Security Center – it's faster and easier for our customers' security teams to apply security policies across all endpoints... including servers, desktops, laptops, virtual machines and mobile devices.

There's no need for administrators and security personnel to keep switching between multiple consoles – to set up different layers of protection technologies. Kaspersky Security Center provides a single, unified management console that gives administrators a 'single pane of glass' view of all core Kaspersky Lab security technologies and functions.

## Multi-layer protection... from a single solution

We provide defenses for every stage of an attack – and at each stage, we don't just deliver one layer of defense, we provide multiple defense techniques... so our customers benefit from multi-layered protection at every stage of an attack.

### Defense Stage 1 – Exposure Prevention

We help to block attacks at potential entry points.

Our protection layers include:
- Network filtering
- Cloud-enabled content filtering
- Port controls

### Defense Stage 2 – Pre-Execution Security

We help to stop the 'intruder' from launching.

Our protection layers & services include:
- Endpoint hardening
- Reputation services
- Pre-execution detection – based on Machine Learning

### Defense Stage 3 – Runtime Control

We proactively look out for suspicious behavior on any devices attached to your corporate network… including your employees' own mobile devices.

Our protection layers include:
- Behavioral analysis – based on Machine Learning – including:
  - Exploit prevention
  - Ransomware protection
- Execution privilege control

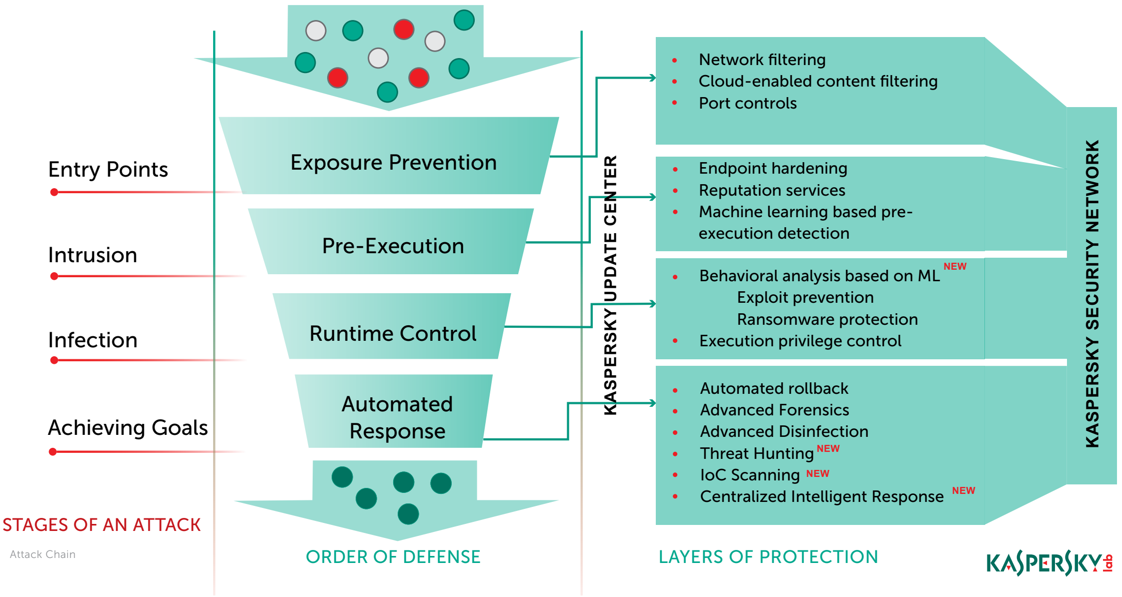
### Defense Stage 4 – Automated Response

If your business has suffered an attack, we help you to deal with the aftermath of an attack… more rapidly.

Our technologies and services include:
- Automatic rollback – to help restore systems to their pre-attack state
- Advanced forensics
- Advanced disinfection
- Threat hunting
- Incident of Compromise (IoC) scanning
- Centralized intelligent response

… and our special Meta-Layer boosts protection – by correlating the findings of individual defense layers… to identify threats that may be capable of slipping through individual defenses.

The Meta-Layer helps enterprises to do more to protect against dangerous Targeted Attacks and APTs.



- Network filtering
- Cloud-enabled content filtering
- Port controls

- Endpoint hardening
- Reputation services
- Machine learning based pre-execution detection

- Behavioral analysis based on ML NEW
  - Exploit prevention
  - Ransomware protection
- Execution privilege control

- Automated rollback
- Advanced Forensics
- Advanced Disinfection
- Threat Hunting NEW
- IoC Scanning NEW
- Centralized Intelligent Response NEW

## Next Gen security... and beyond

For many years, we've been pioneers in the development of many of the technologies that are now classed as Next Gen Security. Our first forays into Machine Learning (ML) date back to 2008 – when we used these techniques within our own malware discovery lab.

Since 2008, we've continued to develop new Machine Learning techniques – later using them to power specialist Next Gen technologies, such as:

- Advanced, ML-based pre-execution threat prevention
- Suspicious behavior prevention – based on Deep Learning
- Fileless attacks and exploits prevention
- Heuristic and emulation engines
- Ransomware protection mechanisms
- Automated rollback system
- Application isolation – execution privilege control
- Cloud-assisted protection
- Advanced Application Control, with dynamic whitelisting
- Advanced Disinfection

  ... that are built into the security solutions that run on our customers' own systems.

## A track record that others can't match

33% of our 2,500 employees are Research & Development specialists – including over 40 of the world's leading security experts. That's why Kaspersky Lab has been credited with discovering more of the world's most dangerous attacks than any other single security vendor.

Our major discoveries include:

- Cyberespionage malware:
  - Flame
  - Gauss
  - Sofacy
  - Project-Sauron

- Cyberespionage campaigns:
  - Red October
  - Careto / The Mask

- Complex cyberattack platforms:
  - Regin
  - Equation
  - Duqu 2.0

- Cyberespionage & sabotage – financial attacks:
  - Lazarus

- Cybercriminal operation:
  - Lurk

**Recognized for protection performance**

Kaspersky Lab security technologies are the world's most tested and most awarded.

Our security products successfully combine high detection rates and low 'false positives' – and that helps us to win so many awards.

In 2017, Kaspersky Lab products participated in 86 independent tests and reviews*. Our products achieved:

- 72 first places
- 78 top-three finishes

## Dedicated to customer satisfaction

In the 2017 Gartner Peer Insights Customer Choice Awards in Endpoint Protection Platforms, we were the only vendor to achieve a Platinum Award[1].

The Gartner Peer Insights initiative gave business customers an opportunity to rate how their chosen security vendor had been performing. That's why we're so proud to have been singled out to receive the highest level of award.

In addition to winning the Platinum award… 2017 also saw Kaspersky Lab being named as a Leader in Gartner's Magic Quadrant[2] – for the sixth time.

Finally, Kaspersky Lab endpoint solution's leadership is recognized by leading global analysts:

- Ovum Decision Matrix: Selecting an Endpoint Protection Solution, 2017 (Market Leader).
- IDC MarketScape – Worldwide Mobile Threat Management Security Software 2017 Vendor Assessment (a Major Player)
- The Forrester Wave™: Endpoint Security Suites, Q4 2016 (A Leader).

## Designed for enterprises

### Enterprise-level scalability

Kaspersky Endpoint Security – one of our core protection products – is easy to scale. Up to 100,000 physical, virtual and cloud-based endpoints can be managed through a single server installation of Kaspersky Security Center.

### Integrated Endpoint Detection and Response (EDR)

Because Endpoint Detection and Response is a vital element in any enterprise's security strategy, Kaspersky Endpoint Security includes built-in sensors… so it can send data – that's gathered from endpoints – directly to EDR systems.

Furthermore, Kaspersky Endpoint Security includes full native integration with our own EDR solution – Kaspersky Endpoint Detection and Response – so, Kaspersky Endpoint Security can also be used as a response agent to support incident response teams.

### High-performance security… with a low-footprint

Kaspersky Lab's development teams are constantly refining our security technologies – to deliver protection that puts less load on our customers' computing resources. The latest version of Kaspersky Endpoint Security can use as little as 100 MB of memory (RAM).

In addition, a special Cloud AV Mode helps to reduce resource usage even further:

- Enabling light detection databases – which reduce traffic for day-to-day updates, by up to 45%
- Cutting RAM consumption by 10%
- Reducing installation package size by 50% – to help enable rapid deployment

* https://www.kaspersky.com/top3

[1] The Gartner Peer Insights Customer Choice Logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customer Choice Awards https://www.gartner.com/reviews/customer-choice-awards/endpoint-protection-platforms are determined by the subjective opinions of individual end-user customers based on their own experiences, the number of published reviews on Gartner Peer Insights and overall ratings for a given vendor in the market, as further described here and are not intended in any way to represent the views of Gartner or its affiliates.

[2] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

**Discover True Cybersecurity**

We believe that True Cybersecurity doesn't just prevent IT security incidents… it also:

- Predicts security issues
- Detects threats
- Responds to security problems

For more information about how we deliver True Cybersecurity for enterprises – please visit https://www.kaspersky.com/true-cybersecurity

### Simplified user interface – makes sophisticated security easy to monitor and manage

Our latest user interface helps to give administrators an 'at a glance' overview of the security status of endpoints… and the performance of all of the Next Gen Security functions within Kaspersky Endpoint Security, including:

- Threat Protection
- Exploit Prevention
- Behavior Detection

… and more.

The vast majority of Kaspersky Endpoint Security applications can be controlled via a single, unified management console.

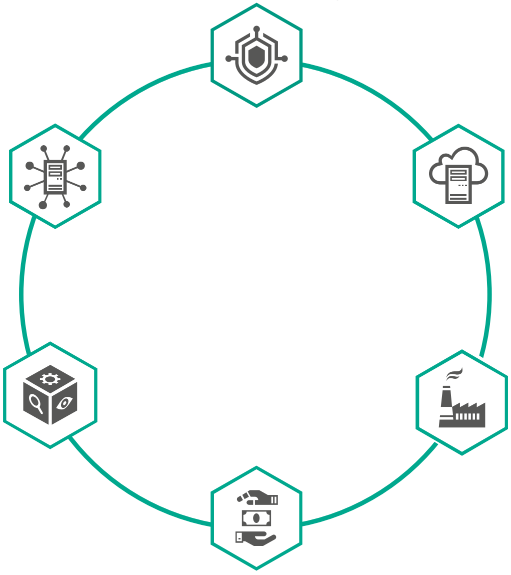
### Behavior Detection, Exploit Prevention & Remediation Engine

Kaspersky Endpoint Security proactively looks for suspicious activities on the corporate network.

Whenever an application launches, Next Gen technologies monitor the application's behavior. If suspicious behavior is detected, our technologies automatically block the application. In addition – because Kaspersky Endpoint Security keeps a dynamic log of the operating system, registry and more – it can automatically roll back malicious actions that the application implemented before it was blocked.

## More security solutions – for every Digital Enterprise

Next Gen endpoint protection – via Kaspersky Endpoint Security – is just one of the solutions we've developed to help enterprises to stay safe in today's high-threat environment:



**Threat Management and Defense**
Discovering and mitigating the risk associated with advanced threats and targeted attacks

**Endpoint Security**
The leading multi-layered endpoint protection platform, based on Next Gen cybersecurity technologies

**Hybrid Cloud Security**
Borderless security engineered for your hybrid cloud environment

**IoT Security**
All-in-one security specifically designed for IoT systems

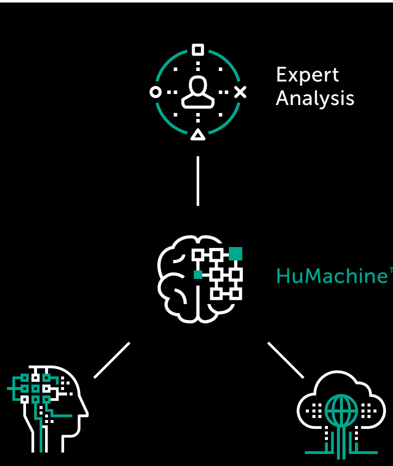
**Industrial Cybersecurity**
Specialized protection for industrial control systems

**Fraud Prevention**
Proactive detection of cross-channel fraud in Real Time

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**



Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence