

# WithSecure<sup>™</sup> Elements Endpoint Detection and Response

WithSecure<sup>™</sup> Elements - Reduce cyber risk,  
complexity and inefficiency.

# Contents

1. Executive summary .....	3
Flexibility to build resilient cyber security with WithSecure™ Elements .....	3
Benefits of the integrated solution .....	4
Introducing WithSecure™ Elements Endpoint Detection and Response .....	6
2. Key benefits .....	7
3. Solution overview .....	9
3.1 Management portal: Elements Security Center .....	10
3.2 Endpoint clients .....	11
3.3 Application visibility .....	12
3.4 Behavioral Analysis .....	13
3.5 Broad Context Detection™ .....	13
3.6 Incident management.....	13
3.7 Guidance to respond .....	14
3.8 Elevate to WithSecure™ .....	15
3.9 WithSecure™ Co-Monitoring Service .....	15
3.10 Automating actions.....	15
3.11 Advanced Response Actions.....	16
3.12 Event Search .....	16
3.13 Event Search for Threat Hunting.....	16
4. Data security.....	17
4.1 Data protection and confidentiality .....	17
4.2 Data security measures .....	17
4.3 Data centers .....	17

DISCLAIMER: This document gives a high-level overview of the key security components in the WithSecure™ Elements Endpoint Detection and Response solution. Details are omitted in order to prevent targeted attacks against our solutions.

WithSecure™ is constantly improving its services. WithSecure™ reserves the right to modify features or functionality of the Software in accordance to its product life cycle practices.

Last updated: December, 2023

# 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 data breaches. The average cost of a data breach is over four million dollars.<sup>1</sup> Fileless attacks are commonly not recognized by traditional antivirus protection, and targeted attacks often go unnoticed for months or even years.<sup>2</sup> By using our WithSecure™ Elements Endpoint Detection and 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.

## Flexibility to build resilient cyber security using WithSecure™ Elements

In today's agile business environment, the only constant is change. WithSecure™ Elements offers companies all-in-one security that adapts to changes in both the business and the threat landscape, growing along with the organization. It offers flexibility in licensing models and in its pick-and-choose security technologies. WithSecure™ Elements integrates a full range of cyber security components, including vulnerability management, patch management, endpoint protection, and detection and response, into a single lightweight software package that is managed in one unified, cloud-based management console. Using the same console companies can manage

the security of their Microsoft 365 collaboration services and their security posture in cloud environments like AWS and Azure. The solution is available as a fully managed subscription service through our certified partners or as a self-managed cloud solution. Customers can easily shift from self-managed to a fully managed service, so companies that struggle to find employees with cyber security skills can stay protected amid the ever-developing attack landscape.

WithSecure™ Elements consists of five solutions that are all managed with the same console, WithSecure™ Elements Security Center, and complemented by our co-security services.

### WithSecure™ Elements Endpoint Protection:

WithSecure's multiple AV-TEST Best Protection winner, cloud-native, AI-powered endpoint protection can be deployed instantly from your browser and manage the security of all your endpoints, keeping your organization fenced in from attacks. WithSecure™ Elements Endpoint Protection covers mobiles, desktops, laptops and servers.

### WithSecure™ Elements Endpoint Detection and Response:

Gain full visibility to advanced threats with our endpoint detection and response. With our unique Broad Context Detection, you can minimize alert noise and zero in on incidents, and with automated response actions you can effectively stop breaches around the clock. WithSecure™ Elements. Endpoint Detection and Response covers desktops, laptops and servers.

### WithSecure™ Elements Vulnerability Management:

Discover and manage critical vulnerabilities in your network and assets. By exposing, prioritizing and automatically patching vulnerabilities you can reduce your attack surface and minimize entry points for attackers.

### WithSecure™ Elements Collaboration Protection:

Fortify Microsoft 365 cloud collaboration platform's built-in security measures with a powerful security layer to ward off malicious content and phishing attacks, and to detect account compromises and inbox rule manipulations. Our multi-layered approach goes beyond Microsoft's standard security controls, covering your email, calendar, OneDrive, SharePoint and Microsoft Teams.

### WithSecure™ Elements Cloud Security Posture Management:

Manage the security of your cloud infrastructure through the proactive identification of misconfiguration risks on a regular basis. The solution performs environment scans and completes comprehensive checks for insecure cloud configurations, providing guidance on the remediation steps for the found security issues.

WithSecure™ Elements Endpoint Protection (EPP), Endpoint Detection and Response (EDR), Vulnerability Management, Collaboration Protection and Cloud Security Posture Management (CSPM) are packed into a single automatically updated software packet, saving your time and money in software deployment and administration.

<sup>1</sup> Ponemon Institute's 2023 Cost of a Data Breach Report (research analysis by IBM Security) reported the average data breach cost to be USD 4.45 million.

<sup>2</sup> Ponemon Institute's 2023 Cost of a Data Breach Report indicated that average time to detect and contain data breach is 277 days (research analysis by IBM Security).

## Benefits of the integrated solutions

The modular WithSecure™ Elements solution adapts to your company's changing needs. Unified cyber security means easier licensing, fewer security management tasks and more productivity without sacrificing your company's cyber security posture. The cloud-based console – WithSecure™ Elements Security Center - provides centralized visibility, insights and management across all endpoints and cloud services. It is fully managed by one of our certified Managed Service Providers, or self-managed with on-demand support from WithSecure™ for tough cases. The Elements Security Center provides a single view to the security status combining Elements EPP, EDR, Vulnerability Management, CSPM, and Collaboration Protection.

All the Elements endpoint solutions (EPP, EDR, and Vulnerability Management) are using a single software agent that is required to deploy only once. The add-on solutions can then later be activated without having to deploy additional solutions. WithSecure™ Elements Collaboration Protection and Cloud Security Posture Management are cloud-based solutions that do not require installations to company endpoints. In addition to deployment and management benefits, WithSecure™ Elements solutions are designed to work together, maximizing the security benefits for the company. For example, you can change Elements EPP profile assignment based on detections from Elements EDR thanks to our outbreak control feature.

	Endpoint Protection standard	Endpoint Protection premium	Detection and Response	Vulnerability Management	Collaboration Protection	Cloud Security Posture Management
Advanced anti-malware and patch management	✓	✓				
Additional anti-ransomware protection with DataGuard and application control, and endpoint encryption management		✓				
Advanced threat protection			✓			
Vulnerability management and prioritization				✓		
Advanced cloud-based email and collaboration security for Microsoft 365					✓	
Manage cloud security posture through identification of misconfigurations in cloud infrastructure						✓

Note: available features may vary by operating platform

More information on [WithSecure™ Elements](#).

## Introducing WithSecure™ Elements Endpoint Detection and Response

WithSecure™ Elements Endpoint Detection and Response 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. It protects the business and its sensitive data by detecting attacks quickly, and enables fast response with expert guidance.

With its deep bidirectional intelligence and high level of automation, WithSecure'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.

The solution is uniquely backed by WithSecure™, which means that a detection can be elevated to WithSecure™ for further threat analysis by experienced cyber security experts. You can also choose to complement your EDR by using WithSecure's Co-Monitoring Service that is delivered by threat hunters who monitor severe-risk detections 24/7 or during

out-of-office hours. Co-Monitoring ensures that true positive incidents are escalated to the WithSecure™ partner or your own IT, with guidance on how to contain and remediate the threat.

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 WithSecure™, we combine our technology and that unsurpassable human expertise to deliver a world-class endpoint detection and response solution.

WithSecure™ Elements Endpoint Detection and Response 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.

### 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.

WithSecure™ Elements Endpoint Detection and Response as a post-compromise solution for detecting advanced attacks still requires a strong endpoint protection solution that blocks commodity threats, like ransomware.

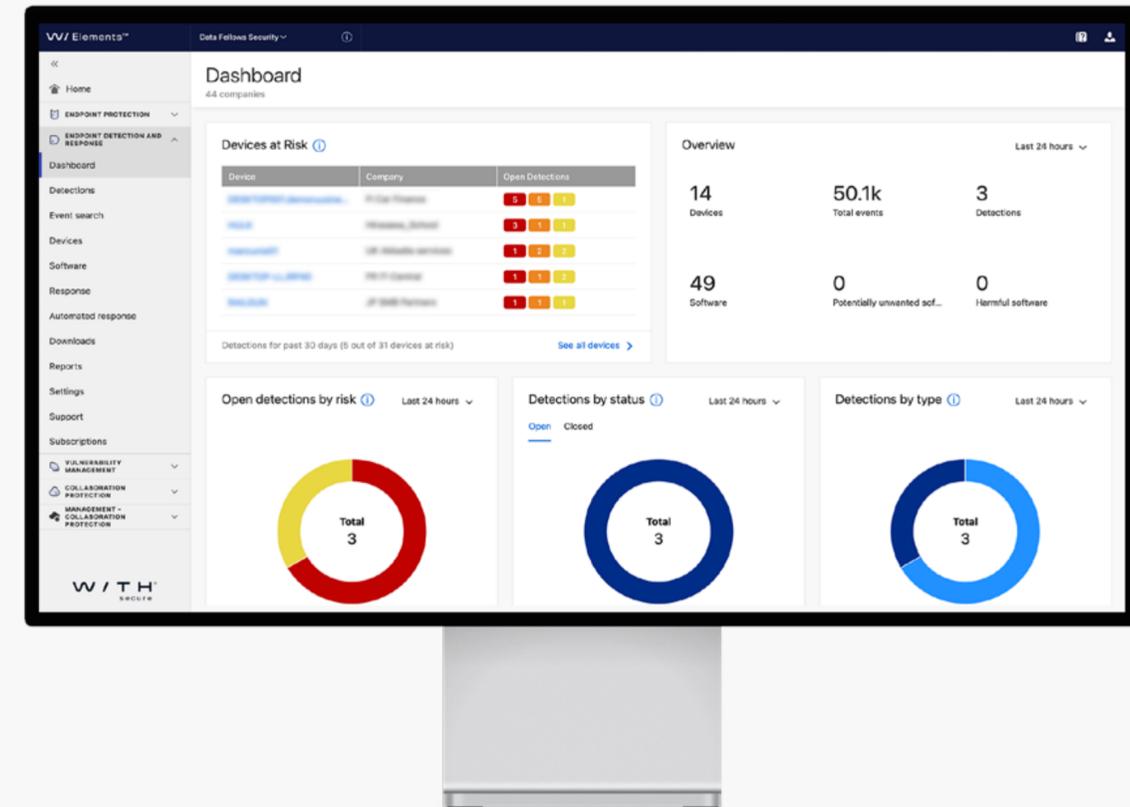
## 2. Key benefits

By using WithSecure™ Elements Endpoint Detection and 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 those by utilizing WithSecure'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
- Identify threats or signs of attack that were done in endpoint and are still active in memory when EDR functionality is activated
- 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, or use full incident data for your own SOC investigations

- 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
- Overcome skill or resource gaps in your teams by outsourcing advanced threat monitoring to an WithSecure™ certified managed service provider backed by WithSecure™ experts
- Take into use our additional WithSecure™ Co-Monitoring service with 24/7 or out-of-office hours monitoring by WithSecure's security experts, for your severe-risk detections that are generated by Elements EDR
- Alternatively for customers or partners with threat hunting capabilities WithSecure™ Elements for Endpoint Detection and Response can provide the full raw data on the incidents with additional Event Search for Threat Hunting service

## Solution to match your cyber security skills and resources

WithSecure™ Elements Endpoint Detection and Response can be acquired in multiple different ways that match your cyber security skills and resources:

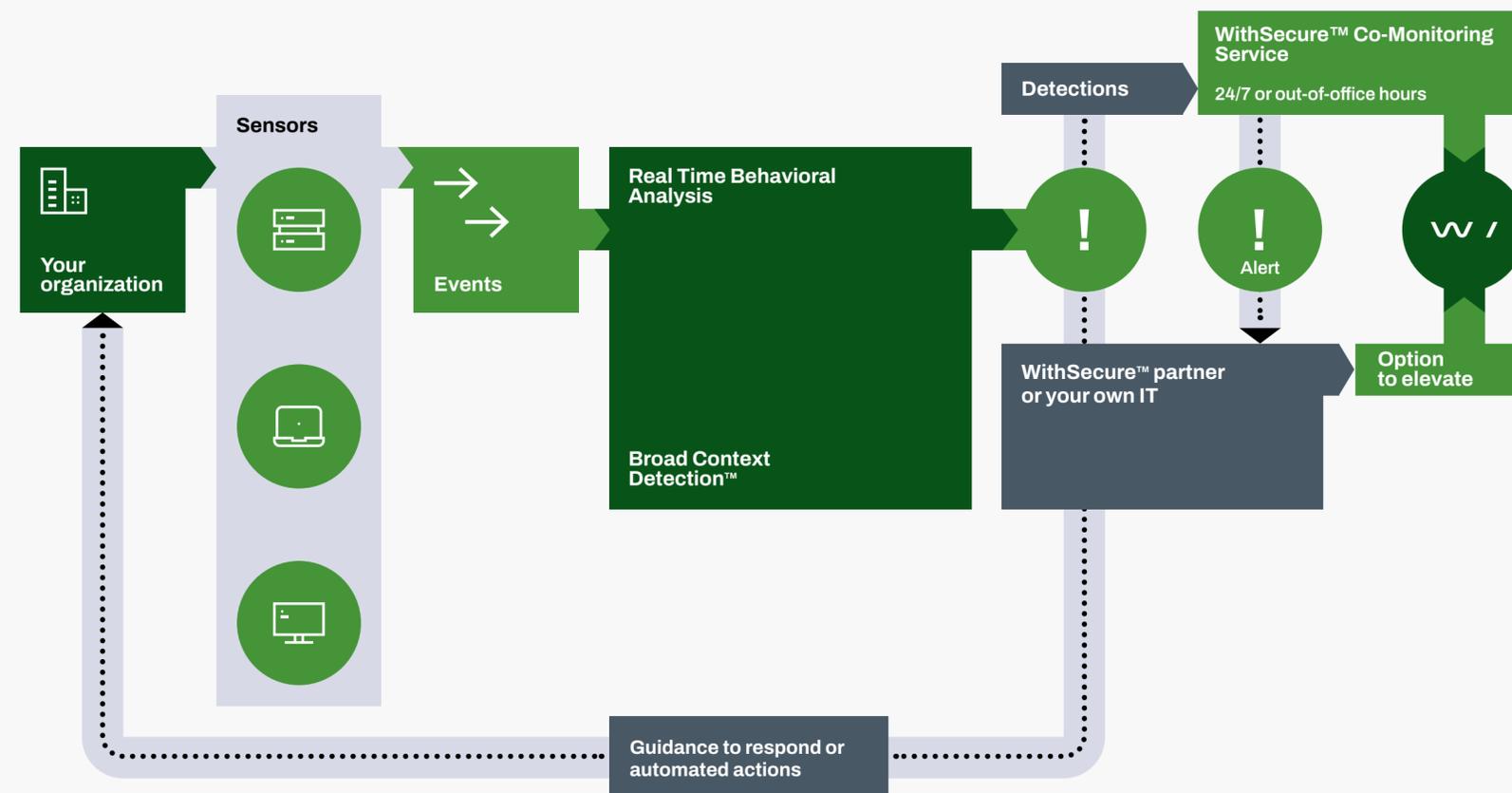
- 1. Fully managed service delivered by WithSecure™ partners:** this option is best for companies that want to be protected against advanced targeted threats but have a strategy to outsource their cyber security.
- 2. Managed in-house with incident help by WithSecure™:** this option is best for companies with limited cyber security skills. Difficult incident cases can be forwarded to WithSecure™ by using the built-in WithSecure™ Elevate feature.
- 3. Managed in-house with Co-Monitoring Service by WithSecure™:** this option is best for companies needing 24/7 or out-of-office hours monitoring of severe EDR detections by WithSecure™, to have constant readiness for swift incident response. The service ensures that true positive incidents are escalated in a timely fashion to the customer representative, with remediation advice.
- 4. Managed in-house:** this option fits those companies that have IT department with cyber security skills on good level. The basic incident response flow covers detecting the incidents with help of Broad Context Detections and responding to those threats.
- 5. Managed in-house with full Threat Hunting capabilities:** this option fits for those companies with their own Security Operations Center (SOC) that can perform advanced threat hunting as part of their investigations.

### 3. Solution overview

WithSecure™ Elements Endpoint Detection and Response solution consists of a combination of easily deployable clients on hosts, a cloud-based Elements Security Center, 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.

The figure describes on a high level how the WithSecure™ Elements Endpoint Detection and 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.



You also have the option purchase our co-security services to help with severe **Broad Context Detections™**: You can elevate tough investigations to WithSecure™ via our built-in Elevate to WithSecure™ service. You can also choose to complement your EDR by using WithSecure's Co-Monitoring Service that is delivered by threat hunters who monitor severe-risk detections 24/7 or during out-of-office hours. Co-Monitoring ensures that true positive incidents are escalated to the representative WithSecure™ customer or partner contact, with guidance on how to contain and remediate the threat.

### 3.1 Management portal: Elements Security Center

The Elements Endpoint Detection and 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, but it complements especially WithSecure's Elements Endpoint Protection that can be managed from the same client and management infrastructure.
- 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 WithSecure™, 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 Edge, Mozilla Firefox, Google Chrome and Safari.

The management portal is available in English, Finnish, French, German, Italian, Japanese, Polish, Portuguese, Spanish (LatAm) and Swedish.

**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 especially seamlessly with our own endpoint security solutions.

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

### WithSecure™ Elements

	Windows workstations	Windows servers	Mac os	Linux
<b>Operating systems</b>	10 / 11	2022 / 2019 / 2016	13 / 12 / 11	<i>See User Guide for supported distributions</i>
<b>Single-client by WithSecure™</b>	Yes	Yes	Yes	Yes
<b>Behavioral events</b>	Yes	Yes	Yes	Yes
<b>Application visibility</b>	Yes	Yes	No*	No*
<b>Remote host isolation</b>	Yes	Yes	Yes	Yes

\* **Expected later: The feature is not yet available.**

**More information** about system requirements and client deployment in the user guide at <https://www.withsecure.com/userguides/product.html#business/edr/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.

#### Collecting event data to detect and contain threats

WithSecure™ Elements Endpoint Detection and Response collects data from a variety of endpoints to help detect and contain threats in your environment. This data is provided in three different ways:

1. **Broad Context Detection™.** This automated threat identification method is designed to spot real threats from vast amount of behavioral event data collected from company endpoints. In addition, with the built-in WithSecure™ Elevate feature you can request professional guidance from our specialized cyber security experts in solving tough cases. You can also choose to purchase WithSecure's Co-Monitoring Service for 24/7 or out-of-office hours monitoring of severe-risk Elements EDR detections.
2. **Event Search.** With this built-in feature you can view, search, and explore the event data collected from your company endpoints that are related to any Broad Context Detections.
3. **Event Search for Threat Hunting.** This advanced feature is used to explore and interact with all the raw event data collected from the endpoints. Its sophisticated filtering capabilities lets your cyber security experts at SOC execute proactive threat hunting to detect and stop the most sophisticated hidden threats. Event Search for Threat Hunting is an optional component of WithSecure™ Elements Endpoint Detection and Response.

### 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.

WithSecure™ 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 WithSecure™ combines data science and cyber security expertise – an approach WithSecure™ refers to as “Man and Machine”.

### 3.5 Broad Context Detection™

WithSecure'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, this may trigger Broad Context Detection™ to alert 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.

### 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 with matching process parameters, through a process called "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.

WithSecure'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 for responding to a wide range of advanced threats. 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.

### 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 WithSecure'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

### 3.8 Elevate to WithSecure™

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

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

WithSecure'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 WithSecure™ 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 WithSecure™ 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 WithSecure™ Co-Monitoring Service

WithSecure™ Co-Monitoring is a 24/7 or out-of-office hours monitoring service through which WithSecure's cyber security experts investigate and provide remediation advice relating to severe-risk Broad Context Detections™ generated by Elements EDR. WithSecure's Co-Monitoring Service comprises four primary service elements:

1. Maintaining constant watch over severe risk detections in customers' IT environments
2. Validating and investigating detections to establish if they are true positive incidents that require action to remediate, or false positives which can be closed

3. Ensuring that true positive incidents are escalated in a timely fashion to the correct contact customer representative(s) with the authority and ability to respond to the security incident
4. Providing advice to the customer representative(s) for containment and remediation of the incident, for example recommending network isolation of the affected systems or termination of malicious processes.

### 3.10 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.

### 3.11 Advanced Response Actions

Advanced Response Actions can be used to reduce the impact of targeted cyber attacks and to gather more information of the incidents and the IT environment. Response actions can be set for multiple endpoints at the same time increasing efficiency in responding to the incidents. In addition, endpoints that are currently not online will execute the actions immediately when becoming online.

The response actions available for WithSecure™ Endpoint Detection and Response include:

- performing network isolation for the endpoint (this response can be automated)
- scanning the endpoint for malware and other harmful content
- retrieving different kind of data, logs, process- and task lists
- deleting and isolating files, folders, registry data, processes, and services

By using these response actions, a network administrator can efficiently stop the data breach before they cause further damage to the business. Please note that advanced response actions are not available when used with WithSecure™ Business Suite products.

### 3.12 Event Search

With this built-in feature you can view, search, and explore the event data collected from your company endpoints that are related to any Broad Context Detections. Event Search allows to filter and search for events based on the time they occurred, and on the device and the organization where the event took place.

### 3.13 Event Search for Threat Hunting

This advanced feature is used to explore and interact with all the raw event data collected from the endpoints. Its sophisticated filtering capabilities lets your cyber security experts at SOC execute proactive threat hunting to detect and stop the most sophisticated hidden threats. As the feature includes much richer set of events (other than those related to the Broad Context Detections) the amount of data is also much bigger. For this reason, Event Search for Threat Hunting is an optional component of WithSecure™ Elements Endpoint Detection and Response.

## 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 WithSecure™ 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. WithSecure™ operates under the Finnish implementation of the EU Data Protection directive and the WithSecure™ Elements Endpoint Detection and Response solution has been designed in accordance with the European Union's General Data Protection Regulation (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 WithSecure™ 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 Endpoint Detection and 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 Elements Endpoint Detection and Response subscription and there are no additional data storage fees based on the amount of data collected.

# Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

