WithSecure™ Elements Exposure Management

Exposure remediation through the attacker's lens

September 2024

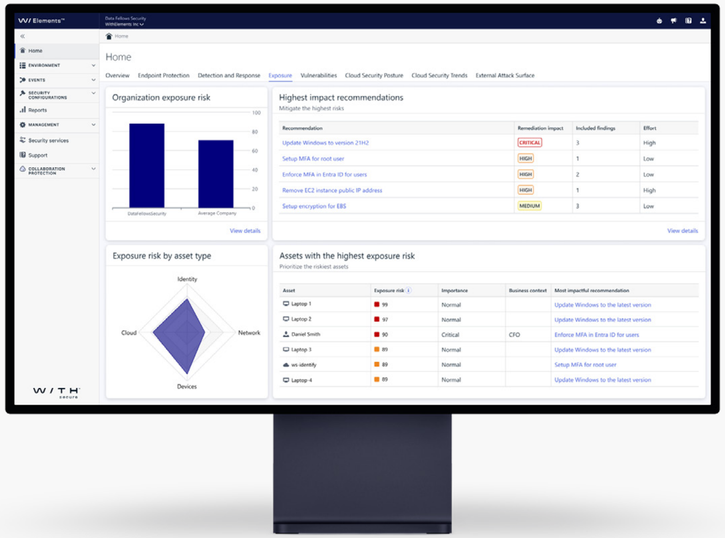
Introduction

WithSecure™ Elements Exposure Management (XM) is a continuous and proactive solution that predicts and prevents breaches against your company's assets and business operations. Elements XM provides visibility into your attack surface and its recommendations enable the efficient remediation of your highest-impact exposures from a unified view. Get one solution for 360° digital exposure management and visibility across your external attack surface and internal security posture, to proactively prevent cyber-attacks.

The shift from reactive to proactive cybersecurity has long been a priority for security professionals, but satisfactory solutions have been in short supply. In today's digital age, businesses face an ever-evolving threat landscape, with new vulnerabilities emerging constantly, especially with the development of Artificial Intelligence (AI) enabling new types of cyber attacks. Organizations have increasingly hybrid environments with unclear borders. The challenge is not only to protect the systems and data within these borders but also safeguard business continuity against external threats, like digital supply chain compromises.

The innovative and AI-powered WithSecure™ Elements Exposure Management (XM) addresses these challenges by providing comprehensive exposure management capabilities. WithSecure™ is the thought-leading Exposure Management provider for European small and medium-sized enterprises and Managed Service Providers – and for organizations that want cyber security done the European Way. Elements XM provides tooling and processes that evaluate how accessible and exposed an organization's digital assets are, and how easy it is to exploit them. The solution offers continuous recommendations by simulating attack paths, identifying critical vulnerabilities, and offering risk focused outputs to proactively strengthen defenses.

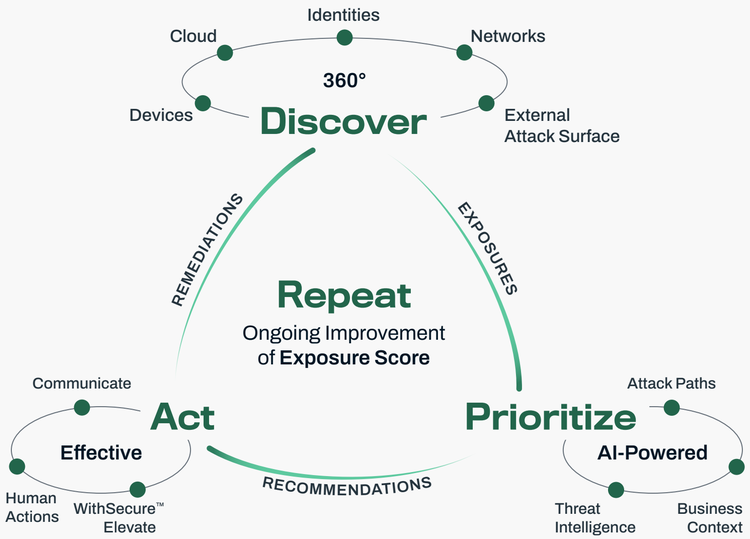
Most commonly, organizations are siloing exposure activities such as penetration testing, threat intelligence management, and vulnerability scanning. These siloed views provide little or no awareness of the whole situation regarding the effective risks the organization has. However, Elements XM combines data from your external attack surface, identity management systems (Entra ID), devices, network, and cloud services (Azure, AWS). The solution enriches this data with real-time threat intelligence and business context for a holistic security approach. The AI-powered recommendations include guidance for technical teams on how to take the most impactful actions to quickly improve security posture. Visual attack paths make security risks easy to understand for business decision-makers.



Our additional WithSecure™ Elevate service allows a specific recommendation to be sent to us for further analysis. This consultation from our experts ensures the validity and priority of the elevated item, providing further guidance.

Maximize your cyber resilience with minimum effort

Discover and act on your digital exposures before cyber criminals do. Elements XM offers continuous recommendations on how to improve security posture based on asset exposure scores that utilize business context, attack path modelling, and dynamic threat intelligence as their key inputs.



1. Discover
Discover your digital perimeter and identify the most critical assets and identities. See an overview of your attack surface from a single user interface, including assets like devices, cloud (AWS, Azure) and networks, as well as your external attack surface and identities (Entra ID). Get a 360° view of your organization's cyber risks, to identify its dangerous exposures without gaps in visibility.

2. Prioritize
Our findings on which exposures to prioritize in remediation are based on attack path simulation that integrates data from WithSecure's threat intelligence and your business context. You can have peace of mind against new attacks by having the latest threat intelligence data as an integrated part of exposure management, and know the solution is tailored to your individual business needs thanks to business context information. Ensure your most critical assets are being kept safe by using continuous exposure management, where our AI-powered recommendation engine combines related findings together and gives actionable recommendations on what to remediate next based on impact.

3. Act
Implement prioritized remediation actions to reduce your attack surface and decrease your business risk level, using our actionable guidance. Start working on protecting your attack surface by getting AI-powered recommendations to prioritize the most harmful exposures, or, if you're short of time, make quick fixes to exposures that have the highest impact, using minimal effort. Use WithSecure's Software Updater to apply missing patches instantly*. Communicate about the remediation process within the portal for smooth collaboration among your security team. The additional WithSecure™ Elevate service allows a specific recommendation to be sent to us for further analysis and validation. Repeat the process of discovering, prioritizing and acting on your exposures for continuously improving your organization's security posture.

* Requires a license for WithSecure™ Elements Endpoint Protection (part of WithSecure™ Elements Endpoint Security).

What is an Attack Surface?

"The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment"*.

What is an Identity?

Identity is a digital presence that can be a user, a group of users, or an entire organization. One person can also have multiple digital identities. Identities may represent humans or machines and can operate in on-premises, hybrid, regular, or privileged environments.

In the context of WithSecure Elements solutions, an identity consists of a collection of data associated with the entity, safeguarded by the Elements solution. This data may include Personally Identifiable Information (PII), access rights and privileges, roles and groups the entity belongs to, assets associated with the identity, online behavior and activity, contacts, and more. Our current implementation of Identities within Elements XM uses Entra ID as its foundation.

What are Attack Paths?

An attack path simulates the potential routes and actions an attacker might take within an organization's environment, with a focus on gaining access to the most business-critical assets. The reasoning engine of Elements XM is designed to prioritize the most accessible and likely actions by attackers, focusing on the primary attack paths, to ensure effective risk assessment and response activities.

* NIST (National Institute of Standards and Technology). "attack surface" definition (Sources: NIST SP 800-172 from GAO-19-128). https://csrc.nist.gov/glossary/term/attack_surface (Accessed 22.8.2024)

Why WithSecure™ Elements Exposure Management?

European Exposure Management
Thought-leading European Exposure Management with local threat intelligence, compliance, and privacy – as well as our over 30 years of real-world attack experience.

Visualized attack path modeling
AI-powered attack path modeling, where our reasoning engine and attack paths are built on heuristic scoring through the lens of the attacker.

Tackle identity-based risks
Covers identities as assets that are easily phished and stolen. Identities can be used as powerful choke points in breaking attack paths.

Designed for midsize businesses
Optimized for minimum effective security and designed to offer democratized cyber security for midsize organizations – providing ease of use with limited resources.

AI-powered recommendations
Creates actionable recommendations on what to remediate based on exposure risk scores that utilize our unique attack path modeling approach as their key component.

Unified security user experience
Part of the WithSecure™ Elements Cloud that offers a unified user experience from a single pane-of-glass, complemented by Co-Security Services such as WithSecure™ Elevate.

Benefits

Discover your Attack Surface

Know what makes up your attack surface by getting an overview of your environment including assets, external attack surface and identities, from a single user interface. Integrate data across your managed devices (workstations, servers), cloud services (AWS, Azure), identity (Entra ID), network (network equipment, unmanaged devices), and external attack surface (internet discovery, internet detections). See your environment through a single pane of glass.

Understand your Attack Paths

Attack paths expose various internal assets to cyber-attacks. Typically, an attacker would try to use these attack paths to reach critical company assets – for example, as part of a ransomware attack. Elements XM integrates data from your internal and external organizational environment that makes up your attack surface. It then enriches this data with intelligence about your business context and the latest threat intelligence to model potential attack paths into your organization. As the latest threat intelligence data is an integrated part of exposure management, you can have peace of mind knowing that you're protected against the latest attacks. The use of business context information enables the tailoring of our attack path modeling and recommendations to your individual business needs.

Elements Exposure Management detects detrimental attack paths that lead to crucial assets before attackers can exploit those paths. By identifying the choke points that can stop attacks on their tracks, Elements XM enables you to massively improve the protection of your company assets and data while minimizing the needed remediation effort. In other words, Elements Exposure Management focuses on breaking most of the dangerous attack paths into your organization first.

Remediate in a Prioritized Way

Ensure your most critical assets cannot be exploited and keep them safe by using AI-enabled continuous exposure management. Elements Exposure Management empowers your people with the right tools and means to remediate successfully. Start working on protecting your attack surface by getting AI-powered recommendations to prioritize the most harmful exposures, or, if you're short of time, make quick fixes to exposures that have the highest impact using minimal effort. You can also use WithSecure's Software Updater to apply missing software patches instantly, with a press of a button and without jumping between solutions*.

Our recommendation engine functions like a red team, a group of people pretending to be the cyber attacker, by looking for potential attack paths into your organization. While traditional red teaming is an occasional exercise, our Elements Exposure Management enables AI-run "virtual red-teaming" continuously. Elements XM helps you to recognize the critical weak points in your attack surface, like assets or identities, that can function as acceleration points in an attack path – and reversely from a defender's point of view as choke points in effectively breaking attack paths. Your security administrator can easily remediate the choke points of attack paths by using AI-powered recommendations, thereby minimizing the risk of cyber-attacks that succeed in causing compromise to critical company assets.

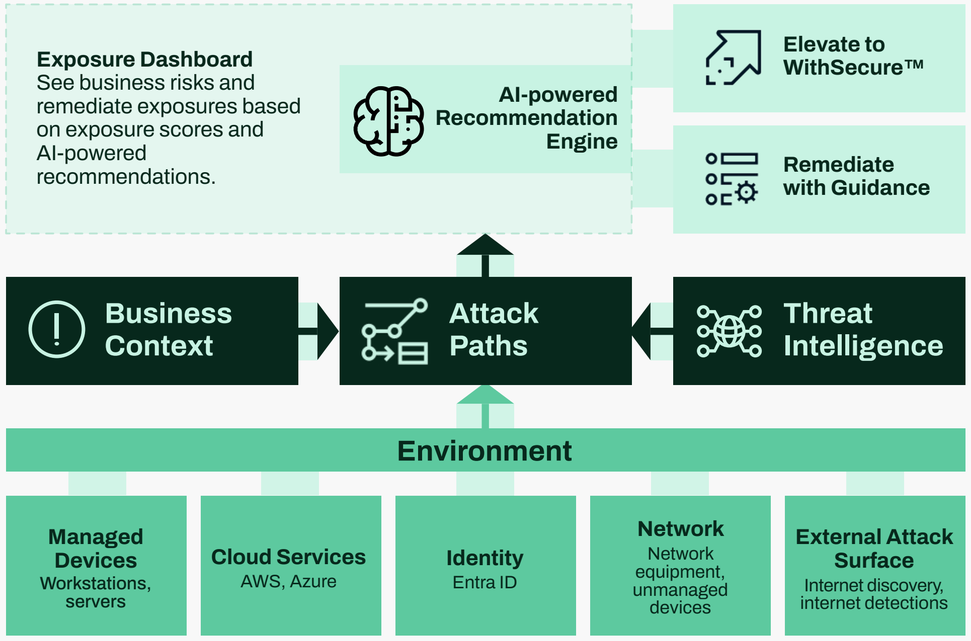
GenAI Luminen™

Use our helpful Elements Cloud platform AI assistant, Luminen, to get more value out of using the Elements XM solution (availability of assistant coming soon also to WithSecure™ Elements Exposure Management).

*Requires a license for WithSecure Elements Endpoint Protection (part of WithSecure Elements Endpoint Security) that includes the Software Updater functionality.

How it works

Get a 360° view of cyber risks. See your complete attack surface and remediate the highest-impact vulnerabilities, misconfigurations and other exposures that pose the most risk of intrusion to your organization. Safeguard the attack paths to your business-critical assets.



1. Elements Exposure Management integrates data from your internal and external environments to form a holistic overview of your attack surface:
   - External attack surface (covering internet discovery and internet detections)
   - Cloud services (Azure, AWS)
   - Identities (Entra ID)
   - Managed Devices (workstations and servers)
   - Network (network equipment like firewalls and switches, unmanaged devices)

2. Elements XM uses vulnerabilities, misconfigurations and other exposures in your environment to identify potential attack paths. It combines knowledge about the external attack surface with internal security posture information like asset vulnerabilities and cloud misconfigurations. This provides understanding about dangerous exposures and attack paths that lead to business-critical assets. Elements XM enriches the integrated data with up-to-date threat intelligence and your business context information, simulating attack paths based on this intelligence. The solution visualizes your attack paths and uses them to offer AI-powered recommendations that help you prioritize what to remediate next.

3. The overview provided by the Exposure Dashboard helps drive prioritized remediation actions and gives you a risk-based overview of the identified weaknesses in your attack surface. The AI-powered recommendation engine recommends remediation actions to you based on groups of findings with high impact on your overall exposure. Our recommendations come with practical guidance on how to take remediation actions. We also offer the quick action of using WithSecure's Software Updater to apply missing software patches instantly, with a press of a button*. Seeing the exposure scores of your company, your different asset types and individual assets further helps you in prioritizing remediation.
   - Additional WithSecure™ Elevate service allows a specific recommendation to be sent to us for further analysis. This consultation from our experts ensures the validity and priority of the elevated item.

*Requires a license for WithSecure™ Elements Endpoint Protection (part of WithSecure™ Elements Endpoint Security).

Continuously manage your digital exposures with our technology

Exposure Dashboard

No more alert fatigue. Keep exposure remediation simple and effective with our Elements Exposure Management dashboard, which shows you where to focus your remediation efforts from a single view. Understand your business risk and recommend actions to improve security posture. See how strong your attack surface is via the exposure summary view that gives you a risk-based overview of the identified weaknesses in your attack surface. See the business-critical assets at risk by using Exposure Scores to start prioritizing the remediation of the assets causing the severest risk of exploitation. Know the next steps to improve exposure by getting recommendations on what to fix first for quick and easy action, thanks to our AI-powered recommendation engine.

Attack Paths

Elements XM simulates the attack paths that an attacker could take to compromise a customer's estate. Instead of building attack paths that are optimized for the shortest route from the external attack surface to the business-critical assets, our reasoning engine and attack paths are built on heuristic scoring through the lens of the attacker. This means that our AI engine scans the customer's environment from an attacker's perspective, trying to find weaknesses by finding the path from one asset to the next that causes maximal damage. Our decision-making logic leans on decades of expertise on disassembling real-life attacks and on our Extended Detection and Response (XDR) detection telemetry.

This is what true AI-enabled red teaming means. Our recommendation engine functions like a red team – a group of people pretending to be the cyber attacker – by looking for potential attack paths into your organization. While traditional red teaming is an exercise that can occasionally be a useful investment for some companies, our Elements Exposure Management enables AI-run virtual red-teaming on a continuous basis.

Attack Path Visualization

Elements XM visualizes the attack paths related to a recommendation, enabling you to dive deeper into the underlying reasoning. Attack path visualization provides expanded information about the assets, steps and identities involved in the attack path, also covering the techniques used, access gained and related resources. The following are the key use cases of attack path visualization:

- **Validation**: Attack paths validate the recommendations provided by our AI-powered recommendation engine, enabling you to have informed response priorities for transparent decision-making.
- **Stakeholder Collaboration**: Facilitates communication of attack path insights to stakeholders – including customers, business decision-makers and IT administrators – thanks to easy-to-understand visuals.
- **Risk Assessment**: Provides alternative risk perspectives, enhancing your risk assessment activities.

AI-powered Recommendation Engine

WithSecure has been using multiple machine learning models to support detection and response capabilities for nearly a decade and our multi-year AI research project “Blackfin” was recognized by the AI Excellence award for collective intelligence techniques. Thanks to our AI-powered recommendation engine that finds attack paths between assets, Elements XM helps reduce your exposure risk level by giving recommendations on which exposures to address first. Our recommendations are based on exposure scores that utilize elements like our threat intelligence data feed, your individual business context information, and our cutting-edge AI-powered attack path modeling approach.

External Attack Surface Management (EASM)

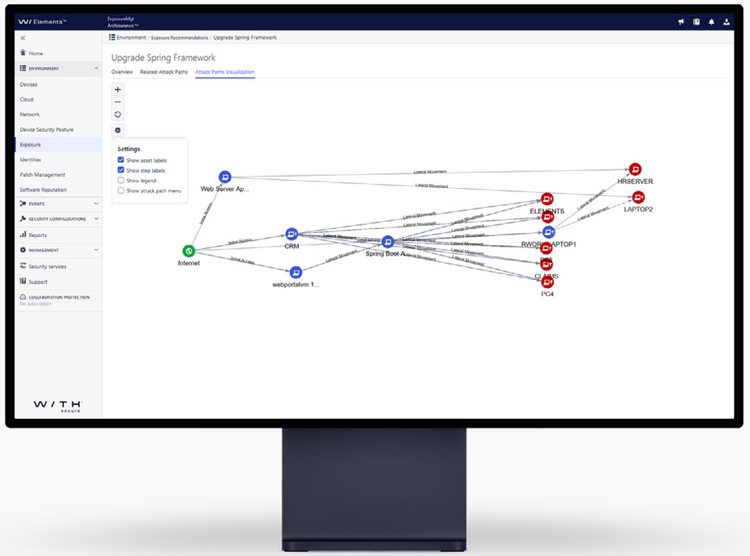
Protect your domains, IPs, and public-facing assets. Exposure Management uses Internet discovery via crawling and port mapping, to collect data on public systems. You can use the data based on location, top-level domain, pay-level domain, keywords, host name, and IP address. Internet detections help you detect risk of domain takeovers and information disclosure from directory listing. We are also continuously adding new internet detections based on the current threat landscape.

Exposure for Identity Risk

Use data on digital identities, whether human or non-human, and tackle identity-based risks by having your Entra ID data as an integrated part of Elements XM. This provides identity context for each exposure and includes identity-related data as an input in identifying dangerous attack paths. Cover the identity attack vectors that enable the potential escalation of identity access rights. Our exposure functionality for identity risks provides continuous assessment of identity-based risks in your environment and helps prevent the use of identity as part of attack paths. Take care of your own part in preventing supply chain breaches and improve employee security practices and security hygiene.

WithSecure™ Elevate

Elements user can request a specific recommendation to be sent to WithSecure to analyze and get WithSecure’s consultation on the validity and priority of the elevated item. Get support from our security experts for taking the next steps and understand why certain findings are important. Our team of threat hunters and security consultants will pick up the Elevate request, investigate the referred finding, recommendation or attack path and update the customer appropriately.



Scan your environment

WithSecure™ Elements Exposure Management combines multiple available scanning methods to ensure your full attack surface is covered:

Managed Devices and Network		External Attack Surface, Identity and Cloud Services		
Local / Cloud Scan Node	**Elements Agent**	**External Attack Surface**	**Identity Integrations**	**Cloud Integrations**
Discovery Scan Identify and map all assets within your network	**Agent-based Scan** Scan Windows workstations and servers automatically	**Internet Discovery** Identify your organization's internet-facing systems	**Entra ID** Discover potential threats associated with all identities in Entra ID	**Azure** Assess the security and compliance posture of your accounts
System Scan Scan all IP (Internet Protocol) systems for vulnerabilities and misconfigurations	**Device Service Data** System configuration and login information	**External Assets** Evaluate the security posture of your externally exposed assets	**Account Breach** Breached account information	**AWS** Assess the security and compliance posture of your accounts
Authenticated Scan* Log into systems to gain more detailed vulnerability data like vulnerable system versions, missing patches, and misconfigurations	**Patch Management** System and 3rd party patch status and automated updates via Software Updater**			
Web Scan Scan and test custom web applications for vulnerabilities				

* Not available through a cloud scan node.

** Requires a license for WithSecure™ Elements Endpoint Protection (part of WithSecure™ Elements Endpoint Security).

Note: Scans for Cloud Integrations are part of the WithSecure Elements Exposure Management for Cloud license, whereas the other scan types come as part of the WithSecure Elements Exposure Management for Users license.

Unified cyber security measures for extensive protection

We have been guiding customers through turbulent cyber security waters for well over 30 years and our modular cyber security solution, WithSecure™ Elements, brings XDR, Exposure Management and Co-Security Services to a unified pane of glass.

Good cyber security can't live in a silo. First, when using a fragmented cyber security tool stack, you must constantly jump from one portal to another. Alert fatigue is real, and managing multiple separate workflows is complex, making it challenging to prioritize. Second, management is not the only inefficiency. Solutions in a set-up like this don't co-operate – and can be completely oblivious of one another. This means silos, missed detections, slow responses and eventually a weaker security posture. To overcome the challenges of a siloed world, WithSecure™ Elements unifies core cyber security capabilities into one intelligent platform.

More elements mean more results, but you can build your own cloud-based cyber security suite with pick-and-choose technology modules. You can easily introduce new capabilities and ramp usage up and down as the time passes and your needs change. When you power up your cyber security stack with a unified combination of Exposure Management, Extended Detection and Response, and Co-Security Services, you can fend off a full spectrum of cyber threats. Unified technologies work together as one – from back-end to front – and are easy and efficient to manage from a single portal, the WithSecure™ Elements Security Center.

Elements Exposure Management offers consistent design with the rest of the Elements solutions, keeping it familiar to existing users and efficient to use for new users with multiple Elements products. Our transparent pricing model and consistent licensing models across all Elements solutions make software management easy. Security teams and partners alike can review all Elements products in one go, as part of their day-to-day role. Instead of siloed pointer solutions, WithSecure™ Elements gives you the means to protect your IT estate in a unified and efficient way. Intelligent technologies are powered by advanced AI and automation, lightening the load for you and your team. You can also offload your daily security management to our certified partners, and free up time to focus on more strategic activities.

Elements XM for cloud services identifies misconfiguration risks proactively

Elements XM for Cloud assesses the configuration of resources deployed in AWS and Azure, to identify weaknesses that could be exploited by an attacker. This includes tens of different AWS and Azure resource types and around two hundred configuration checks. The rule set we use is informed by both cutting-edge research and the latest attack techniques developed by WithSecure's cloud security experts, and by the best practices outlined by AWS and Azure.

WithSecure™ Elements – consolidate your cyber security

Unify your security technologies
security components work together seamlessly without loopholes using a shared data set, and are managed through a single portal, the WithSecure™ Elements Security Center

Be situationally aware
real-time visibility into your environment, including a complete picture of what is happening there, what your risks are, and how to prioritize them

Build your suite
customize your security palette with pick and choose modules

Adapt to changes
no strings attached, with straightforward licensing

Technical Requirements

Supported systems
As our management portal, WithSecure Elements Security Center, is cloud-based, all you need to access it is a modern web browser and internet access. We support the latest versions of the following browsers: Microsoft Edge, Mozilla Firefox, Google Chrome and Safari.

However, depending on which environments you want to onboard as part of WithSecure Elements Exposure Management, you will need to onboard your devices (Windows, Linux; see operating system requirements on the right), cloud accounts (AWS, Azure), network assets and identities (Entra ID). Please find more information about asset onboarding in the Exposure Management user guide.

Secure the environments that make up your attack surface
Our multi-environment approach covers the following assets and environments:

- External Attack Surface
- Cloud services (Azure and AWS platforms)
- Identities (Entra ID)
- Managed devices including workstations and servers
- Network including network equipment

Supported languages
English, Finnish, French, German, Italian, Japanese, Polish, Portuguese (Brazil), Spanish (Latin America), Swedish and Traditional Chinese (Taiwan).

Installation on Devices
Installation of Elements Agent requires one of the following Windows operating systems:

- *For devices:* Microsoft Windows 7, 8.1, 10 or 11
- *For servers:* Microsoft Windows Server 2016 or newer (full installation, not Server Core)

For installing scan nodes, the following operating system requirements apply:

- Windows Server 2012 R2 or newer
- Linux (Ubuntu Server and Debian (both 64-bit versions only); SSH)

Simple pricing model with two parts
Pricing per user: WithSecure Elements Exposure Management for Users (Identity, Network, Managed Devices and EASM)

Cloud bill tax: WithSecure Elements Exposure Management for Cloud (Cloud Services)

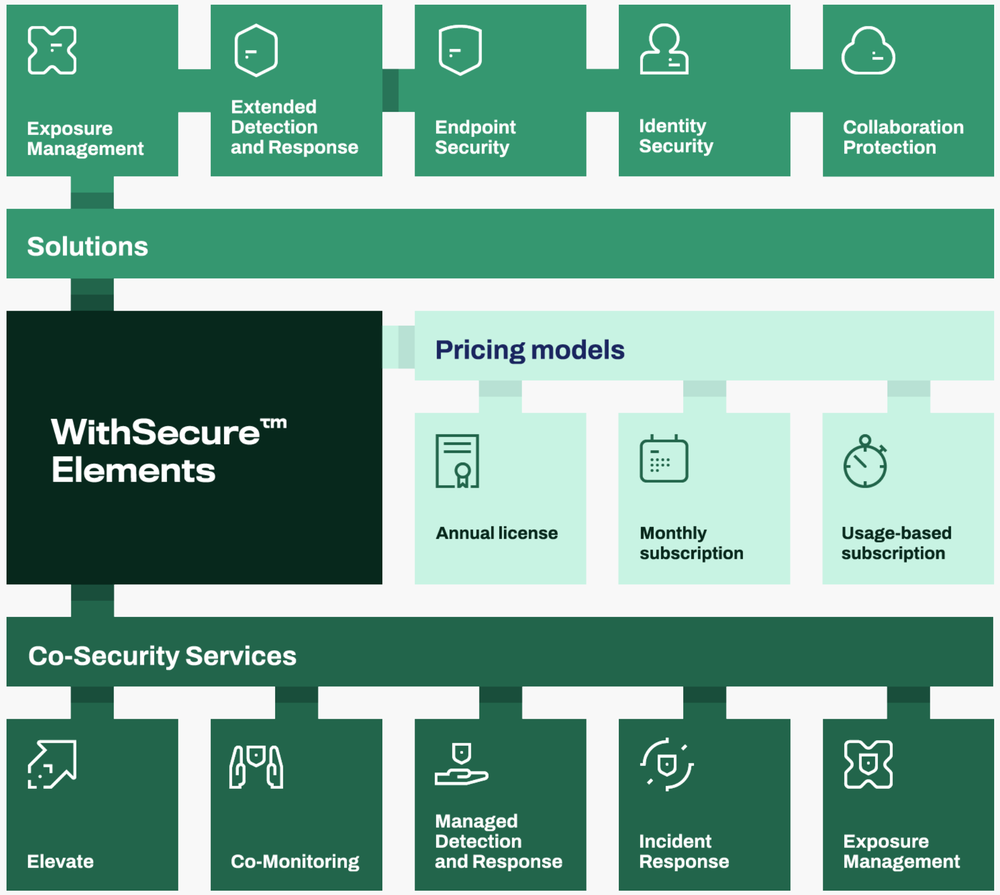
WithSecure™ Elements – Reduce cyber risk, complexity and inefficiency

WithSecure™ Elements Exposure Management 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. 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



Hack your business risk. Outsmart attackers.

Ready to maximize your cyber resilience with minimum effort by using WithSecure™ Elements Exposure Management?

Contact sales

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.

WITH secure