WHY YOU NEED EDR

Guide for Small and Medium-Sized Businesses

F-Secure

CONTENTS

WHY YOU NEED EDR

Is an attacker inside your network right now?

Even with the growing investments in cybe security, most IT leaders still can't answer this question definitively. There's so much to keep track: users, devices, applications, alerts, vulnerabilities, patches – the list goes on. IT teams, especially those in smaller companies, simply don't have the time to monitor their networks 24/7.

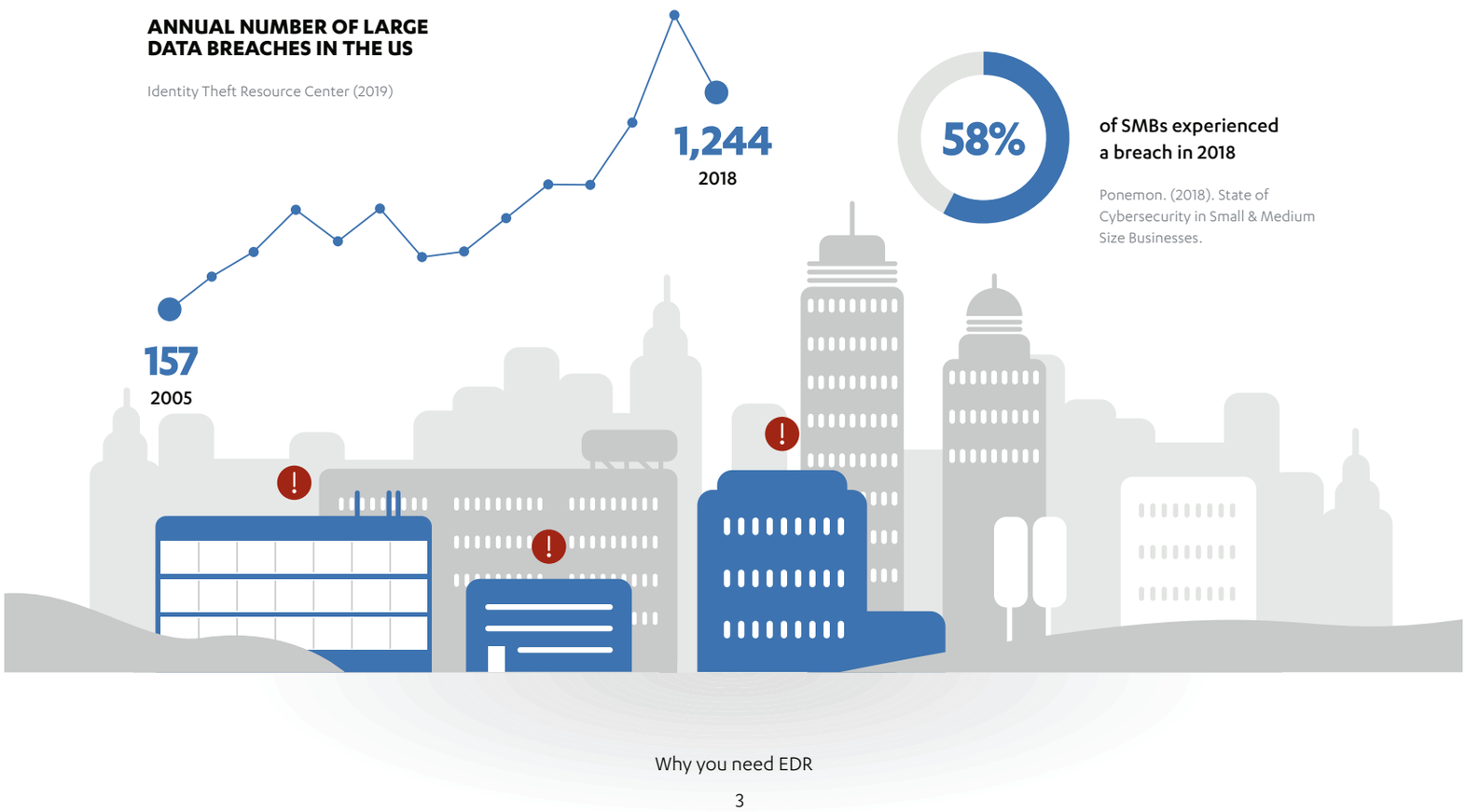
To date, nearly two thirds of global organizations have been breached [1], with 56% of these breaches taking months or longer to discover [2]. And the longer a breach remains uncontained, the more expensive it gets, with response costs quickly skyrocketing up to thousands per day.

These attacks also target smaller businesses, with roughly 58% of SMBs experiencing a breach in 2018 [3]. For these companies, the consequences are even more serious: the National Cyber Security Alliance estimates that 60% of SMBs are forced to close within six months of an incident [4].

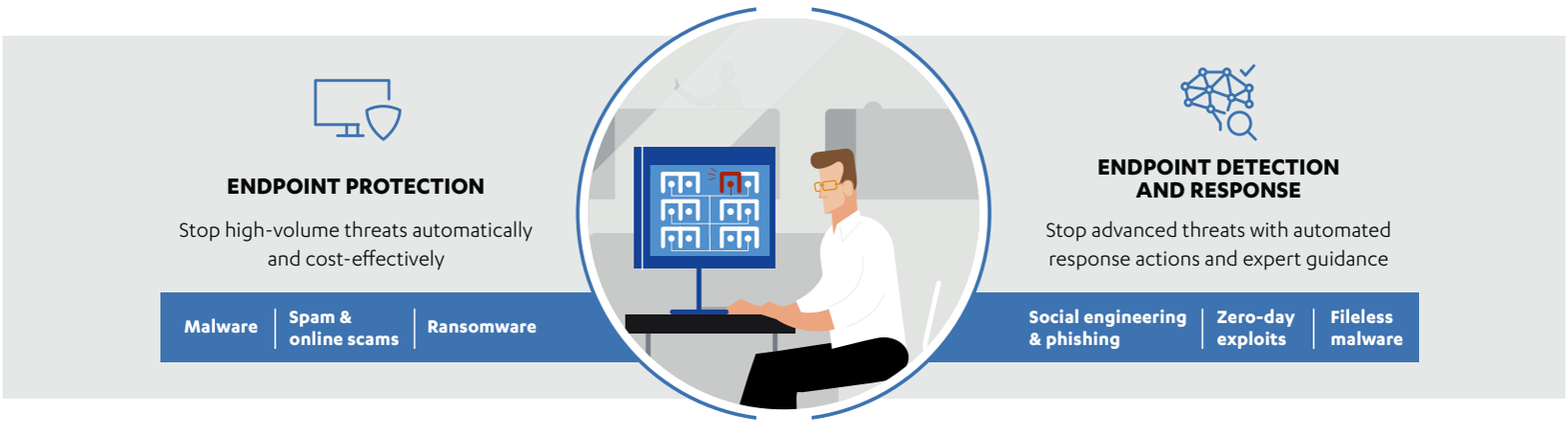
The situation seems gloomy, with attackers bypassing organizations' defenses left and right. As an IT leader with limited resources - but endless liabilities - what can you do?

Enter **endpoint detection and response,** often shortened to **EDR**. EDR solutions are built to augment **endpoint protection** (your business' anti-malware, spam filtering and the like) with better detection and response capabilities. Think of your endpoint protection as a fence, and EDR as a constantly patrolling security team, always on the lookout for anyone trying to breach that fence. It's the next layer of security when your preventive defenses fail to catch an advanced attack or one of your devices misses an important patch. Even if an attacker gets in, it's not game over - you have your security team at the ready.

EDR is becoming more and more important for fighting against cyber attacks, but many IT professionals still find it difficult to quantify its exact benefits for their business. To help you, we've created this guide. It explains how EDR works, why it's necessary for detecting attacks, and how you can use it to improve your overall cyber security posture. We've also included some useful information on evaluating EDR vendors, with references to independent test data.



HOW EDR WORKS



EDR works by collecting a massive number of behavioral data events (like process executions, network connections and file operations) from your organization's workstations and servers with lightweight endpoint sensors. This data is extremely valuable for detecting attacks, but in excess it becomes impossible for human analysts to handle. Think millions and billions of individual pieces of information, with a few real threats among all the noise – a real "needle in a haystack" situation.

By using advanced analytics supported by machine learning, EDR can sort through this data and catch attack indicators matching both known and never-seen-before threats. It does this by contrasting accepted user behavior against the collected data and identifying unusual actions. Here are some concrete examples of what EDR can do:

- Detect fileless malware attacks delivered by websites containing malicious code, PDF documents loaded in browsers, or macros embedded in MS Office files.
- Identify unusual and uncommon processes launched from your company's workstations.
- Detect completely new types of malware in your environment, even without existing signatures
- Uncover your employees using unknown or harmful applications.
- Isolate compromised computers and servers from the network, preventing a cyber attack from spreading further.

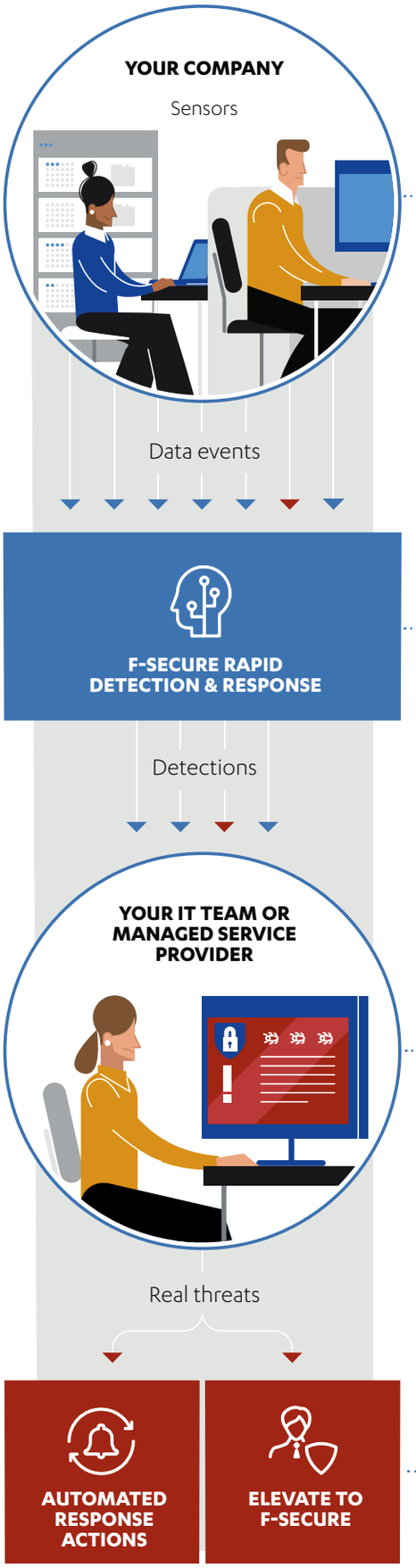
Rather than overwhelming you with a mountain of false positive alerts, EDR can rapidly and accurately narrow the list down to what is really relevant. In the case of one specific customer, F-Secure's solution tracked a total of 2 billion endpoint events over a one-month period – and found the 15 incidents that represented actual threats.

Once threats have been identified, EDR also helps you investigate and respond to them with automated actions and recommendations. This is extremely important for smaller companies, as they usually do not have the resources and expertise to deal with difficult cyber incidents on their own. With an EDR solution like F-Secure Rapid Detection & Response, you not only find out about any problems plaguing your IT environment – you also get concrete help in solving them.

EXAMPLE

A laptop belonging to a junior marketing employee is uploading data to an unknown server on the internet. EDR detects this suspicious behavior in minutes, automatically isolates the computer from the rest of your network and alerts your IT team to investigate. With EDR's help, your team quickly determines this to be a real attack (the employee's computer has been compromised), and investigates its origins. They find the cause to be a process execution launch initiated by a malicious email attachment. Your IT team then remediates the compromised device, updates your spam filtering solution's settings to prevent employees from receiving this weaponized email attachment in the future, adjusts firewall rules to block connections to this domain, and informs users about the risk your organization is under.

In this example, no traditional malware was found as part of the attack – there was nothing for your endpoint protection platform to prevent. Without EDR, you would have been fighting against an invisible enemy.



This is the process behind our EDR solution, F-Secure Rapid Detection & Response:

1. Sensors installed on your Windows computers, Mac computers, and servers track user behavior inside your organization. The collected data events are streamed to our cloud database for real-time analysis. The sensors are invisible to your end users, and your IT team doesn't have to take any extra actions to monitor your IT environment.

2. Our cloud backend examines the collected data, separating suspicious events from normal user activity. This is done through behavioral, reputational, and big data analysis, coupled with machine learning. The analysis is completely autonomous and doesn't require any actions from your IT team.

3. A filtered list of alerts appears on your dashboard, with clear visuals and attack info. You can easily see all impacted hosts and related events on a timeline. The alerts are also placed into context, meaning they account for the importance of affected hosts, the prevailing threat landscape, and current risk levels. With all this information available, you know where to focus your attention first.

4. Real threats are isolated from the network. You now have two options:

a) You can investigate and respond to the issue with your own IT team, using automated response actions and guidance provided by the solution. If your security is managed by one of our certified service providers, they will take the necessary actions on your behalf.

b) You can forward the issue to F-Secure's incident response experts with our built-in **Elevate to F-Secure** feature. They will then investigate the threat and give you advice on how to remediate it before your business is damaged.

HOW ADVANCED ATTACKS HAPPEN

To understand how EDR can protect your organization from targeted and advanced threats, we need to examine how attackers usually operate. Adversaries hoping to breach your preventive security layers will usually start with one of these tactics:

1 **Exploiting a Vulnerability:** Common security weaknesses in your public-facing systems are an attractive attack avenue, with 57% of breaches resulting from known vulnerabilities that could have been patched [5]. With over 16,000 new vulnerabilities released each year, most companies find it extremely difficult to keep their whole infrastructure up to date [6]. Using modern automation tools, opportunistic attackers can scan the public internet for any one of these common vulnerabilities, potentially finding thousands of devices that haven't been patched.

2 **Spear Phishing:** Targeted, deceptive communications designed to trick someone in your organization into sharing sensitive information or opening an executable file. Spear phishing is extremely common, and extremely effective – Verizon's yearly threat report estimates that 32% of breaches involve this attack tactic [2].

3 **Watering Hole:** The attacker looks for vulnerabilities in websites known to be popular among your employees. They then insert malicious code in JavaScript or HTML on these sites, which pushes targets to another compromised site with malware waiting in ambush. When someone in your organization uses the common and popular website, the trap is sprung.

4 **Man-in-the-Middle:** The attacker intercepts your communications, passing them on only after examining or even altering them – creating the illusion that you are talking directly to a trusted counterpart. Man-in-the-middle attacks are done in close proximity through unencrypted Wi-Fi networks, or remotely via malware.

5 **Buying Access:** Criminal organizations crowd-source so many attacks on so many systems, that a certain percentage of those systems are bound to be compromised at any given time. In many cases, attackers can save themselves time and trouble by simply buying access to a system that has already been compromised. Do you know if your company has been breached in the past? If this is the case, access to your systems might be available on the black market behind a cheap paywall.

Once an attacker gets in the door, their next step is to roam around inside your system and see what they might be able to get away with. They may add new local users or modify existing user accounts to elevate their privileges, search for domain administrator passwords with a memory-scraping tool, or move laterally from one system to another looking for anything of interest.

Of course, they do not want to be spotted while doing any of these things, so skilled attackers will typically use legitimate OS components to establish their presence inside your company and hide within normal traffic. Firewalls and traditional endpoint protection products will not be able to detect the attacker at this point in the process.

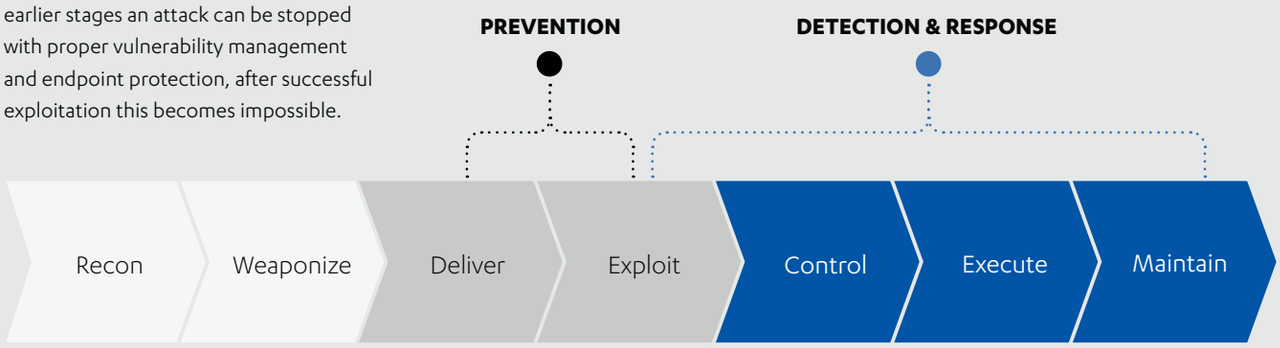
Finally, the attacker will use your own IT administrator tools against you, exploiting PowerShell, Service Commands, or Windows Remote Management to get whatever they came for in the first place – such as customer data or intellectual property. When the attacker exfiltrates the data, the process will be carefully crafted to look like regular user behavior and raise no red flags. Now your crown jewels are available on the black market, available to the highest bidder.

Sophisticated attacks like this cannot be stopped by static defense methods alone, and no organization should consider itself immune to them. In fact, most cyber criminals prefer to target small to medium-sized companies, as they usually have less defenses and a lower IT security headcount compared to large enterprises. SMBs are also often found in larger companies' supply chains, making them a viable attack avenue when trying to breach these companies via spear phishing or other methods.

By using EDR, you flip this arrangement on its head. Although an adversary might get past your preventive security with a sophisticated attack, they will find it much harder to hide among your normal network traffic. You will be able to detect any unusual behavior before your business gets damaged. In many cases, simply running an EDR solution acts as a powerful deterrent against opportunistic cyber criminals.

CYBER ATTACK LIFECYCLE

The Cyber Attack Lifecycle is a simplified version of the sequence that an adversary follows to breach a network. Although in earlier stages an attack can be stopped with proper vulnerability management and endpoint protection, after successful exploitation this becomes impossible.



HOW EDR HELPS YOU AS AN IT LEADER

As the person responsible for your company's cyber security, EDR gives you several advantages:

1. **If anyone asks about your security status, you'll be able to give a clear, confident, and accurate answer:** Cyber security has moved from a niche IT topic into mainstream risk management. IT managers face a growing pressure to report their company's security status to top leadership, including the board. When you're faced with the inevitable question: "How secure are we right now?", EDR allows you to give an insightful and honest answer. Coupled with data from your vulnerability management and endpoint protection platforms, you can clearly explain how well you're protected; what kind of attacks your systems have encountered; whether your employees are following set IT security guidelines; and so on.

2. **You can rest easy knowing that any attempted attack will be quickly detected and reported – without spending your whole IT security budget:** As we've stated countless times in this guide, attack prevention alone doesn't cut it anymore. But developing effective detection and response capabilities is not easy – or cheap – when you're starting from scratch. A turn-key EDR solution is a great option for small and medium-sized companies, as you'll get all the core functionality of detection and response without the price tag that comes with fully managed services. In fact, some solutions like F-Secure Rapid Detection & Response also give you access to the security professionals usually reserved for these premium solutions. With our **Elevate to F-Secure** feature, you can forward serious or complex threat detections straight to our incident response center's experts – the same people who manage our enterprise customers' cyber security on a daily basis.

3. **When a threat is detected, you'll be able to respond and remediate it much more rapidly:** On top of detections, EDR also gives you tools and actionable recommendations on dealing with different security issues. Host isolation, direct user communication, remote response actions – your EDR solution guides you through the best way to solve a given security incident as quickly as possible. Although the goal is always to prevent an attack in the first place, these tools are invaluable when you do find yourself dealing with an active threat.

4. **If a breach occurs, you'll be able to see and understand exactly what happened, to prevent it from ever happening again:** Detecting and stopping attacks is one thing – but understanding how they happened is equally as important. To improve your company's security posture in any meaningful way, you need to go back and look at the methods that were successful against your defenses. By collecting all relevant forensic data, EDR gives you the possibility to analyze how an attack was performed, learn from it, and harden your security against similar attempts in the future. Getting data about unsuccessful attack attempts is also important, as this can reveal that you're being targeted by a persistent cyber criminal.

5. **Under the EU's General Data Protection Regulation or GDPR, companies are required to report any data breaches within 72 hours. Rather than worrying about compliance issues, you'll know for certain that your company can meet the requirements:** We've already seen the first GDPR-fines levied against companies that were breached since the regulation took effect. EDR helps you comply with the GDPR on two fronts: firstly, you can show EU authorities that you've undertaken the basic actions to protect your data by monitoring your IT environment. Secondly, should an attack get through your defenses, you can collect enough information to report it to the authorities within the 72 hour deadline.

HOW TO EVALUATE EDR VENDORS

Hopefully now you have a better idea about the core working principles and benefits of EDR. But how do you know which solution is right for your organization?

When it comes to evaluating different EDR vendors, the field is a lot less cluttered than traditional AV. The golden standard is a program developed by US-based non-profit MITRE. It evaluates EDR solutions against the organization's own "ATT&CK framework", a continually updated set of tactics, techniques and procedures used by cyber criminals. This gives companies impartial results to benchmark different EDR vendors' performance, along with insights into the kinds of telemetry, alerts, interface, and output you can expect from each. MITRE's evaluations are widely used by several industry authorities, such as Gartner and Forrester.

F-Secure's EDR detection capabilities were tested by MITRE in the summer of 2019. We received excellent results, showing that F-Secure can detect even the most sophisticated nation state attacks. MITRE's evaluation is not a competitive analysis, and they do not assign scores to different vendors. However, Forrester published an evaluation script that counts and scores the results in an attempt to measure how different vendors performed. Using their simple metric, F-Secure achieved the highest score.

To sum it up: with F-Secure, you can rest assured you're getting the best possible EDR technology. Please get in touch with us if you'd like to know more about the MITRE ATT&CK framework and how to interpret the test results.

MITRE's evaluation is a great starting point, but you also need to consider other factors besides pure detection performance. When talking to vendors about their EDR solutions, address at least these questions. To give you some examples, we've provided our answers.

QUESTIONS FOR EVALUATING EDR VENDORS

How difficult and time-consuming is it to run their EDR solution? F-Secure Rapid Detection & Response is built to be operated by even junior IT analysts, with a clear UI and dashboards. Because the solution visualizes all activity happening on your endpoints, your team will find it easy to understand when and how an attack is happening. With our automated response actions and built-in guidance, you can also react to attacks without being a fully certified incident response expert.

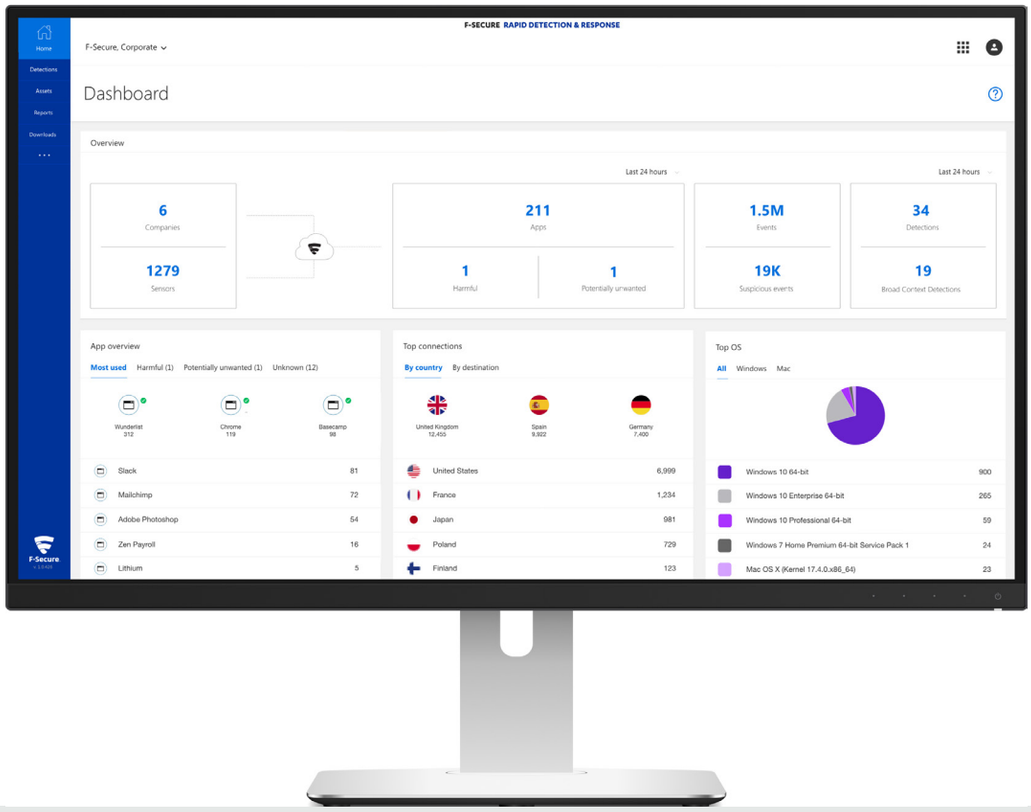
Can the solution be integrated with your other security products? F-Secure Rapid Detection & Response works together with all endpoint protection platforms. What's more, it is fully integrated with our own award-winning endpoint security solution F-Secure Protection Service for Business. With this endpoint package, you can prevent, detect, and respond to all threats effectively. You can also manage both solutions inside the same user portal.

What is solution's performance impact on your endpoints? F-Secure Rapid Detection & Response's endpoint sensors are light and discreet, with extremely low performance impact on your endpoints. As we've heard from multiple customers, they are practically invisible to the end user – which should be the goal of every cyber security solution out there.

How does the solution actually detect threats? F-Secure Rapid Detection & Response uses our proprietary Broad Context Detection™ technology to detect threats. It leverages real-time behavioral, reputational and big data analysis with machine learning to automatically place detections into a broader context. These detections are also enriched with risk levels, affected host importance, and the prevailing threat landscape.

What kind of support does the vendor offer? If your business experiences an attack or a complex threat detection, our solution has a built-in feature called Elevate to F-Secure. With one button click, you get help from our trained incident response experts who have hands-on experience in dealing with countless cyber attacks. In addition, you can also choose to purchase F-Secure Rapid Detection & Response as a managed service, provided by one of our certified resellers. This way you can focus on your core IT tasks, while your security is handled by experts.

Large and highly targeted organizations may also want to consider F-Secure's fully-managed threat hunting service. It helps you stop even the most demanding nation state attacks in minutes, with 24/7 support from our threat investigators and incident response experts.



F-SECURE RAPID DETECTION & RESPONSE

- Get immediate visibility into your IT environment
- Detect cyber attacks and IT problems in minutes
- Respond to threats with automation and guidance
- Get help with difficult threat detections from F-Secure

ENDNOTES

1 451 Group. (2019). Thales Data Threat Report.

2 Verizon. (2019). Data Breach Investigations Report.

3 Ponemon. (2018). State of Cybersecurity in Small & Medium Size Businesses.

4 National Cyber Security Alliance. Cyberthreats and solutions for small and midsize businesses.

5 Ponemon. (2018). Cost of a Data Breach.

6 CVE Details (2019). Number of New CVEs Published Each Year.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure