Solution overview

Part of WithSecure™ Elements
Extended Detection and Response (XDR)

WithSecure™ Elements Endpoint Detection and Response

See attacks. Stop them.

WITH secure

Contents

Last updated: September 2025
Information security classification: Public

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.

Introduction

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. 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.

Introducing WithSecure™ Elements Endpoint Detection and Response

The average cost of a data breach is over four million dollars.[1] Fileless attacks are commonly not recognized by traditional antivirus protection, and targeted attacks often go unnoticed for months or even years[2]. By using our WithSecure™ Elements EDR solution, you can gain contextual visibility into your security, automate threat identification, and stop attacks before data breaches involving the exposure of sensitive, confidential or otherwise protected data to an unauthorized party, like a cybercriminal, happen.

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.

[1] Ponemon Institute's 2024 Cost of a Data Breach Report (research analysis and publication by IBM Security) reported the average data breach cost to be USD 4.88 million.
[2] Ponemon Institute's 2024 Cost of a Data Breach Report indicated that average time to detect and contain data breach is 258 days (research analysis and publication by IBM Security).

Backed by cyber security experts

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 unsurpassable human expertise to deliver a world-class EDR solution.

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.

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.

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. 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 exposure management and extended detection and response, into a single lightweight software package. By having a single automatically updated software packet, you can save time and money in software deployment and administration. Elements consists of proactive and reactive security solutions that are all managed with the same console, WithSecure™ Elements Security Center, and complemented by Co-Security Services.

WithSecure™ Elements is available as a fully managed subscription service, through our certified partners or our WithSecure™ Elements Infinite service, or as a self-managed cloud solution. Customers can easily shift from self-managed to a fully managed service. In other words, companies that struggle to find employees with cyber security skills can stay protected amid the ever-developing attack landscape, thanks to the flexibile Co-Security Services.

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. 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, proactively.

By putting more effort into pre-compromise prevention, for example by adopting the WithSecure™ Elements Exposure Management solution, you're making it 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.

Elements Endpoint Security combines our EPP and EDR into one comprehensive package for endpoints

WithSecure™ Elements Endpoint Protection (EPP)
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 (EDR)
Gain full visibility into advanced threats with our EDR. With our unique Broad Context Detection™ technology, you can minimize alert noise and zero in on real incidents. Use automated response actions to stop breaches effectively around the clock. WithSecure™ Elements Endpoint Detection and Response covers desktops, laptops and servers.

Flexibly choose from our Elements software modules:

WithSecure™ Elements Endpoint Protection (Standard)	Advanced anti-malware and patch management
WithSecure™ Elements Endpoint Protection (Premium)	EPP Standard features plus additional protection including DataGuard, endpoint encryption, and application control
WithSecure™ Elements Endpoint Detection and Response	Advanced threat detection and response

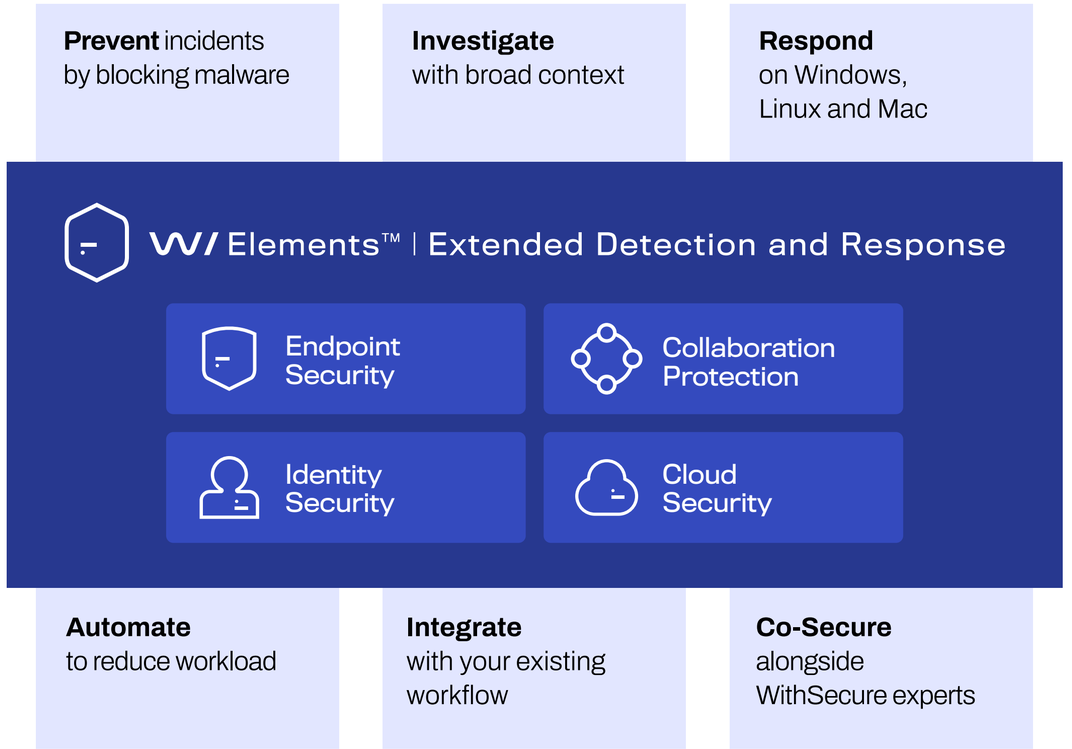
Available features may vary by operating platform. More information on WithSecure™ Elements

1. Part of WithSecure™ Elements XDR

Elements EDR is a module of WithSecure™ Elements Extended Detection and Response (XDR) that is designed for modern IT estates.

By choosing Elements Endpoint Security, you can have extensive protection, detection, and response for your company endpoint like workstations and servers. However, Elements XDR enables you to recognize the entire attack chain that poses a threat to your business, extending beyond endpoints.

Not only does Elements XDR enable organizations to understand and respond to advanced threats across endpoints, identities, cloud, emails, and collaboration tools, but its automated advanced preventative controls keep incident volumes and lower-level attacks at bay. Recognizing attacks early not only gives you a head start in reacting but can also save money by reducing the repercussions that follow from a compromised security posture.

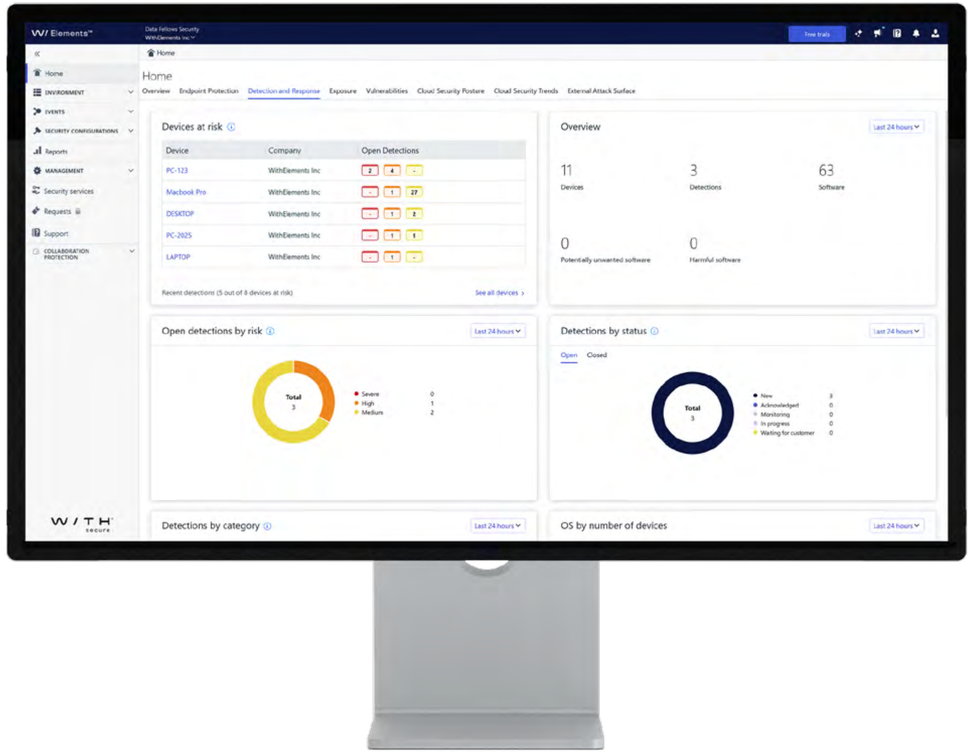


2. Key benefits

Gain visibility and speed in responding to attacks

By using WithSecure Elements EDR, 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. Gain immediate contextual visibility into your IT environment and security status. Some of the key benefits the solution delivers for visibility, detection and response are listed below:

- **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 24/7
- Overcome skill or resource gaps in your teams by outsourcing advanced threat monitoring to a WithSecure™ certified Managed Service Provider (MSP), 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 EDR can provide the full raw data on incidents with our additional *Event Search for Threat Hunting* service
- You can also opt for WithSecure™ Managed Detection and Response (MDR), our continuous 24/7 detection and response service, where our cyber security experts protect your IT environment by monitoring, investigating, and remediating cyber attacks across your estate.

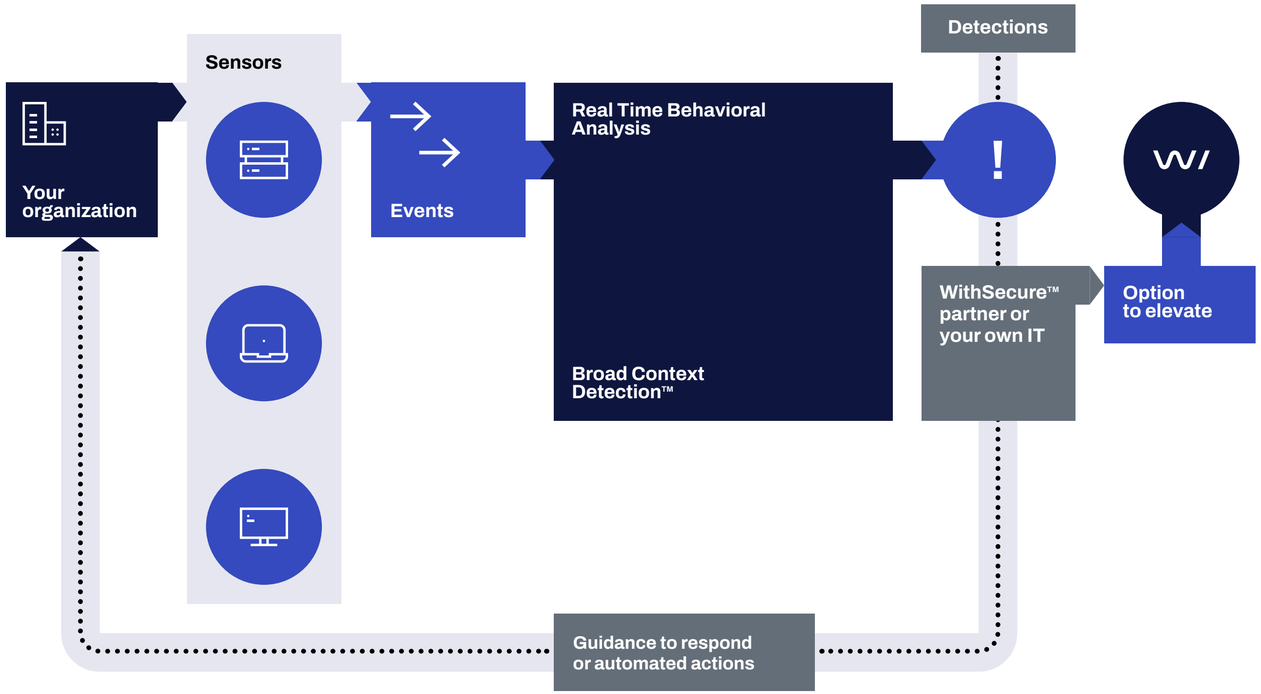
Solution to match your cyber security skills and resources

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

1. **Managed service delivered by WithSecure™ partners:** for companies that want to be protected against advanced targeted threats but have a strategy to outsource their cyber security.
2. **Managed by WithSecure™**: for broader detection and response capabilities and improved visibility into company IT infrastructure, we offer our industry-recognized WithSecure™ Elements Managed Detection and Response (MDR) service or our premium WithSecure™ Elements Infinite services.
3. **Managed in-house with incident help by WithSecure™:** for companies with limited cyber security skills. Difficult incident cases can be forwarded to WithSecure™ by using the built-in WithSecure™ Elevate feature.
4. **Managed in-house with Co-Monitoring Service by WithSecure™**: 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 Co-Monitoring Service ensures that true positive incidents are escalated in a timely fashion to the customer representative, with remediation advice.
5. **Managed in-house:** for companies that have an IT department with a good level of cyber security skills. The basic incident response flow covers detecting the incidents with help of Broad Context Detections and responding to those threats.
6. **Managed in-house with full Threat Hunting capabilities:** for companies with their own Security Operations Center (SOC) that can perform advanced threat hunting as part of their investigations.

3. Solution overview

WithSecure™ Elements EDR consists of a combination of easily deployable clients on hosts, a cloud-based Elements Security Center, and optional services. The solution provides functionality for detecting advanced threats and targeted attacks as well as for clarifying the overall risk and how to respond. The on-site part of the deployment includes an 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 using information on 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 to purchase our managed Co-Security Services to help with severe Broad Context Detections™: You can elevate tough investigations to WithSecure with our on-demand WithSecure™ Elevate service, which is in-built in the Elements platform. You can also 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

Elements EDR makes it easy to deploy, manage, and monitor the advanced threats on your endpoints from a single, intuitive, web-based console. It gives immediate contextual visibility into your IT environment and the 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™ Elements Endpoint Protection (EPP) that can be managed from the same client and management infrastructure.
- Detections are presented with actionable visualization to provide context for the targeted attacks on a timeline, including all impacted hosts, relevant events and recommended actions.
- By consolidating the threat management for 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, Portugese, Spanish (LatAm) and Swedish.

The partner managed version of the Elements Security Center 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 of Elements EDR on each operating system.

More information about system requirements and client deployment in the User Guide.

	Windows workstations	Windows servers	Mac OS	Linux
Operating systems	10*, 11	2025, 2022, 2019, 2016**, 2012**	13, 14, 15	*See the User Guide for supported distributions*
Single-client by WithSecure™	✓	✓	✓	✓
Behavioral events	✓	✓	✓	✓
Software reputation	✓	✓	*Expected later*	*Expected later*
Remote host isolation	✓	✓	✓	*Expected later*

* Windows 10's End of Support (EOS) is on October 14th, 2025. Extended support available, please contact our sales.

** Extended support available, please contact our sales.

3.3 Software reputation

Gaining extensive visibility into your IT environment and cloud services will reduce exposure to advanced threats and data leakage. Our solution’s software reputation 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 software reputation, 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:

- **Broad Context Detection™ (BCD).** This automated threat identification method is designed to spot real threats from a 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.

- **Event Search.** With this built-in feature you can view, search, and explore the BCD-related event data collected from your company endpoints.

- **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 additional component of WithSecure™ Elements EDR.

3.4 Behavioral Analysis

Behavioral Analysisis 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 are 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 the application of machine learning capabilities to continuously improve detections and reduce false-positives. The behavioral analysis capability is a prime example of how 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™ (BCD) 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. A Broad Context Detection flags indicators of possible breaches by alerting admins of Tactics, Techniques and Procedures (TTPs) used in targeted attacks. The indicators 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 BCD to alert you 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 with decisiveness.

GenAI Luminen™

Use our helpful Luminen™ GenAI as your investigation assistant. The security assistant analyzes and provides natural language explanations of Broad Context Detections™ (BCDs) from Elements XDR, enriched with relevant external threat intelligence. It empowers your IT team to focus on what matters the most by immediately assisting users of any experience level to better understand the context and impact of BCDs.

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, the Elements Security Center, to view details and take actions.

The BCDs are listed on the easy-to-use dashboard that helps you prioritize the incidents based on their risk score that 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 higher risk scores.

Actions for BCDs in incident management are the following:

- Acknowledge
- Mark to be in progress
- Mark as being monitored
- Close as confirmed
- Close as false positive
- Close 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 you in taking 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 the correct actions to contain and remediate threats.

Example activities causing 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 in 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. WithSecure™ Elevate 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 up the request within a 2-hour target SLA (Service Level Agreement). They will 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 to 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 that 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 enable initial response actions 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™ Elements 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 kinds 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 it causes further damage to the business. Please note that advanced response actions are not available when Elements EDR is used with the WithSecure™ Business Suite products.

3.12 Event Search

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

3.13 Event Search for Threat Hunting

This additional advanced feature is used to explore and interact with all the raw event data collected from the endpoints. Its sophisticated filtering capabilities let your cyber security experts at SOC execute proactive threat hunting to detect and stop the most sophisticated hidden threats. As the feature includes a much richer set of events (more than the events related to the Broad Context Detections), the amount of data is also much larger. 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 the 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 Elements 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 with the Elements Endpoint Detection and Response subscription and there are no additional data storage fees based on the amount of data collected.

5. Overview of WithSecure™ Elements Cloud Platform

Reduce cyber risk, complexity and inefficiency with our Elements Cloud platform. WithSecure™ Elements EDR is available as an integral capability in the modular WithSecure™ Elements cyber security platform.

WithSecure Elements provides customers with complete protection in one unified platform and easy-to-use security center. The centralized platform combines powerful predictive, preventive, and responsive security capabilities into intelligent protection against threats from ransomware to targeted attacks. Our unparalleled simplicity lets customers focus on what is the most valuable to them.

Modular product packages and flexible pricing models give customers the freedom to evolve. Select the pick-and-choose software modules your business needs and complement them with our flexible Co-Security Services. WithSecure™ Elements can be part of the customer's eco-system. It can easily be connected with their SIEM, SOAR, security management, monitoring, or reporting systems.

Try Elements today

Contact our sales to secure your data with speed

Contact sales

Who We Are

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies.

Committed to the European Way of data protection, WithSecure™ prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's cutting-edge offering is Elements Cloud, which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

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

WITH secure