F-SECURE RAPID DETECTION & RESPONSE

Solution Overview

F-Secure

CONTENTS

DISCLAIMER: This document gives a high-level overview of the key security components in the F-Secure Rapid Detection & Response solution. Details are omitted in order to prevent targeted attacks against our solutions.

F-Secure is constantly improving its services. F-Secure reserves the right to modify features or functionality of the Software in accordance to its product life cycle practices. Last updated: November 26, 2019

1. EXECUTIVE SUMMARY

Targeted cybersecurity attacks can be difficult to analyze and respond to, and become an extremely costly problem for companies even before they turn into actual data breaches. The attack remediation stage alone may take over two months and cost nearly two million dollars.[1] Fileless attacks are commonly not recognized by traditional antivirus protection, and targeted attacks often go unnoticed for months or even years.[1] With the F-Secure Rapid Detection & Response solution, you can gain contextual visibility into your security, automate threat identification, and stop attacks before data breaches involving sensitive, confidential or otherwise protected data exposed to an unauthorized party, like a cybercriminal, happen.

F-Secure Rapid Detection & Response (RDR) is a leading context-level endpoint detection and response (EDR) solution to help companies to gain immediate visibility into their IT environment and security status, protect the business and its sensitive data by detecting attacks quickly, and responding fast with expert guidance. With its deep bidirectional intelligence and high level of automation, F-Secure's solution protects against advanced threats even before breaches happen. It detects incidents with lightweight clients, which are installed on monitored hosts across the organization's network. The clients collect data on behavioral events such as file access, launched processes, network connections being created, or something being written into the registry or system logs. These events are then further analyzed by the solution. In addition to real-time detections, the solution also makes detections based on historical data. At the end of the day, utilizing cutting-edge technology is just one part of the equation, as technology is only as good as the people behind it. Our threat hunters and researchers are among the leading experts in the industry, and immensely dedicated to providing the very best on the cybersecurity market. At F-Secure, we combine that technology and that unsurpassable human expertise to deliver a world-class endpoint detection and response solution.

The solution is uniquely backed by F-Secure, which means that a detection can be elevated to F-Secure for further threat analysis by experienced cyber security experts.

The solution is also available as a partner managed EDR service that combines technology, threat intelligence, and partner services to provide an all-in-one breach detection and response service. The managed EDR services free up an organization's own resources from advanced threat monitoring and incident management to alert the organization only when real threats have been detected.

At the end of the day, utilizing cutting-edge technology is just one part of the equation, as technology is only as good as the people behind it. Our threat hunters and researchers are among the leading experts in the industry, and immensely dedicated to providing the very best on the cybersecurity market. At F-Secure, we combine that technology and that unsurpassable human expertise to deliver a world-class endpoint detection and response solution.

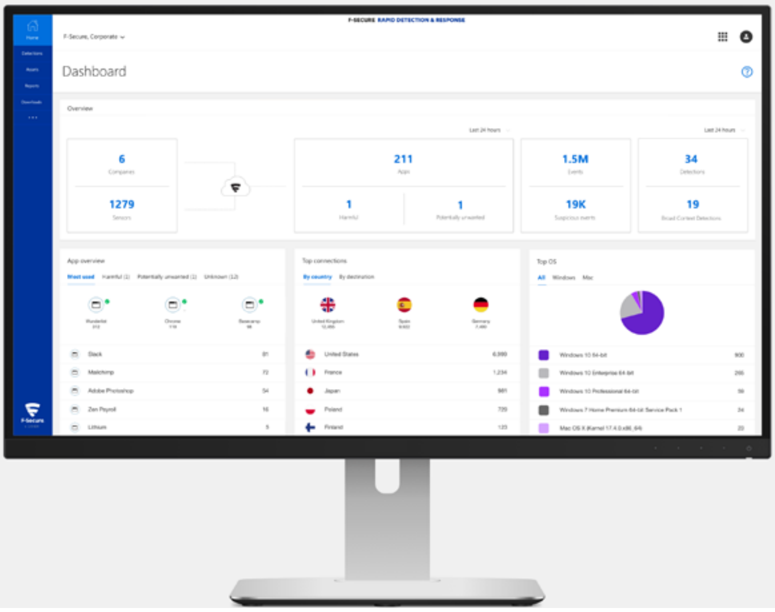
PREVENTION MAKES THE ATTACKERS' LIVES HARDER

Advanced attackers may have the skills to get into your network no matter what, but there's no need to roll out the red carpet. By putting effort into pre-compromise prevention, you're making it a little harder for these attackers to breach your network. When they're forced to put in more effort, their cost structures increase, which helps work as a deterrent.

F-Secure Rapid Detection & Response as a post-compromise solution for detecting advanced attacks still requires a strong endpoint protection solution that blocks commodity threats, like ransomware.

F-Secure Rapid Detection & Response solution has been designed to work with any endpoint protection solution, and it functions with F-Secure Protection Service for Business (PSB) endpoint security solution as a single-client and cloud-based management infrastructure.

[1] Ponemon Institute's 2018 Cost of a Data Breach Report indicated the days to identify data breaches varied by industry sector from 150 to 287 days, and post data breach response activities alone spending alone $1.76 million over 69 days as mean time.



2. KEY BENEFITS

With the F-Secure Rapid Detection & Response solution, you can be prepared to detect advanced threats and targeted attacks using fileless techniques before data breaches happen, and always be ready to quickly analyze and respond to them by utilizing F-Secure's cutting-edge technology.

Some of the key benefits the solution delivers for visibility, detection and response are listed below:

Gain immediate contextual visibility into your IT environment and security status

- Improve visibility into IT environment status and security with application and endpoint inventories
- Easily spot misuse from proper use by collecting and correlating behavioral events beyond malware
- Respond faster to the identified targeted attacks thanks to alerts with broad context and host criticality

Protect your business and its sensitive data by detecting breaches quickly

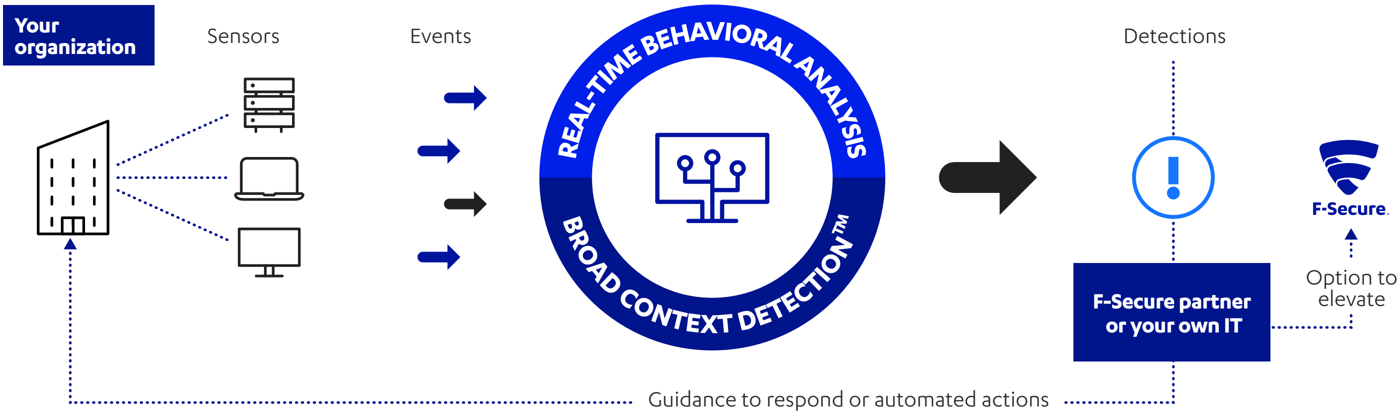
- Detect and stop targeted attacks quickly to prevent business interruptions and impact on company reputation
- Be prepared before breaches happen by setting up advanced threat detection & response capabilities within days
- Meet the regulatory requirements of PCI, HIPAA, and the European Union's GDPR which requires data breaches to be reported within 72 hours

Respond swiftly with automation and guidance when under attack

- Improve your team's focus with built-in automation and intelligence that support a swift response to the real advanced threats and targeted attacks
- Receive guidance on how to respond when you get alerts, with the option to automate response actions around the clock (automation features to be introduced as an update)
- Overcome skill or resource gaps in your teams by outsourcing advanced threat monitoring to an F-Secure certified managed service provider backed by F-Secure experts

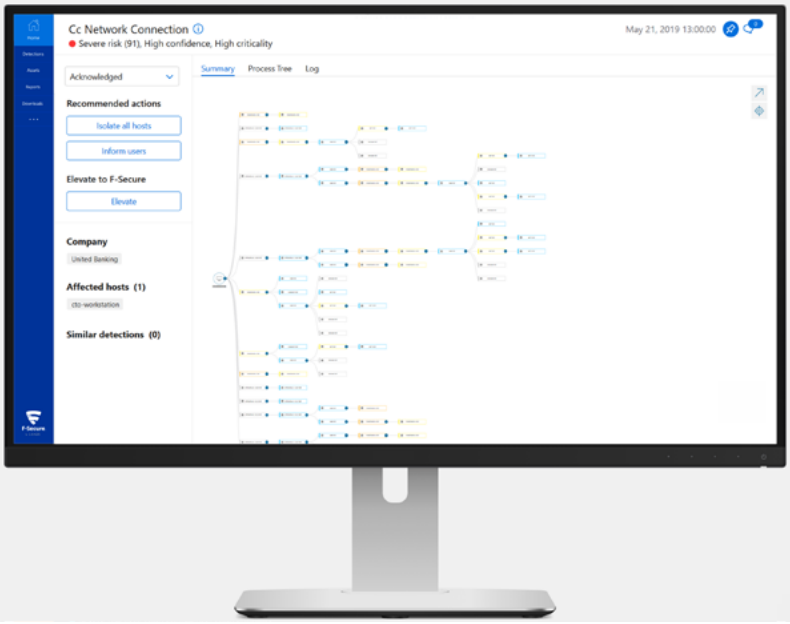
3. SOLUTION OVERVIEW

The F-Secure Rapid Detection & Response (RDR) solution consists of a combination of easily deployable clients on hosts, a cloud-based Management Portal, and optional certified partner managed services. The solution provides functionality for detecting advanced threats and targeted attacks, and Broad Context Detections to clarify the overall risk and response. The on-site part of the deployment includes endpoint monitoring and response client that is installed onto an organization's endpoints.


Your organization
Sensors
Events
REAL-TIME BEHAVIORAL ANALYSIS
BROAD CONTEXT DETECTION™
Detections
F-Secure
Option to elevate
F-Secure partner or your own IT
Guidance to respond or automated actions

The figure above describes on a high level how the F-Secure Rapid Detection & Response solution works:

1. **Lightweight clients** monitor different endpoint activities that are carried out by attackers, and stream behavioral events to our cloud in real-time.
2. **Real-time behavioral data analytics** flag and monitor both the processes and other behaviors that have triggered the events.
3. **Broad Context Detection™ mechanisms** further narrow down the data, placing related events in context with one another, quickly identifying real attacks and prioritizing them with respect to risk level, host criticality, and prevailing threat landscape.
4. **Following a confirmed detection, the solution guides** IT and security teams through the necessary steps to contain and remediate the threat.



3.1 Management portal

The Rapid Detection & Response solution makes it easy to deploy, manage, and monitor the advanced threats on your endpoints from a single, intuitive, web-based console. It gives you immediate contextual visibility into IT environment and security status across your network — regardless of whether employees are at the office or on the go.

The management portal was designed to simplify and accelerate security management in demanding and multi-site environments.

Below are some examples of how the solution considerably reduces the amount of time and resources needed for advanced threat monitoring and management:

- The solution is designed to work with any endpoint protection solution, and it functions with F-Secure's endpoint security solutions in a single-client and management infrastructure.
- When combined with F-Secure Protection Service for Business (PSB), both malware and advanced threats become visible and manageable.
- Detections are presented with actionable visualization to provide a broader context of targeted attacks on a timeline with all impacted hosts, relevant events and recommended actions.
- By consolidating the advanced threat management of endpoints and system tools into one endpoint security portal, the overall management is streamlined considerably, saving time.
- As this is a cloud-based service managed by F-Secure, there is no server hardware or software to install or maintain – all you need is a browser and an internet connection.

The management portal supports the latest versions of the following browsers: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome and Safari.

The management portal is available (as of February 2019) in Bulgarian, Chinese, Chinese (Hong Kong), Chinese (Taiwan), Czech, Danish, Dutch, English, Estonian, Finnish, French, French (Canada), German, Greek, Hungarian, Italian, Japanese, Korean, Lithuanian, Norwegian, Polish, Portuguese, Portuguese (Brazil), Romanian, Russian, Slovenian, Spanish, Spanish (Mexico), Swedish, Turkish and Vietnamese.

The Partner Managed version of the management portal includes specifically designed features to assist service providers, like end-customer reporting, a dashboard with a convenient overview of all the managed companies, and also access to each managed company's own dashboard.

3.2 Endpoint clients

Endpoint clients are lightweight, discreet monitoring tools designed for anomaly detection, including new and previously unidentified events or a sequence of events that most likely result from malicious activities, deployable on all relevant Windows and MacOS computers within the organization. The clients collect behavioral event data from endpoints, are designed to work with any endpoint protection solution, and function seamlessly with F-Secure's endpoint security solutions in a single-client and cloud-based management infrastructure.

The table below describes supported operating systems and features on each operating system.

	WINDOWS WORKSTATIONS	WINDOWS SERVERS	MAC OS
OPERATING SYSTEMS	7 / 8 / 10	2019 / 2016 / 2012 / 2011 / 2008 R2	10.12 or newer
SINGLE-CLIENT WITH F-SECURE	Yes	Yes	Yes
CLIENT WITH COMPETITIVE EPP	Yes	Yes	Yes
BEHAVIORAL EVENTS	Yes	Yes	Yes
APPLICATION VISIBILITY	Yes	Yes	No*
REMOTE HOST ISOLATION**	Yes	Yes	Yes

*** Expected later: The feature is not yet available. ** Available with F-Secure Business Suite through manual actions.**

In addition to F-Secure Protection Service for Business (Computer/Server Protection) and F-Secure Business Suite (Client/Server Security), the solution's compatibility has been tested with the following endpoint protection solutions (as of August 2018): Bitdefender Endpoint Security Tools, ESET Endpoint Security; Kaspersky Endpoint Security; McAfee Endpoint Security; Microsoft Windows Defender; Panda Adaptive Defense 360; Trend Micro Business Security; Sophos Endpoint Security and Control, Symantec Endpoint Protection and Webroot SecureAnywhere.

More information about system requirements and client deployment in the user guide at https://help.f-secure.com/product.html#business/edr/latest/en/deployment-latest-en

3.3 Application visibility

Gaining extensive visibility into your IT environment and cloud services will reduce exposure to advanced threats and data leakage. Our solution's application visibility allows you to list all active applications running on endpoints across your organization's network so you can easily identify unwanted, unknown and harmful applications.

With application visibility you can identify Potentially Unwanted Applications (PUA) and Unwanted Applications (UA). 'Potentially Unwanted Applications' have behaviors or traits that you may consider undesirable or unwanted. 'Unwanted Applications' have behaviors or traits with more severe impact on your device or data.

Applications identified as 'Potentially Unwanted' (PUA) can:

- Affect your privacy or productivity - for example, expose personal information or perform unauthorized actions
- Put undue stress on your device's resources - for example, use an excessive amount of storage or memory
- Compromise the security of your device or the information stored on it - for example, expose you to unexpected content or applications

The impact of these behaviors and traits on your device or data can range from mild to severe. They are not, however, harmful enough to warrant classifying the application as malware.

3.4 Behavioral Analysis

As a core functionality for identifying advanced threats among massive amounts of behavioral data events to spot suspicious events or a sequence of events that have not been seen before and most likely malicious.

F-Secure uses real-time behavioral, reputational, and big data analysis with machine learning to collect multiple suspicious events that can be tied together, for example based on activities. The behavioral analysis leverages artificial intelligence to detect malicious, hidden activity based on small individual events that are executed as part of the attacker's tactics, techniques and procedures. Behavioral analysis is used in automatic host profile identification that impacts risk scoring of detections in relation to the monitored company and host, and the overall IT environment.

The artificial intelligence includes machine learning capabilities to be applied to continuously improve detections and reduce false-positives. The behavioral analysis capability is a prime example where F-Secure combines data science and cyber security expertise – an approach F-Secure refers to as "Man and Machine".

3.5 Broad Context Detection™

F-Secure's proprietary Broad Context Detection™ methodologies are designed to narrow down the number of detections to a small number of meaningful incidents that may indicate that systems or data have been compromised.

Broad Context Detection™ flags indications of possible breaches by alerting admins of tactics, techniques and procedures (TTPs) used in targeted attacks. This can for example include the following possibly suspicious actions:

- Abnormal activity of standard programs
- Calls to running processes from non-standard executables
- Running of unexpected scripts
- Unexpected running of system tools from standard processes

Broad Context Detection™ shows only relevant detections and assigns them a criticality based on risk level, information about affected host criticalities, and the prevailing threat landscape. A single event might not be an indication of attack, yet if several detections happen in a short timeframe may result into higher severity alert and trigger a Broad Context Detection™ as a warning of a possible incident.

As a result of this approach, IT teams are provided with a relatively short list of confirmed detections, each flagged with distinct priority levels and recommended response actions. So not only do teams know what to focus on first, but they also know how to respond and can do so quickly and decisively.

For further information about the Broad Context Detection™, please refer to our Detecting Advanced Attacks whitepaper on www.f-secure.com/RDR.

THE FOLLOWING LIST CONTAINS SOME EXAMPLE ACTIVITIES WHICH CAUSE A DETECTION.

The list is not only limited to known attacks since the detection data is continuously being analyzed and more types of attacks are continuously identified by Broad Context Detection™ methodologies and F-Secure's threat hunters.

Directed attack targeting a host

Lateral movement involving movement between hosts

Spoofing information involved as part of an attack

Persistence for example by using a process on the same host

Privilege escalation for example by brute forcing administrator privileges

Credentials access resulting into access and control over a targeted machine/network

Exfiltration to aid adversary to exfiltrate information from the target machine/network

Abnormal process execution for example with suspicious parameters

Abnormal file access for example multiple document types, non-root accessing system files

Client tamper attempts for example to change client's settings or disabling the client

Injection attempts to another process for example kernel mode or other application

Command and control network connection opened to a remote host

PowerShell script from attacker location flagged as an unusual location to load a script

PowerShell modified a PowerShell script typically part of achieving persistence

Abnormal DLL usage with PowerShell used from a process that loaded the module

Remote connection and execution potentially used for lateral movement

3.6 Incident management

The solution has a built-in incident management feature to view and manage Broad Context Detections. New detections will trigger an email alert that contains direct access to the Management portal to view details and take actions.

The Broad Context Detections are listed on the easy-to-use dashboard that helps to prioritize the incidents based on their risk score, which is automatically calculated based on criticality and confidence levels. Non-critical Broad Context Detections with low risk scores are also listed, since slowly evolving attacks might eventually become more serious incidents with high risk scores.

Actions in incident management are to acknowledge Broad Context Detections, or mark them to be in progress, monitoring, closed as confirmed, closed as false positive, or closed as unconfirmed. Marking a Broad Context Detection™ false-positive will automatically close future detections matching that same detection type, process parameters as "Auto false positive".

3.7 Guidance to respond

Following a confirmed detection, the solution's built-in guidance helps to take the necessary steps to contain and remediate the threat. The containment and remediation steps include recommended response actions, like informing users and isolating hosts.

F-Secure's cyber security experts have used their own experience to analyze a range of common threats to train the solution. As result, the solution can provide easy to understand guidance to respond to a wide range of advanced threats, and related guidance how to respond. The guidance to respond makes it easier even for less skilled IT and security team members to take correct actions to contain and remediate the threat.

3.8 Elevate to F-Secure

F-Secure provides an optional threat analysis service in case a detection requires further threat analysis and guidance from F-Secure's cyber security experts. Elevate to F-Secure is a premium service that must be ordered in advance for a set of cases to be analyzed.

The Elevate to F-Secure requests through the solution will grant F-Secure's threat analysts' permission to access the entirety of metadata collected from the installed clients around a specific detection.

F-Secure's on-shift threat analysts will pick the request within 2-hour target SLA and start identifying the type of the potential incident by collecting additional evidence and providing further expert guidance through the solution to validate the threat, and optionally provide a threat investigation.

- **Threat Validation** provides additional information about a Broad Context Detection™ discovered during the last 7 days. This includes an expert-written summary and description of the detection, along with any other relevant data to help you determine whether it requires response actions.
- **Threat Investigation** provides a highly detailed investigation into a specific Broad Context Detection™, leveraging all recent and historical data. This option also includes actionable incident response guidance from our cyber security experts, along with a comprehensive report of the detected attack type.

The Elevate to F-Secure service focuses on analyzing technical evidence related to the potential incidents in question, such as methods and technologies, network routes, traffic origins, and timelines. However, the F-Secure team only provides guidance through the solution, and further professional services to support incident response must be agreed separately. If the customer suspects a crime, we recommend to contact the relevant authorities and provide the Threat Investigation report.

3.9 Automating actions

Automated response actions are available to reduce the impact of targeted cyber attacks by automatically containing them outside business hours whenever risk levels are high enough. The automation has been designed specifically for teams that are monitoring detections and available to respond to incidents only during business hours to make initial response action over the night or weekend.

4. DATA SECURITY

4.1 Data protection and confidentiality

The collected behavioral event data from endpoints is stored within European Union (Ireland) for one year on a rolling basis during the customer engagement and is deleted within two months after termination of engagement.

The solution is not intended for monitoring non-security-related activities such as profiling employees' activities, interests, or interactions. The focus of data collection is not on individual employees, business documents or email contents. Please see the solution specific privacy policy for further detail.

As F-Secure is based in Finland, we abide by both Finland's and the European Union's strict privacy and security legislations. We are compatible with the European Union privacy framework, and understand the privacy needs of our customers. F-Secure operates under the Finnish implementation of the EU Data Protection directive and the F-Secure Rapid Detection & Response solution has been designed in accordance with the European Union's General Data Protection Regulation (GDPR). For further information about F-Secure's compliance with the GDPR, please see https://www.f-secure.com/GDPR.

4.2 Data security measures

As a security company, we take the security of our data centers very seriously and use dozens of security measures to ensure it, such as:

- Security by design: Our systems are designed from the ground up to be secure. We embed privacy and security in the development of our technologies and systems from the early stages of conceptualization and design to implementation and operation.
- Rigorous access controls: Only a small vetted group of F-Secure employees have access to the customer data. Access rights and levels are based on their job function and role, using the concept of least privilege and matching that to the defined responsibilities.
- Strong operational security: Operational security is an everyday part of our work, including vulnerability management, malware prevention and robust incident management processes for security events that may affect the confidentiality, integrity, or availability of systems or data.

4.3 Data centers

Our Rapid Detection & Response solution uses Amazon Web Services (AWS) data centers to ensure the highest possible availability and fault tolerance, in addition to better response times and the ability to scale as needed. AWS states that each of their data centers are in alignment with Tier 3+ guidelines. For further information about the AWS datacenters, please see https://aws.amazon.com/compliance/

The collected behavioral event data from endpoints is stored on AWS in Europe (Ireland). Data retention for one year is included within the F-Secure Rapid Detection & Response subscription and there are no additional data storage fees based on the amount of data collected.

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.