WithSecure™ Elements Cloud Security Posture Management

Manage cloud security posture through the identification of cloud infrastructure risks.

WITH secure™

WithSecure™ Elements Cloud Security Posture Management (CSPM) helps you to 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.

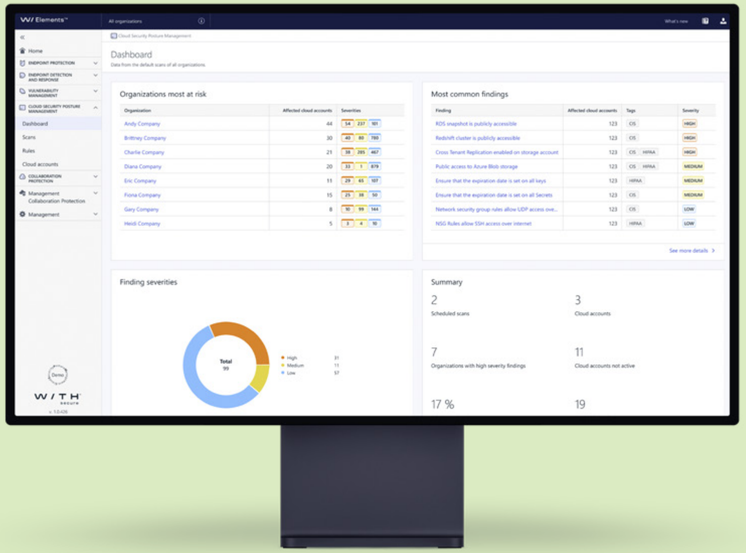
Organizations' IT environments are getting more and more multifaceted, combining technologies from multiple eras. Most enterprises operate hybrid, multi-cloud set-ups. These hybrid environments are not only complicated to manage but they are also hard to defend. Mistakes are inevitable.

What is key in cloud setups is the scope of configurations – or misconfigurations. The importance of configurations is enhanced in the cloud environment, as misconfigurations could mean opening an organization's resource to the internet. Misconfigurations pose a huge risk, as they can easily leave the cloud infrastructure and the data in it exposed to attackers. The risks related to misconfigurations have increased, as cloud attacks are opportunistic – attackers are looking for mistakes. These misconfigurations come in such quantity and variety that they can be hard to detect and manually remediate.

Moreover, cloud platforms are developed at a very fast pace, which means that some of the new functionality might also expose organizations to new risks. AWS and Azure introduce multitudes of new features and services each year, making constant changes to further increase the risk of misconfigurations. CSPM helps organizations to understand the risks that the new features and changes in the cloud environment might bring to their cloud estate.

Also, the scarcity of cloud security skills makes cloud vendors' tools for correcting misconfigurations hard to maintain, and users can have difficulty in interpreting the outputs of the tools. For example, engineering teams may oversee cyber security, and thus they may not understand the concepts and practices related to security as well as cyber security experts do.

Regulators requesting evidence that security controls governing data in the cloud are working, for example by doing regular auditing, add pressure for the cloud environment users. In the worst-case scenario, as data breaches can be costly, some medium-sized organizations could even go out of business, if they must pay a hefty fine for a breach.



Strengthen your cloud security posture

It can be complex to securely implement your cloud services while taking compliance into consideration. However, with our CSPM solution, you can control your cloud security posture despite the speed, complexity, dynamics, and scale of cloud deployments.

Visualize Your Risks

Risk severity is calculated and ranked as high, medium, or low. Risk-based guidance to remediate the cloud misconfigurations is offered. Easy-to-read reports visualize cloud security risks and empower correct responses for administrators, as well as help to report on security practices to auditors and regulators. CSPM also enables the visualization of historical data, and seeing your security posture at a time point in the past.*

Easy Management

Manage cloud credentials and your cloud security posture from one unified security center along with your existing endpoint security, collaboration protection and vulnerability management products. WithSecure™ Elements Cloud Security Posture Management (CSPM) brings visibility into your cloud environment and its risks. It gives you instant and constant insights into your cloud misconfigurations and gives you risk-based guidance on how you can remediate them.

Actionable Scans

Set up scheduled scanning of cloud accounts for assessing the security configuration of cloud resources or conduct scans on an on-demand basis. Apply groups of security rules to your cloud environments. The scans result in findings about your current security status as well as recommendations for improving your security status. Gain actionable insights of your risk status, prioritize efficiently, and remediate threats based on risk level to bridge security gaps quickly.

* Evolution based on historical data will be available in the general availability version, during November of 2023.

** AWS (n.d.). What Is IaaS (Infrastructure as a Service)? https://aws.amazon.com/what-is/iaas/ (Accessed 11.08.2023)

What is IaaS?

Infrastructure as a Service (IaaS) is a cloud computing service model, where IT infrastructure like storage, compute and network resources are provided over the internet on a pay-as-you-go basis.** AWS and Azure, both of which Elements CSPM currently covers, are prominent examples of this.

What are Cloud Accounts?

Cloud Account is an entity that allows segmentation and deployment of cloud infrastructure assets in the public cloud ecosystems, like AWS accounts or Azure tenants/subscriptions. This is also one of the methods of limiting and controlling access to the cloud infrastructure.

What are cloud-specific security misconfigurations?

It is important to realize that the public cloud and IaaS are layers of abstraction on top of the traditional layers that organizations protect and manage exposure risks for. The usage of IaaS comes with a whole new range of cloud specific risks that stem from insecure configurations or improper usage of the cloud services. Moreover, cloud providers' default configurations may not always be secure.

Why WithSecure™ Elements Cloud Security Posture Management?

Fortify your cloud security posture

Scan regularly

Conduct comprehensive cloud security posture scans that utilize the expertise of our research team about real-world threats.

Your cloud – secured

Coverage for AWS and Azure cloud platform infrastructures.

Prioritize efficiently

Review our visual CSPM dashboard to see important information which requires your attention, in easy-to-interpret graphs.

Risk-based guidance

We provide risk information and severity to allow you to understand and assess the risk to your organization.

Simplified reporting

Easy-to-read reports visualize cloud security risks and empower correct response for administrators – as well as help to report on security practices to auditors and regulators.

Consolidated security management

Manage your cloud security posture from one easy-to-use security center along with endpoint security, collaboration protection and vulnerability management.

Benefits

Spot mistakes before attackers do

We cover a wide range of use cases and make the user's daily job easier with intuitive views summarizing the security posture, and clear flows which focus only on the essentials.

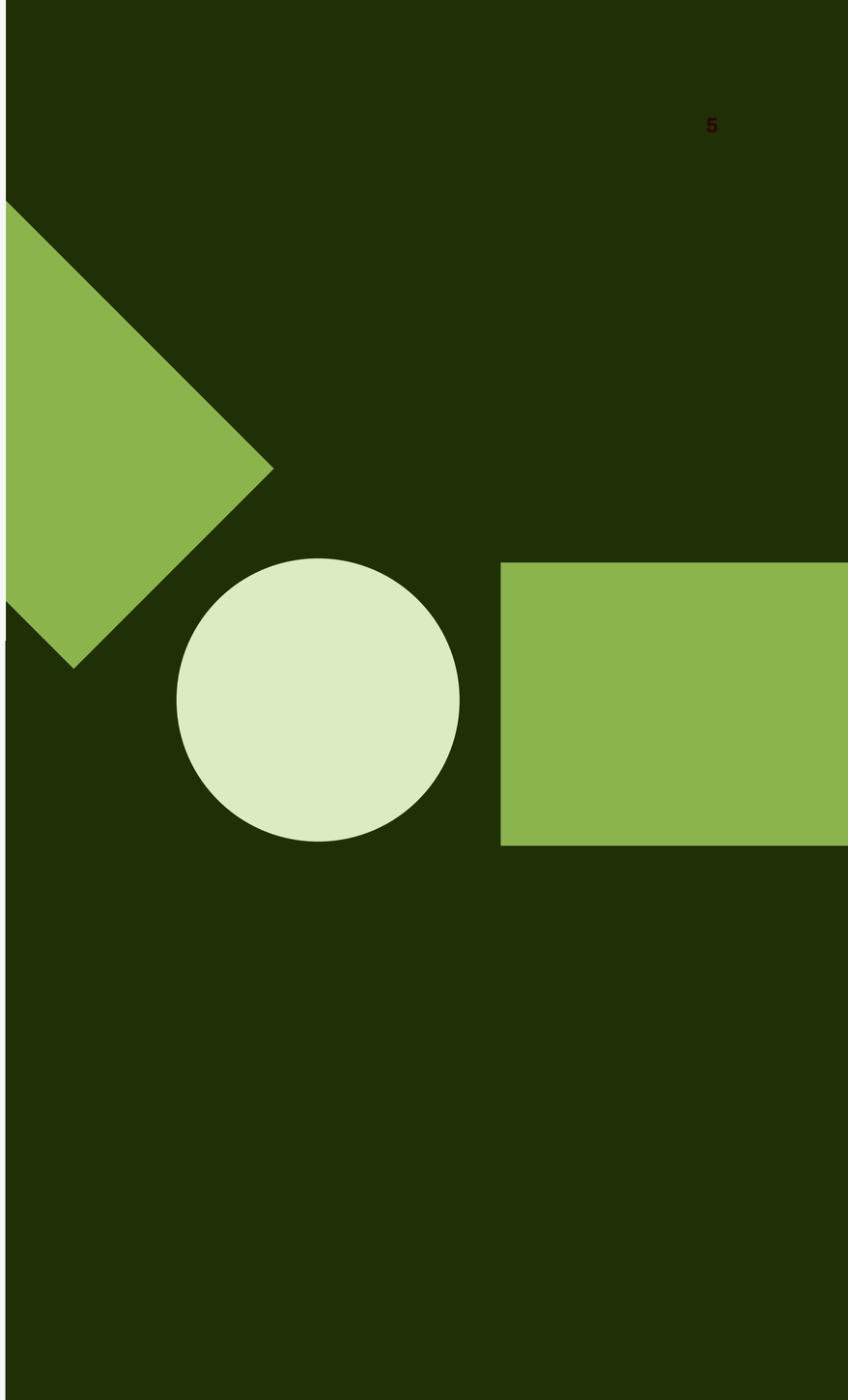
Identify misconfigurations quickly

Just add your account and start scanning. We save customers' and partners' time through enabling efficient detection of misconfigurations. The scans are fast, and you can easily see the evolution of the remediations.*

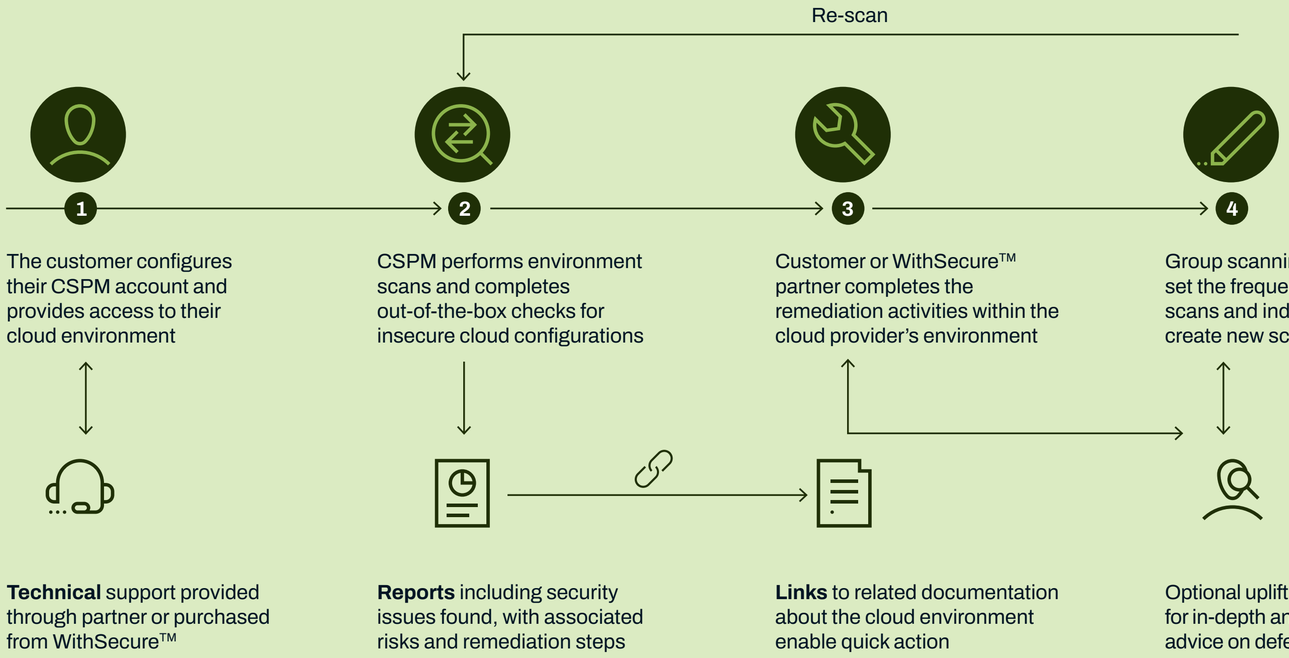
Reduce risk, complexity, and inefficiency

Prioritize remediation efficiently based on risk and effort level. Effectively remediate misconfigurations with helpful, actionable insights. Our visual reporting not only empowers administrators to make the changes that improve security posture the most, but also helps provide evidence to auditors and regulators.

* Evolution based on historical data will be available in the general availability version, during November of 2023.



How it works



1. The customer provides access to their cloud environment. CSPM is quick and easy to configure. If technical support for using the solution is needed, this can be provided by the WithSecure[tm] partner or directly by WithSecure[tm], for example through purchasing advanced or premium level technical support. Also, Technical Service Manager (TSM) services can be purchased from WithSecure[tm] for personal advice and support on using the whole Elements environment, including CSPM.

2. WithSecure[tm] CSPM technology performs environment scans, completes out-of-the-box checks for insecure configurations, and produces reports including security issues found, with associated risks and remediation steps. Moreover, links to relevant documentation about the cloud environment enable quick action.
   - If there are questions about the findings, customers can ask for advice on the report findings by purchasing consulting services from WithSecure[tm].

3. The customer or WithSecure[tm] partner completes the remediation activities within the cloud provider's environment.

4. Customers can independently create new scans, group scanning rules together and configure the scans' target accounts, as well as determine used scan rules and scan frequency. Customer can additionally purchase consulting services for optimization of security posture, including in-depth environment analysis, re-design of the environment and advise on defense in depth.

Customers can choose between managing Elements CSPM themselves, purchasing Elements CSPM from one of our trusted partners or alternatively, outsourcing Cloud Security Posture Management to WithSecure™ by purchasing it as a fully managed service.

Manage cloud security posture effectively with our technology

Scan and re-scan on a regular basis

Get visibility into your cloud infrastructure risks through the cloud security posture scan. The scan can be scheduled to run weekly, once every two weeks, monthly, or it can be run on an on-demand basis, to give you time between reporting cycles for remediation activities. CSPM provides information to help in prioritization and instructions for fixing misconfigurations based on their risk level. The solution also enables the downloading of scan results in PDF or CSV format.

Security posture for workloads on the most popular public cloud platforms

Currently CSPM covers both AWS and Azure. In total for both cloud platforms, there are around two hundred configuration checks. Our checks are continuously developed along with the evolving cloud environments. The checks have been built based on our cyber security expertise, real customer cases from the consultants within our Solutions unit, and major compliancy frameworks.

Expertise and research

Our WithSecure™ portfolio means we can draw on our consulting expertise to build checks that add security value based on in-depth client consulting engagements. Our research team has developed the checks based on their threat model, including misconfigurations attacks that are used to gain a foothold into customer environments. The checks include identification of overly permissive IAM privileges, unencrypted data at rest, cloud instances with access to public IP addresses and whether logging is enabled for incident investigation.

Dashboard

A dedicated view where we present the most important information which requires your attention in easy-to-interpret graphs. The graphical format conveys various useful information, like the evolution of security posture over time* and different security posture insights. Find out how the number of findings has changed over time and find the changes in posture to trigger more in-depth investigations*. As a WithSecure™ partner, you can also see which of the organizations that you manage are most at risk and how the security posture has evolved over time* by using different metrics.

MSP and MSSP Partner Support

We enable the possibility for partners, like MSPs and MSSPs, to provide CSPM as a managed service to their customers. Features like Elements Common Scope Selector and CSPM rule templates can help partner administrators to manage many end customers, and to provide various CSPM service levels for different customers.

* Evolution based on historical data will be available in the general availability version, during November of 2023.

Unifying Cloud Security Posture Management with preventive and responsive cyber security measures for extensive protection

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 vulnerability management, endpoint protection and endpoint detection and response, cloud security posture management and cloud application protection, 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 CSPM 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 makes 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.

Scanning of AWS and Azure Resources

CSPM 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

Integrate easily
connect security data easily with your third-party SIEM, SOAR, security management, monitoring or reporting systems

Adapt to changes
no strings attached, with flexible subscription options ranging from usage-based to annual

Technical Requirements

Supported systems
As Elements Cloud Security Posture Management is entirely cloud-based, all you need is a modern web browser and internet access. Elements CSPM supports the latest versions of the following browsers:
Microsoft Edge, Mozilla Firefox, Google Chrome, Safari

Secure workloads on the most popular public cloud platforms
Currently the multi-cloud approach covers both AWS and Azure IaaS (Infrastructure as a Service) platforms. Configuration checks are continuously developed along with the evolving cloud environments. The checks have been built based on our cyber security expertise, real customer cases from our consultants, and major compliance frameworks.

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

Installation
Installation of Elements requires one of the following Windows operating systems:
Windows Server 2008 R2 or newer (full installation, not Server Core)

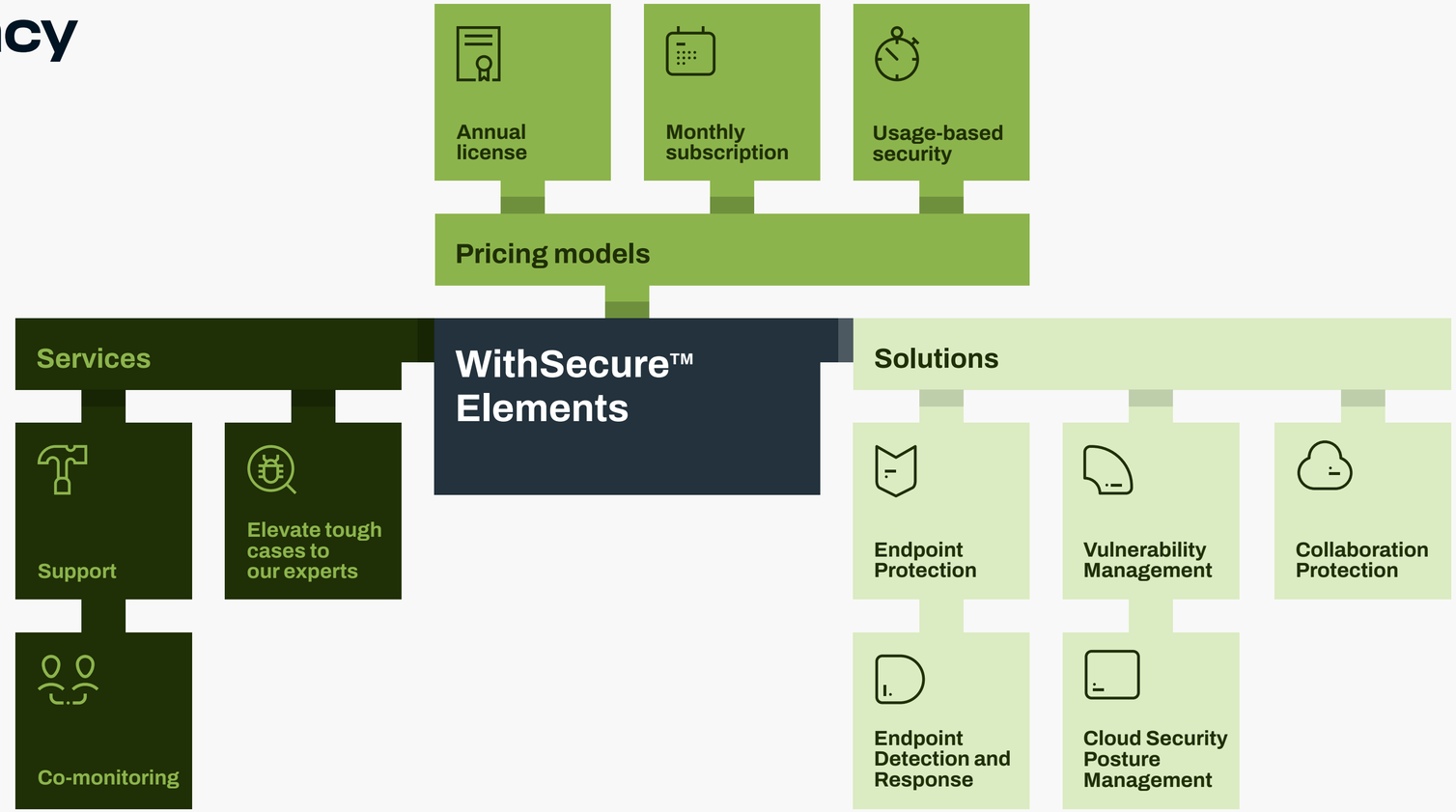
WithSecure™ Elements – Reduce cyber risk, complexity and inefficiency

WithSecure™ Elements Cloud Security Posture Management is available as a standalone solution or 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.

At any time, customers can elevate complex and critical cases to our elite threat hunters for investigation and response guidance. 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 it yourself today



Tackle misconfigurations, manage exposure and protect your workloads on cloud infrastructure platforms from a single easy-to-use security center, along with your other cyber security solutions. Manage CSPM yourself or co-secure your organization by outsourcing CSPM management to WithSecure™ or our trusted partner.

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