Brochure

Stop targeted **attacks**

WithSecure™ Elements Endpoint Detection and Response

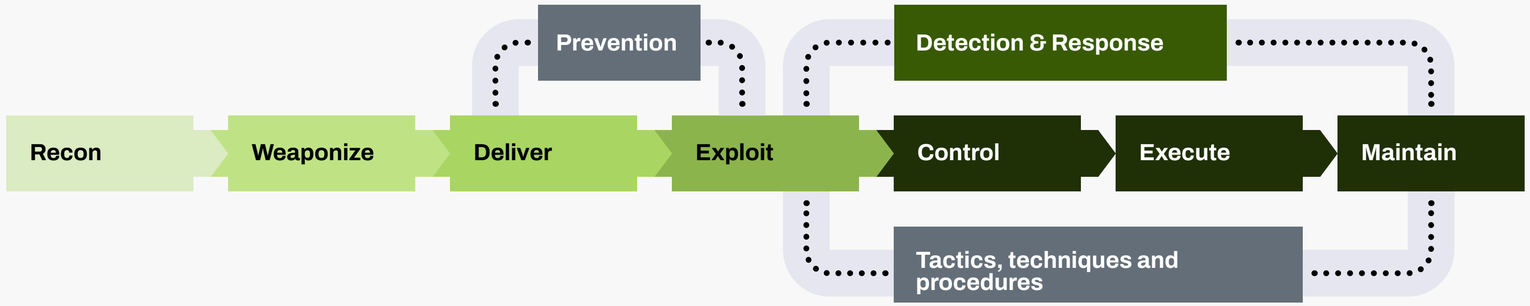
Protect your business and its data against advanced cyber attacks

Effective pre-compromise threat prevention is the cornerstone of cyber security, but you can't rely on preventive measures alone to keep your business and its data safe from the Tactics, Techniques and Procedures adversaries use in targeted attacks.

The continuously evolving threat landscape, along with regulatory demands such as GDPR, require companies to be prepared for post-compromise breach detection. That means ensuring a company is capable of rapidly responding to advanced attacks.

WithSecure™ Elements Endpoint Detection and Response solution, which is trained by an experienced threat hunting team, enables your own IT team or a certified service provider to protect your organization against advanced threats.

With the backing of WithSecure's world-class cyber security experts, your own IT specialists will be able to respond to incidents swiftly and effectively. Or by letting a service provider manage your organization's detection and response operations, you can focus on your core business and rely on expert guidance whenever under attack.



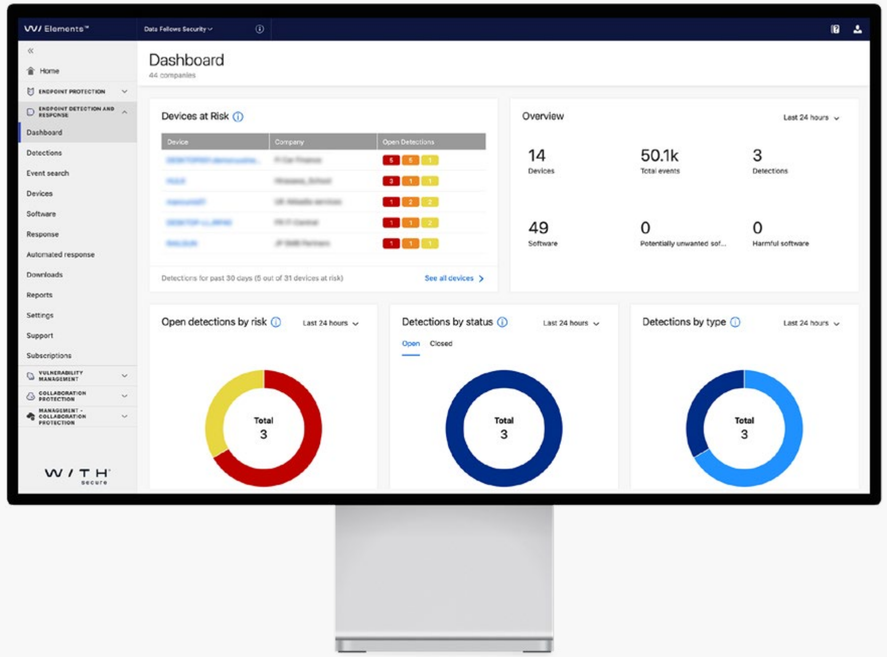
Overview

Stop targeted attacks quickly with guidance and automation

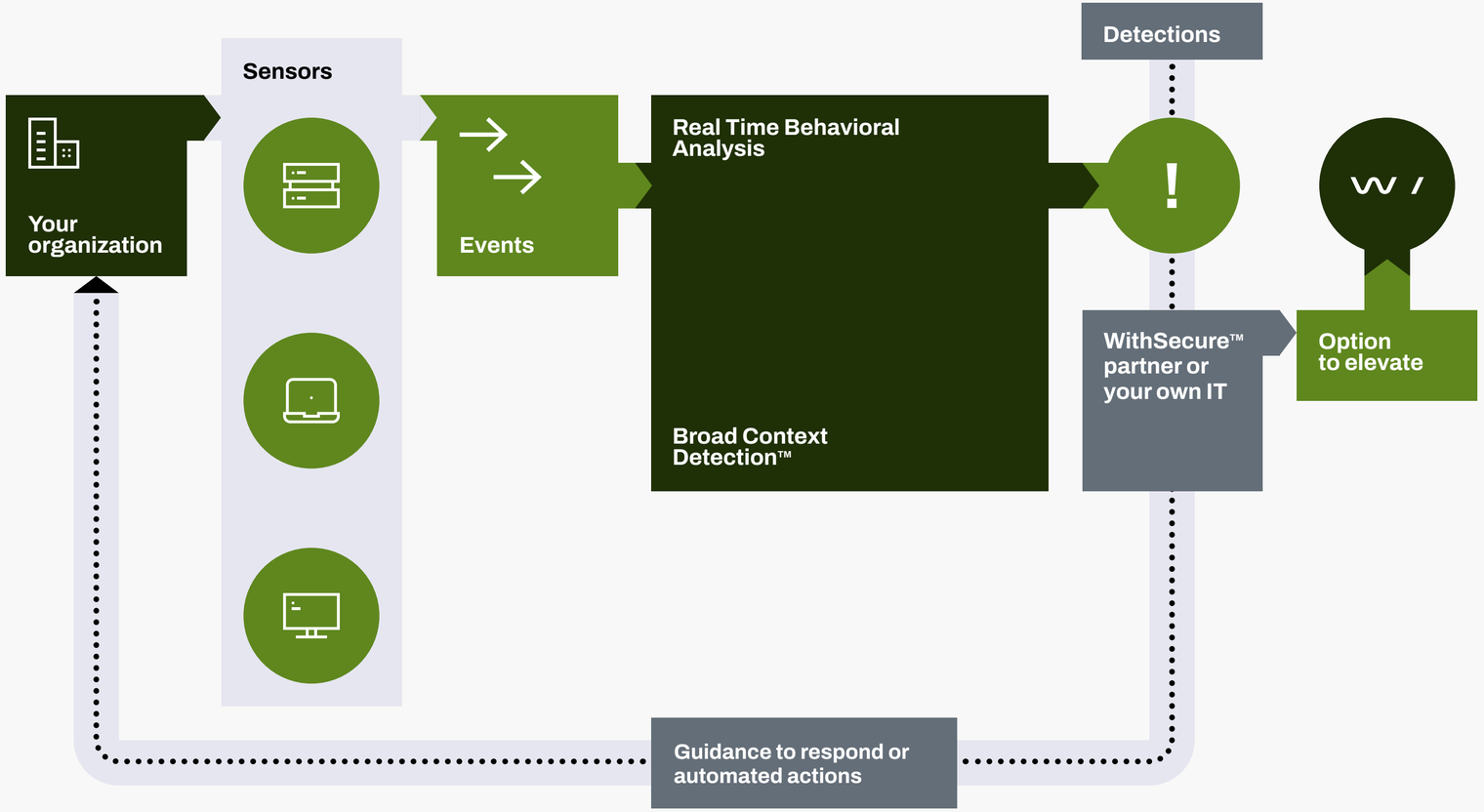
How do you detect a sophisticated attack? You make use of the most advanced analytics and machine learning technologies to shield your organization against advanced cyber threats and breaches

WithSecure's industry-leading Endpoint Detection & Response (EDR) solution gives you contextual visibility into advanced threats, enabling you to detect and respond to targeted attacks with automation and guidance.

When a breach occurs, you need more than just an alert. In order to plan the best response possible, you need to understand the specifics of the attack. Our Broad Context Detection™ mechanisms, together with certified service providers and built-in automation, will quickly stop the attack and provide actionable advice for further remediation actions.



How it works



WithSecure's industry-leading technology and cyber security experts at your service

1. Lightweight sensors deployed across endpoints monitor behavioral events generated by users, and stream them to real-time behavioral data analytics and Broad Context Detection™ mechanisms to distinguish malicious behavior patterns from normal user behavior.
2. Alerts with risk scores and visualized broad context across all impacted hosts makes confirming a detection easy, either by the WithSecure™ Partner or by your own IT team, with an option to elevate tough investigations to WithSecure™, or to automate response actions.
3. Following a confirmed detection, the solution provides advice and recommended response actions to guide you through the necessary steps to quickly contain and remediate the attack.

How it works

Looking for a needle in a haystack – a real world example

Detecting advanced threats by spotting the small individual events attackers trigger is like trying to find a needle in a haystack.

In a 325-node customer installation, our sensors collected around 500 million events over a period of one month. Raw data analysis in our back end systems filtered that number down to 225,000 events.

Suspicious events were further analyzed by our Broad Context Detection™ mechanisms to narrow down the number of detections to a mere 24. Finally, those 24 detections were reviewed in detail, with only 7 being confirmed as real threats.

Enabling IT and security teams to focus on fewer and more accurate detections results in faster and more effective response actions whenever under a real cyber attack.

500 million
data events / **month** collected by 325 endpoint sensors

225 000
data events / **month** cafter real-time behavioral analysis of the events

24
detections after adding broader context to the suspicious events

7
real threats after confirming detections as real threats

Benefits

Visibility

Gain immediate visibility into your IT environment and security status

- Improves visibility into IT environment and security status through application and endpoint inventory
- Identifies suspicious activity by collecting and correlating behavioral events beyond commodity malware
- Provides alerts with broad context information and asset criticality, making incident response easier

Detection

Protect your business and its sensitive data by detecting breaches quickly

- Detect and stop targeted attacks quickly to minimize business interruptions and negative brand impact
- Have the solution set up within hours, allowing you to be ready for breaches immediately
- Meet the regulatory requirements of PCI, HIPAA, and GDPR that require breaches to be reported within 72 hours

Response

Respond swiftly with guidance and automation whenever under attack

- Built-in automation and intelligence help your team focus only on real attacks
- Alerts include appropriate response guidance, with an option to automate response actions around the clock
- Overcome your skill or resource gap by responding to attacks with a certified service provider that is backed by WithSecure™

Features

Endpoint sensors

Lightweight, discreet monitoring tools designed to work with any endpoint protection solution

- Lightweight sensors are deployed on all relevant computers within your organization
- Single-client and management infrastructure with WithSecure's endpoint security solutions
- The sensors collect behavioral data from Windows, Mac and Linux devices without compromising users' privacy

Broad Context Detection™

WithSecure's proprietary detection technology makes understanding the scope of a targeted attack easy

- Real-time behavioral, reputational and big data analysis with machine learning
- Automatically places detections into a context visualized on a timeline
- Includes risk levels, affected host criticality and the prevailing threat landscape

Application visibility

Gaining visibility into your IT environment and security status has never been easier

- Identifies all harmful or otherwise unwanted applications, and the foreign destinations of different cloud services
- Leverages WithSecure's reputational data to identify potentially harmful applications
- Restricts potentially harmful applications and cloud services even before data breaches happen

Guided response

Prepares you to deal with even the most advanced cyber attacks with your existing resources

- Built-in step-by-step response guidance and remote actions to stop attacks
- Certified service providers guide and support you through response actions
- Unique Elevate to WithSecure™ threat analysis and expert guidance service backs you up

Automated response

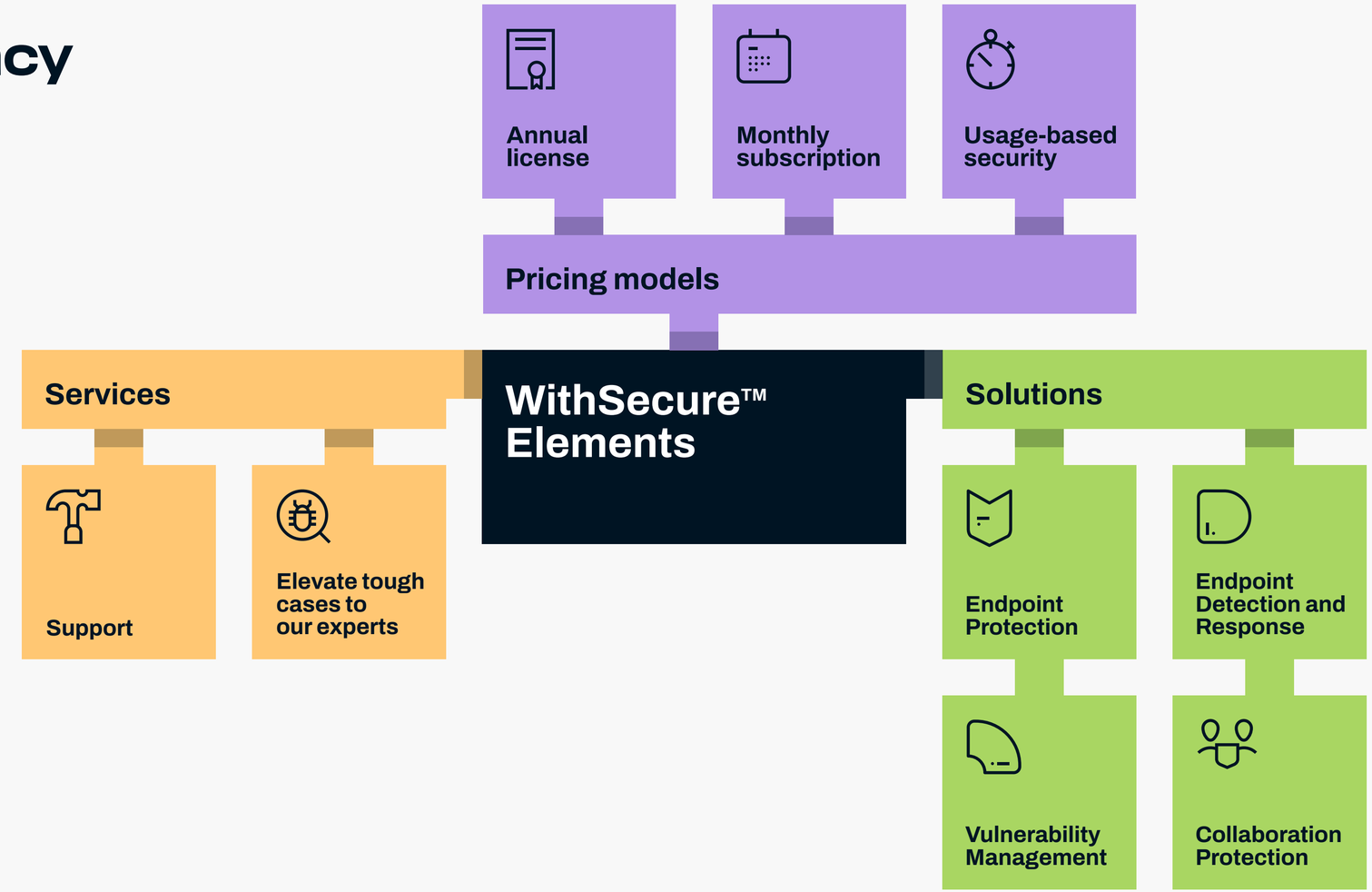
Reduce the impact of targeted cyber attacks by automating response actions around the clock

- Automated response actions based on criticality, risk levels and predefined schedule
- Criticality and risk levels provided by the solution allow prioritization of response actions
- Contain attacks quickly even if your team is only available during business hours

WithSecure™ Elements – Reduce cyber risk, complexity and inefficiency

WithSecure™ Elements Endpoint Detection and Response is available as a standalone solution or as an integral capability in the modular WithSecure™ Elements cyber security platform.

Try it yourself today



Who We Are

WithSecure™ 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 & response is 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™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure™