Kaspersky For Business

KASPERSKY lab

SECURITY SPOTLIGHT

Connecting the dots: Integrating human and technological elements in your security solution

Cybersecurity. Most business owners know they need it, but understanding it is a daunting task. With the responsibilities of running a business, fully grasping the ever-changing threat landscape and knowing how to protect your business can feel overwhelming. It doesn't need to be. We'll walk you through what you need to know about security solutions—how you can harness both the human side of things and the technological side to protect your business.

$6 trillion Expected losses from cybercrime by 2021.[1]

True cybersecurity protection does not just prevent cyberincidents from happening, but also predicts, detects and responds to them. It requires many layers of protection—both from the human side and from the technical side, which can make finding the right solution a very complicated mission.

You need to find a solution that continuously monitors your system but doesn't put such a load on your endpoints that business continuity is affected.

It has to block everything malicious but not bog down your IT department with a parade of false positive results.

It has to have the most advanced technology available to keep up with the latest threats. At the same time, your IT department has to be able to understand it and use it with ease.

It has to be all of these things, and fit within your budget and scale to meet the needs of your growing business. It sounds like a tall order, but there are ways to break down this problem to find the right solution to meet your needs.

In addition to having the right technology in place, there are many steps you can take to ensure that your employees—which are your greatest area of vulnerability—act as a firewall against threats. We'll cover all of the points you need to look for in a cybersecurity solution and the important steps you can take from both a human and technological standpoint to protect your company.

[1] *Cybercrime damages expected to cost the world $6 trillion by 2021*

PREVENT

The first step in ensuring that your company is protected is **preventing an attack from happening in the first place**. This is no small task in a world where there are many threats to your organization each and every day. At Kaspersky Lab, our technology detects over 300,000 new malicious files every day. How can you keep up with that? There are some important steps you can take in both the human and technological spheres.

The Human Element

There are several ways that prevention is the most effective tool in your cybersecurity arsenal, and it starts with educating your executives and those at the Board level, if you are in a larger organization.

Costs. Just one cyberattack can cost an organization an enormous amount of money. **For small- and medium-sized businesses in North America, the average impact of just one data breach is $117,000. For a large enterprise, the average impact is $1.3 million.**[2] These are surprise costs that no one wants to incur, and they include such factors as additional internal staff time, the use of external consultants, lost business, and the public relations needed to clean up the damage to your brand. Add it all together, and the up-front cost of cybersecurity prevention is worth more than the out-of-pocket expenses you will pay for a cure.

Cybersecurity culture starts at the top. No one can help to create a culture of cybersecurity awareness better than your executives. If they highlight this issue as an important one and promote it amongst your whole staff, employees will be more likely to report incidents and follow cybersecurity guidelines. Get them on board. Ask them to be ambassadors for this important layer of protection.

Too small to target? Think again. Many businesses assume that they are too small to be a target of cybercrime. This is a myth. In our surveys, the two most common and costly methods of intrusion into large enterprises were the breach of third-party suppliers and an incident at a third-party supplier that a large enterprise did business with.[3] This means that cybercriminals use smaller businesses to get at the big data in larger enterprises, knowing full well that their defenses may not be as strong. No executive at a small- or medium-sized company wants to have to explain a breach to their clients.

[2,3] *Global IT Security Risks Survey 2017* from Kaspersky Lab and B2B International

The Technological Element

When you have security that is embedded into your infrastructure, it is going to fight most of the battle for you. Let's look at some of the technological elements that you should look for in a security solution in order prevent an attack.

Analysis. Cyberthreats are a moving target, so you need security that moves with them. In order to do this, your security solution should continually gather threat data and learn from the data it collects. Machine learning technology that analyzes the behavior of a threat and adjusts its algorithms accordingly is going to give you the best protection.

Anticipation. Drawing from this analysis, a strong security solution should be able to anticipate where an attack is going to unfold, not just where it exists right now. That way, it can wipe out the threat on arrival.

Assessment. Obviously, not every piece of new data coming into your organization is a threat. Technology that can assess each threat accurately enough to prevent false positives is essential. The last thing your organization needs is a slowdown in productivity due to a heavy security load on your network.

Beyond the endpoint. You need to protect your entire network, not just the endpoint. That means servers, mobile devices and cloud all need to be protected. Any point on the landscape that has access to your data is a potential point for a breach.

PREDICT

In a world where losses to cybercrime continue to climb at an exponential rate, it can feel like you are facing an insurmountable fight against cybercriminals. What if you had the knowledge of where your network is most vulnerable and how to protect it? Short of building a time machine, this knowledge would form an important firewall to protect your business. You're in luck. There are specific steps you can take to identify vulnerabilities and shore up your network.

The Human Element

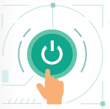
Certain elements of human behavior are easy to predict. One of them is that people will make mistakes. But there are steps you can take to avoid those mistakes and get ahead of the problem.

Employee education is your secret weapon. Imagine this scenario. An employee gets an email from a trusted vendor with what appears to be an invoice attached. Only this vendor never sends invoices from this particular email address, and the employee is not expecting to be billed at this time. Now imagine that your employee knows enough not to open the email or the attachment and instead calls the vendor directly to verify the message. The vendor confirms that this email did not, in fact, come from them. Armed with this knowledge, your employee notifies the IT department who identifies it as a phishing attack and warns others in the organization not to open anything similar.

Right there, your employee has prevented a phishing attack that could spread quickly through your whole network, knocking out servers or even stealing important data. The time you spent on employee education paid off.

Cyberattacks are a matter of *when* not *if* your organization will be breached. We can predict that for certain. Knowing this inevitability, the time you spend educating employees and teaching them to predict intrusions will be time well spent.

Hire people who make cybersecurity a priority. IT security is a multi-layered effort, bringing together the human and technical in a way that forms many layers of protection around your business. If you have people in your IT department who can assess where your vulnerabilities are and make the right recommendations for protecting your business, then those layers will only grow and strengthen.



The Technological Element

All cybersecurity companies would like to see into the future. Most spend a great deal of time studying the threat landscape and trying to predict what is going to happen in cybercrime. The quality of their research and their commitment to learning and applying this intelligence is going to make a big difference in whether or not your organization is well protected. Here's what you should look for.

Threat Intelligence. Tracking, analyzing, interpreting and mitigating evolving IT security threats is a massive undertaking—one you don't have time for when you are running a business. With the right threat intelligence in hand, you can not only stay informed about the changing threat landscape but also learn where to shore up vulnerabilities in your organization. Partner with a security vendor that makes this a priority, and you will find that it is an empowering tool that can make your organization safer.

Penetration Testing. One of the best ways to predict vulnerabilities is to perform penetration testing. While your IT and security specialists work hard to ensure that every network component is secure against intruders, it only takes one vulnerability to open the door to cybercriminals.

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls and obtain high access privileges in your system. With these tests in hand, you can have a greater understanding of security flaws in your infrastructure and how an attack may roll out, as well as evaluating the effectiveness of your current security measures.

DETECT

When it comes to detecting a threat, no company is an island. You need people and technology to work together in a way that keeps your company safe, while keeping it running. Here is how to combine the vigilance of human beings with the advancements of technology to build many layers of protection around your organization.

The Human Element

When looking at the human side of cyberthreat detection, it's important to note that detection and notification go hand-in-hand. If an employee notices something that doesn't seem secure or feels that something is off, they should know how and when to contact IT.

Post instructions clearly. Even though we are dealing with the virtual world, old school posters and flyers about cybervigilance can make a difference. Let people know what to watch out for and how to contact IT if something seems awry. Post these instructions where people gather and where they will be highly visible.

Encourage bravery. Staying ahead of cyberthreats is both a human and a technological effort. No one should feel hesitant or silly for contacting IT, since many cyberintrusions are carried out in strange ways.

Share stories. People remember stories more than data. Share real-life examples of how employees have thwarted phishing attacks or how cybercriminals managed to get around employees to intrude an organization. To underscore our point about employees feeling comfortable about contacting IT, the stories you tell should show how clever and brazen cybercriminals can be in getting people to do their bidding.

The Technological Element

Detecting a threat is the most fundamental function of a cybersecurity solution, but some do it better than others. What features should you look for? What technology is the most cutting edge on today's threat landscape? We've got some answers for you.

Machine learning v. artificial intelligence. In today's threat landscape, no antivirus would work without machine learning. If they all incorporate elements of machine learning, then what should you look for? Solutions that incorporate behavioral analysis make for very advanced detection rates. This is often called heuristic analysis, and it means that the machine learns from different patterns, just as a human does. Many companies call this technology artificial intelligence, but most systems are actually machine learning-based, meaning that they are just very sophisticated robots that still need a human to teach them.

Multi-layered protection. As important as the fundamental technology is, it is also very important that your system has many layers of protection that can check for known, unknown and advanced, targeted attacks. Without layers of protection that can tackle increasingly sophisticated threats, certain solutions will let malicious malware into your system.

★★★ **High detection rates.** Check the detection rates of your anti-virus solution. There are many independently verifiable tests that will give you the answers.

Find the balance of performance and efficiency. Technology comes down to speed and consistency. While you need protection that delivers at the highest possible rates, you should look for a system that doesn't place such a heavy load on your system that it slows down business continuity.

There are certain pitfalls in all cybersecurity solutions that you should check for.

False positives. No IT department needs alarm bells going off all the time, especially when it leaves them chasing a false lead. For a cybersecurity solution to work at peak efficiency, it must not view objects as malicious that are not actually malicious. When learning about any IT security solution, it's important to learn about their rate of false positives.

Humans learn how to trick machines. Cybercriminals always have more scams in their bag of tricks. Their main focus is to look for new ways to trick cybersecurity solutions into letting them in. Therefore, you should look for a cybersecurity company that is knowledgeable about the threat landscape and applies that knowledge to updating its algorithms.

RESPOND

How you respond to an attack has a great deal to do with how much preparation you did up front. From both the human side and the technological side, there are steps you can take to ensure that you can respond as quickly and efficiently as possible when an attack happens.

The Human Element

Since it is a matter of *when* and not *if* your company will be attacked, your IT department needs to prepare for the inevitable.

Have a plan in place. No one likes to imagine the worst case scenario, but doing so is a necessary part of being prepared. If the attack is on your endpoints, your servers or your cloud services, what will you do to respond? Make a list of all areas of vulnerability and cover whether you will shut everything down or shut down certain services. Set aside time for your IT department to write up a plan and practice drills. Like any good sports team, this will leave you in good shape to tackle the problem.

Backups. Few measures give executives and IT departments as much peace of mind as having backups available when an attack happens. In the case of a ransomware attack, for example, this will give you the ability to avoid paying the ransom to cybercriminals and save your own data. Be sure to store backups in a secure place and don't leave them plugged into your main network. Certain attacks are sophisticated enough to search for backups so that they can corrupt them also, leaving your company completely vulnerable.

Do updates and patches on a regular schedule. Most software companies find vulnerabilities regularly and send out patches and updates to fix them. These require time and effort to do, but they are one of the primary ways that cybercriminals get at data. Many high profile attacks that have recently been in the news have been the result of unpatched vulnerabilities. Your IT department should set aside time on a regular basis, usually weekly, to get this important job done.

Read threat intelligence. Knowledge is power. If you know that ransomware attacks are on the rise or that a certain application has a high rate of breaches occurring, you can make the informed decisions you need to make about what to block, what to look for, and how to respond to an attack.

Call in reinforcements. Know who to call in the event of an attack. Many companies need to hire outside experts or alert law enforcement. Have this contact information at the ready and make it a part of your plan to know when to escalate your response.

The Technological Element

All good cybersecurity protection involves much more than just the technology. When an attack happens, how will your cybersecurity company help you respond to an attack? Here are some of the important ways you can ensure that you have the best coverage.

Digital Forensics. One of the most important parts of responding to an attack is what you learn from the experience. Many cybersecurity companies will offer digital forensics services that will help you analyze what happened so that you can close up those vulnerabilities and prevent it from happening again.

Support Services. When your company is attacked, you are going to need help. Being able to pick up the phone and reach an expert will make a huge difference in your ability to respond. Find out what support services are available from any cybersecurity vendor.

Kaspersky Lab HuMachine™ brings together flexibility, expertise and knowledge into a cybersecurity solution that covers your organization and empowers you with the latest threat research.

Big Data. Threat Intelligence.

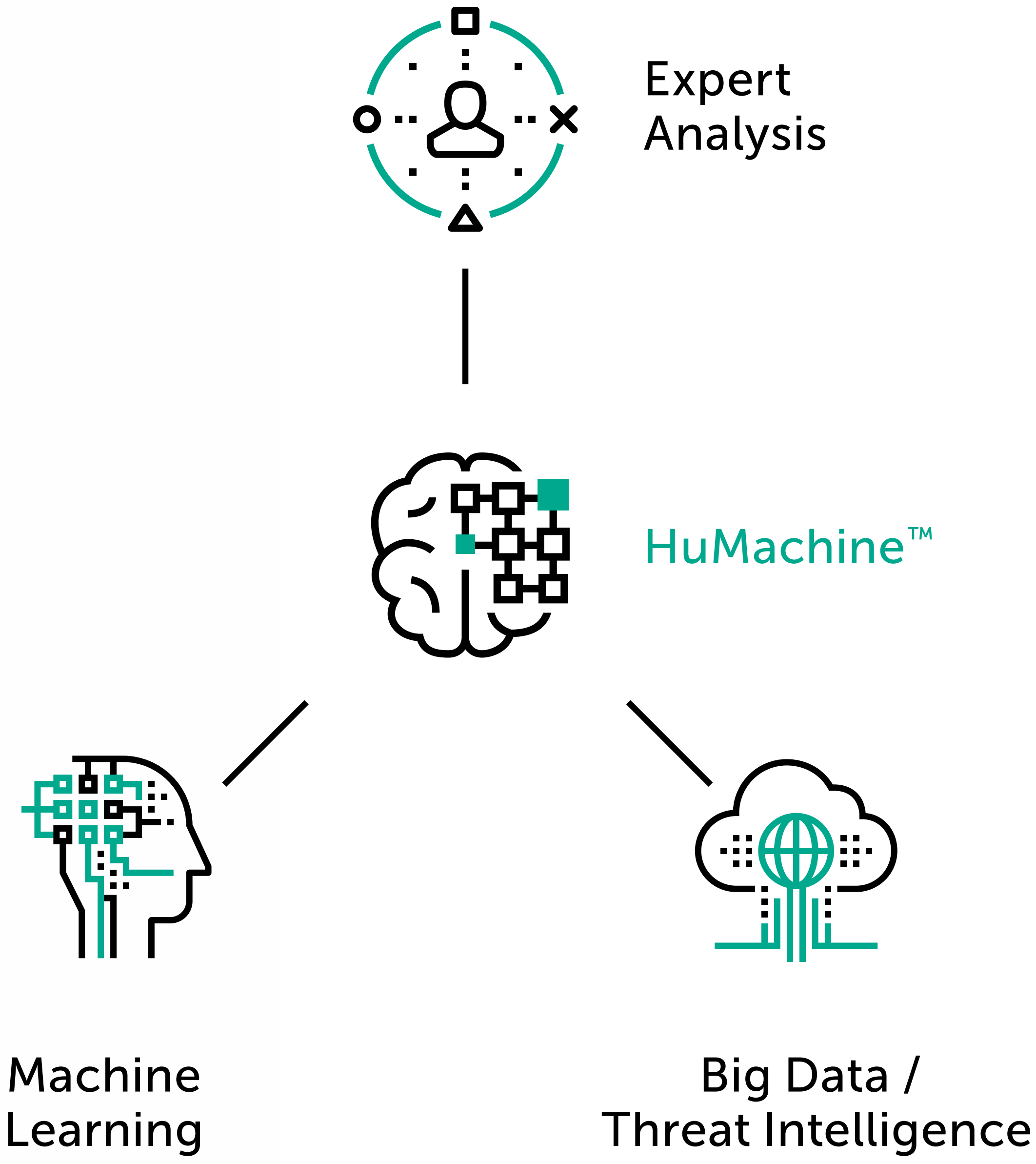
Big data-based threat intelligence feeds analysis of attack targets, their locations and damage done, which is critical to effective protection and updating our technology. Big data influences how we program our machine learning algorithms, which we train to identify malware on sets comprising more than 200 million malicious and 1 billion clean files.

Expert Analysis.

Kaspersky Lab's GReAT (Global Research and Analysis Team) is a worldwide team of top-notch security experts whose research into advanced threats helps us hunt down the hunters. Our security intelligence research into some of the most advanced threat actors in the world forms the backbone of Kaspersky Lab's threat data and helps organizations and law enforcement agencies all over the world deal with incident impact, response and investigation. Kaspersky Lab releases more public reports on advanced persistent threats (APTs) than any other cybersecurity vendor. In 2016 alone, we discovered and reported five zero-day application vulnerabilities to vendors.

Machine Learning.

Our mathematical model analyzes over 100,000 samples features and uses 10 million behavior logs to teach the models so that our algorithms can identify anomalies in incoming data streams. Our experts classify more than ten new unique, pivotal malware families per month and add them to our training set. Combining heuristic analysis with our unique System Watcher technology, our solution monitors applications and processes activity to discern behavioral patterns, rather than just relying on one isolated action, making it one of the most advanced and effective technological solutions in the world.



True Cybersecurity for Business

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

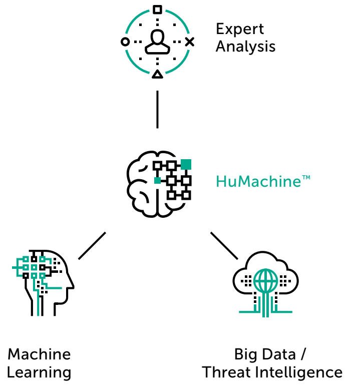
About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Learn more about cybersecurity: **www.securelist.com**

www.usa.kaspersky.com
#truecybersecurity

AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com


Expert
Analysis
HuMachine™
Machine
Learning
Big Data /
Threat Intelligence