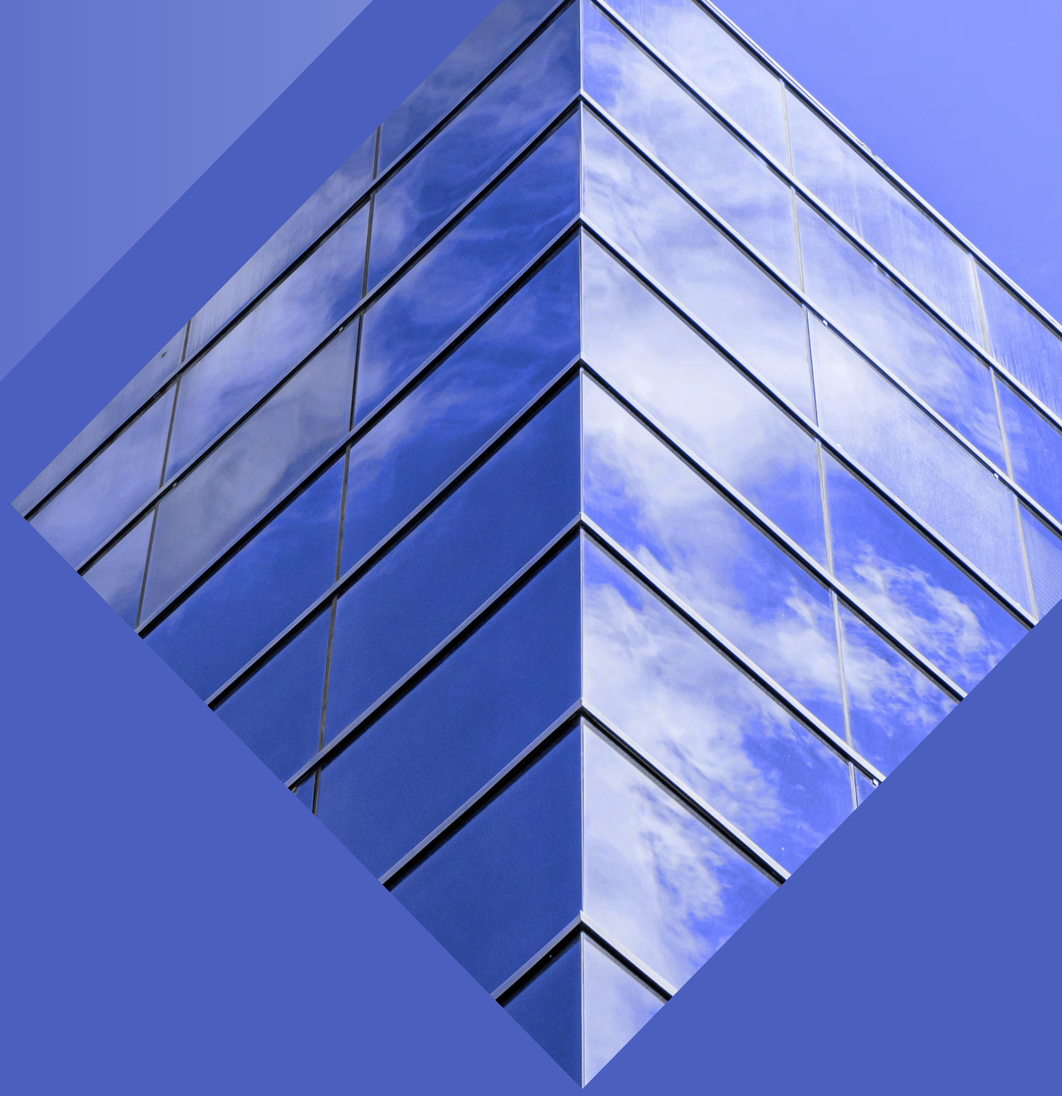
Solution overview

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



WithSecure™ Elements XDR Cloud Security

Don't let cloud attacks stop you

Contents

Last updated: September 2025
Information security classification: Public

Disclaimer: This document describes the Early Access version of the product and gives a high-level overview of the key security components in the WithSecure™ Elements XDR Cloud Security.
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

WithSecure™ Elements XDR Cloud Security provides threat research-based detection for your Azure cloud environment, securing your cloud resources against threats like data breaches, resource hijacking, and ransomware.

4 out of 5 data breaches involve data in the cloud*, making cloud-based attacks a real threat to your secure cloud transformation. Workloads are increasingly moving from on-premises to the cloud while still requiring similar security and access controls. Moreover, additional cloud specific controls and visibility are needed. Cloud resources need to be resilient against common cyber threats like data breaches, resource hijacking, and ransomware.

However, many cloud security tools produce too much work for a mid-size organization, making cloud security a challenging domain to master. CNAPP, CWS, CDR, CWPP — the list goes on for available cloud security tools on the market. These tools are nice to have, but often excessive for the average mid-market customer, as the tools have been designed for larger dedicated cloud teams to use. In other words, cloud security tools often create so much work that it is impossible for a single security analyst to manage and review everything. The cloud skills gap is a real and painful issue for the mid-market, meaning that the customer would need to invest in expensive cloud expert resources to protect their data properly with such solutions.

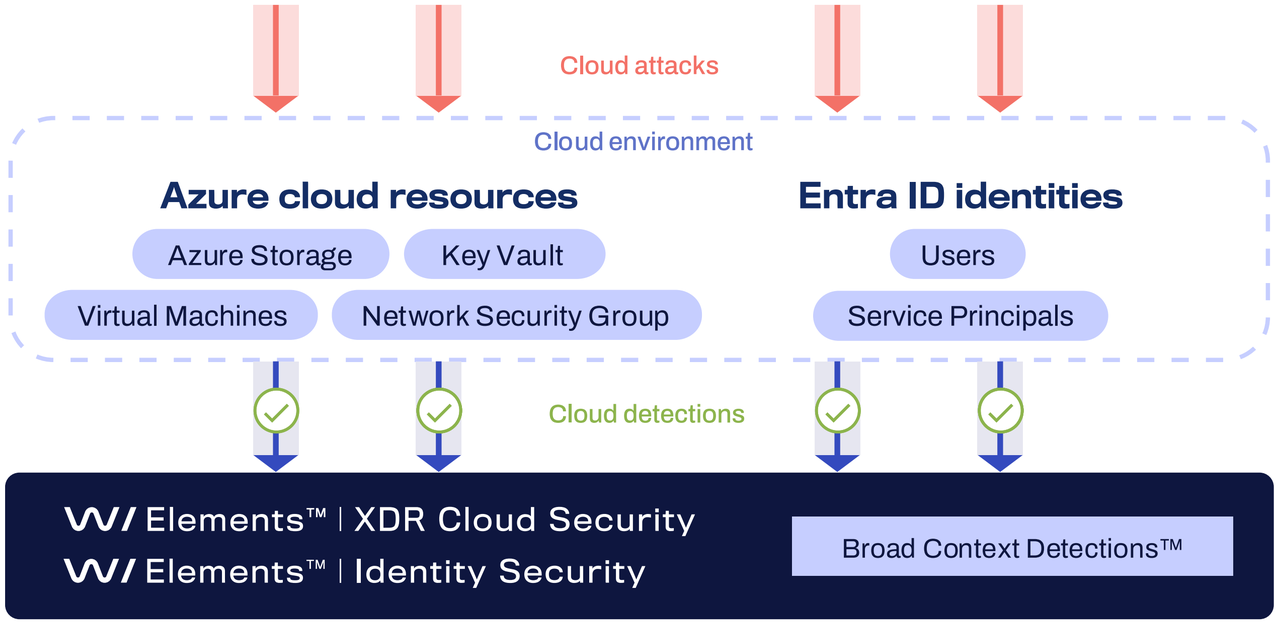
Moreover, the cloud is a complicated and new security domain to manage. Cloud environment adoption introduces an additional, complex attack surface that needs to be secured against cyber threats. When it comes to security in the cloud, data protection is up to you, as most vendors have a shared responsibility model for the cloud infrastructure they provide. The IT or security generalist of a midsized company needs an easy-to-use, effective cyber security tool to safeguard the company data in the cloud, which is continuously transferred as part of cloud workloads and integrated into cloud resources.

* Source: IBM Cost of a Data Breach 2024 report

WithSecure™ Elements Extended Detection and Response (XDR) Cloud Security

The solution provides easy-to-understand cloud detections with AI-powered recommendations. It empowers security analysts to quickly learn cloud tooling for the most important use case: taking quick action to mitigate cloud threats. Elements XDR Cloud Security delivers threat research-based detection for your Azure cloud environment, helping secure your cloud resources.

It is an easy-to-use solution that supports your cloud transformation from on-premise to hybrid setups mixing cloud and on-premise environments. The solution helps mitigate threats to your critical company data in the cloud and secures your seamless cloud-based service delivery. WithSecure™ Elements XDR Cloud Security for Azure produces Broad Context Detections™ that combine suspicious Azure cloud events and Entra ID identity related threat signals from WithSecure™ Elements Identity Security to form the full picture of a cloud attack.

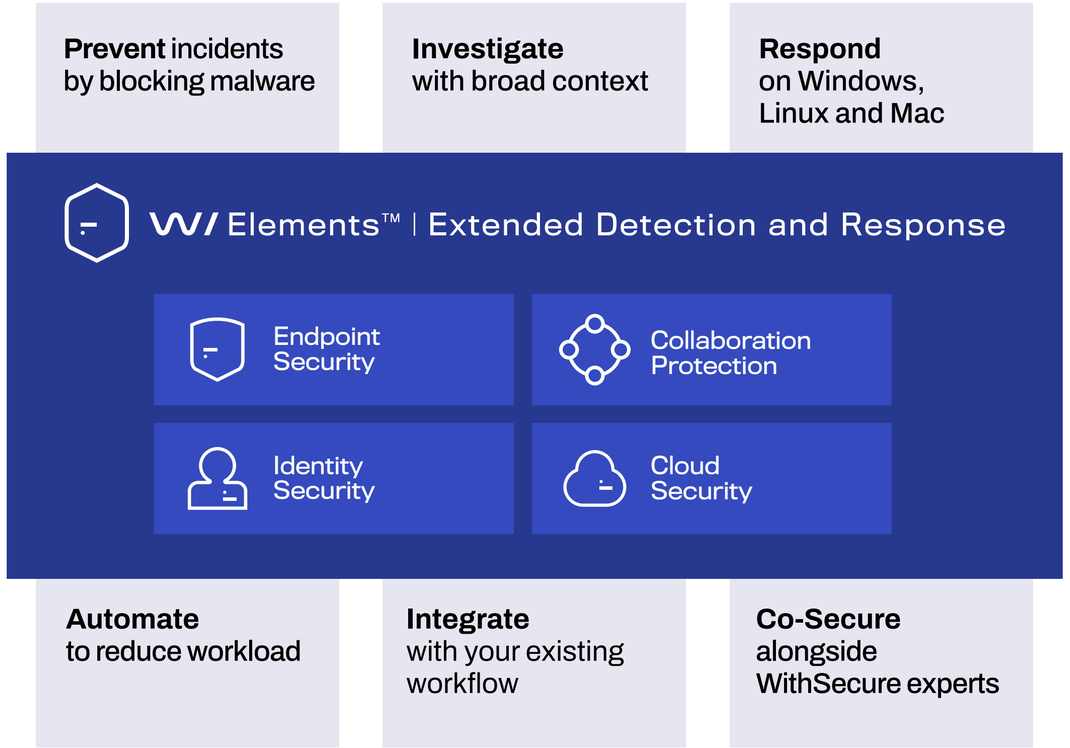


1. Part of WithSecure™ Elements XDR

WithSecure™ Elements XDR Cloud Security is a module of WithSecure™ Elements Extended Detection and Response (XDR) that has been designed for modern IT estates. Not only does Elements XDR enable organizations to understand and respond to advanced threats across endpoints, identities, emails and collaboration tools, but its automated advanced preventative controls keep incident volumes and lower-level attacks at bay. Elements XDR enables you to recognize the entire attack chain that poses a threat to your business, extending beyond endpoints. 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.

Why doesn't Endpoint Security cover the cloud broadly enough?

Endpoint Security (EPP and EDR) is not enough, as the modern attacks intertwine across traditional endpoint and cloud-adjacent Techniques, Tactics, and Procedures (TTPs). EDR can cover certain endpoint-like assets in the cloud, such as virtual machines, but cannot cover the wider spectrum of common cloud threats.
The rise of serverless workloads and Platform-as-a-Service (PaaS) offerings means that there's often no Operating System to attack or defend in cloud environments.
As an attack surface, the cloud is thus very different from a traditional on-premise network. The use of Public APIs for managing cloud infrastructure means that identity is a key component to securing the cloud.



Tap into the Power of WithSecure™ Elements Cloud

Elements XDR is part of our complete Elements Cloud platform that includes a wide range of tools and capabilities that are delivered from the cloud. Elements Cloud platform provides exposure management, automated patch management, dynamic threat intelligence and continuous behavioral analytics. Moreover, Elements Cloud allows you to manage all your security capabilities from a single, unified management portal – the Elements Security Center. Users of Elements Cloud can easily gain access to WithSecure's experts with our flexible Co-Security Services, so that you don't need to face cyber security challenges alone.

WithSecure's wide range of Co-Security Services seamlessly augment Elements XDR with flexible service options. For instance, when you experience ongoing major incidents, our Incident Response Retainer allows incidents to be smoothly escalated to our skilled and Service Level Agreement (SLA) backed incident responders. Our certified Incident Response experts have experience in handling challenging real-world cloud attacks, among many other demanding attack scenarios. Handoffs are seamless and well-practiced, and the incident response team can act quickly whenever your organization needs to minimize the impact of an attack. We also offer a 24/7 Emergency Incident Response hotline service (no SLA).

Why do you still need EPP and EDR (Elements Endpoint Security)?

Attackers are constantly seeking new ways to evade detection. It's a perpetual cat-and-mouse game between attackers and defenders. The increasing exploitation of Entra IDs indicates a lack of effective coverage against identity-based attacks. The rise in identity-related attacks doesn't diminish the importance of guarding against endpoint threats, as ransomware remains a significant threat to many organizations. For more detailed information, please refer to our latest Monthly Threat Intelligence Reports.

How does the pricing for XDR Cloud Security work?

We use a cloud bill tax model for pricing, similarly to WithSecure Elements Exposure Management for Cloud. This means that the pricing is based on a percentage (%) of the monthly cloud bill. Organizations provide us with their monthly cloud bill for Azure and convert it to "cloud units". Cloud units are calculated by dividing the monthly cloud bill (in euros) by 1,000.

2. Why WithSecure™ Elements XDR Cloud Security?

WithSecure™ Elements XDR Cloud Security empowers midsized organizations to secure their Azure cloud infrastructure with powerful threat detection via Broad Context Detections™ (BCDs). BCDs provide unparalleled visibility into threats across the hybrid IT environment that extends from on-premises to the cloud. Bridge the cloud skills gap and take cloud response actions effectively by using our Luminen™ GenAI assistant's recommendations.

Powerful detections against cloud threats

Protect your cloud infrastructure against threat research-based cloud attack vectors, with defenses against ransomware, data breaches, and resource-jacking.

Focus on efficiency and simplicity

Our democratized approach to cyber security and reasonable use of GenAI in security analyst workflows makes complex cloud security topics easier to understand – for security operators of all experience levels.

Designed for hybrid environments

WithSecure™ Elements XDR provides consolidated visibility across the hybrid mix of cloud environment combined with on-premise servers – a common setup in mid-size organizations.

Unify identity and cloud detections

Broad Context Detections™ connect the dots between your Entra ID identities* and Azure cloud infrastructure, enabling efficient responses cloud-related threats by consolidating all relevant information is in one place.

Part of WithSecure™ Elements Cloud

The unified experience provided by our Elements Cloud platform supports frictionless security analyst workflows, by integrating proactive Elements Exposure Management and reactive Elements XDR security capabilities.

Access expert services easily

For the times when you may experience ongoing major incidents, use our Incident Response Retainer for 24/7 SLA-backed Incident Response service provided by our highly skilled, certified experts.

*WithSecure Elements Identity Security license is required, as Elements XDR Cloud Security is designed as an add-on to Elements Identity Security.

3. Benefits

Ease the path to your cloud transformation

Ensure your critical company data is kept safe when taking cloud infrastructure into use. The cloud detections from Elements XDR Cloud Security help you to adequately secure your company data that is part of Azure cloud resources and workloads. The solution allows you to manage the security of cloud resources from the same management portal as your on-premise servers, with unified visibility across your hybrid IT environment. Moreover, you can cover both your proactive and reactive security needs with our single WithSecure™ Elements Cloud platform – by combining Elements XM (Exposure Management) and Elements XDR for extensive security across devices, identity, cloud environments, and your external attack surface.

Minimize financial losses with rapid response

Limit the damage caused by cloud attacks. Elements XDR Cloud Security detects incidents in your Azure cloud environment, enabling you to take quick response actions. The solution's tailored alerts save you time by letting you focus on incidents that matters the most in your business context. The solution provides clear, AI-powered descriptions on detection, associated risks, and remediation steps – to save your security analyst's time. Our Luminen™ GenAI assistant explains the cloud incidents in simple terms and provides recommendations on how to respond in multiple local languages. These insights enable you to prevent data breaches easily, thus minimizing your financial losses.

Fortify your operational processes in the cloud

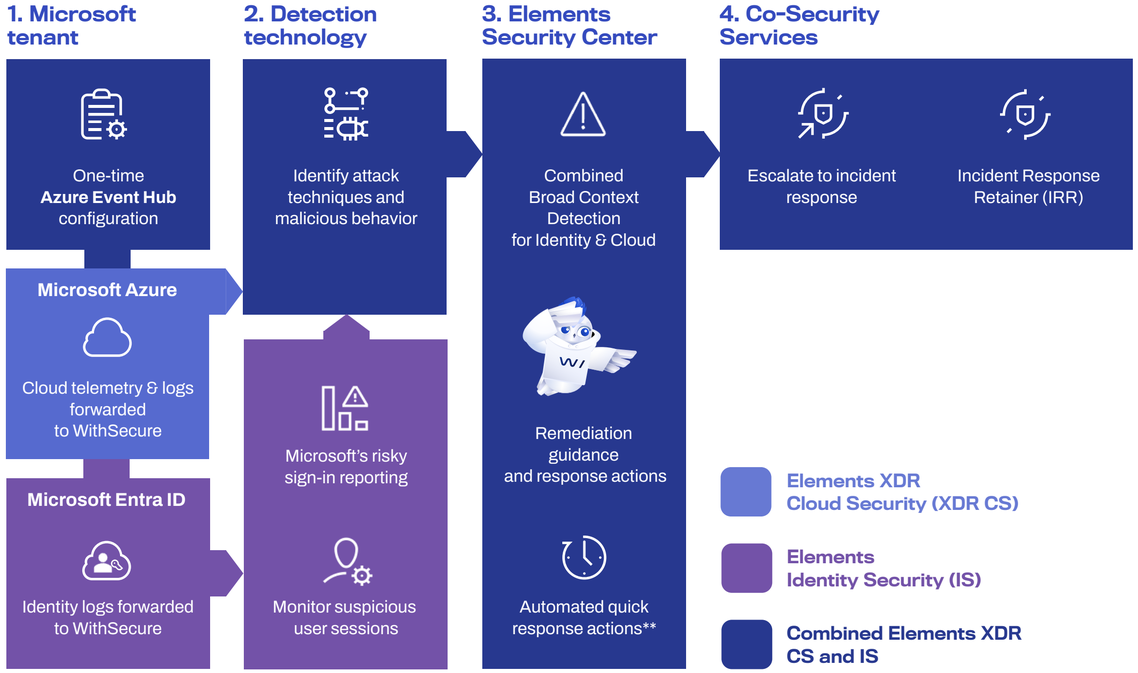
Keep your cloud infrastructure operational against threats with reduced business risk, continued service availability, and minimized operational downtime. Elements XDR Cloud Security delivers 24/7 monitoring for your Azure cloud environment, protecting your resources against constantly evolving threats. It uses WithSecure's global and dynamic threat intelligence to correlate and prioritize threat signals, providing you with cutting-edge threat research-based Broad Context Detections™. The solution detects cloud threats like ransomware, resource-jacking, and data exfiltration. All of these threaten your critical company data in the cloud as well as your seamless cloud-based service delivery.

The European Way of data protection for your Azure Cloud

Get European regulatory compliance from day one.
Sidestep the dominant tech giants and trust your security to a provider that operates in Europe with adherence to the European Way of data protection: privacy, data sovereignty, and regulatory compliance.
Based in Europe since 1988, WithSecure™ is a leading European vendor for mid-size companies and Managed Service Providers seeking compliant and effective cybersecurity solutions – tailored to European standards and meeting the needs of global markets at large.
Embracing European values eliminates the need for extensive compliance checks, as the best practices are inherently integrated into our products, services, and operations.
Whether you need support with complying with NIS2, DORA, ISO27001, or GDPR, we've got your back.

4. How it works

WithSecure Elements XDR Cloud Security is designed as an add-on to WithSecure Elements Identity Security. While Identity Security focuses on the initial stages of a cloud attack, cloud detections from XDR Cloud Security provide deeper visibility into how the potentially compromised identities interact with the resources within the cloud environment.



* Read more about the collected data in our Elements XDR Cloud Security User Guide.
More information about what data is collected and its purpose can be found in the Elements Privacy Policy.

** Currently, automatic quick response actions are only available for Entra ID (requires WithSecure Elements Identity Security) or for Virtual Machines in the cloud that can be protected using WithSecure Elements Endpoint Detection and Response (both licenses sold separately).

1. Microsoft tenant

Elements XDR Cloud Security identifies potentially malicious activities within your Azure cloud environment by examining logs and telemetry data. Cloud telemetry and logs are impossible to collect from an endpoint agent, so an integration with the Azure tenant is needed to configure the solution. Microsoft Entra ID logs are sent to WithSecure via a customer-hosted Event Hub. The customer must create the Microsoft Event Hub that forwards the logs to WithSecure*.

The onboarding is configured in two parts: firstly, in the Elements Security Center and then, by deploying the infrastructure to the Microsoft tenant.

2. Detection technology

The detection technology of XDR Cloud Security for Azure works so that the solution collects data from activity and resource logs to identify potentially malicious resource behavior in your cloud workloads. Cloud logs are then processed by our detection engine by combining our threat research-based rules and AI logics to generate detections.

Thanks to the capabilities of Elements Identity Security, our detection technology also analyzes Entra ID logs, monitoring for suspicious user sessions and highlighting risky sign-ins.

3. Elements Security Center

Individual detections are then aggregated into Broad Context Detections™ (BCDs), which represent a collection of related suspicious events and activities in one centralized place. The BCDs for cloud combine your Azure cloud activity data with the identity events data from Microsoft Entra ID (collected by WithSecure Elements Identity Security) to provide a comprehensive view of the cloud-related attack chain. This reveals, for example, how stolen Entra ID credentials are used to hijack your Azure cloud resources, showing all this information from just a single BCD.

Our BCDs enable you to effectively investigate your cloud incidents in a prioritized way. Moreover, our Luminen™ GenAI assistant provides additional details about the detections and gives recommendations that help you take impactful response actions to mitigate the cloud threats quickly. The core detection capabilities of XDR Cloud Security are complemented with advanced automated response actions** for Entra ID identities and your Virtual Machines in the cloud.

4. Co-Security Services

If you need additional support, you can easily access the Co-Security Services offered by our experts from the Elements Security Center, for example our SLA-backed Incident Response Retainer service.

We also offer a 24/7 Emergency Incident Response hotline (no SLA).

5. Detect and prevent cloud data breaches with our technology

Detections Against Cloud Attacks

Your environment may change from on-premises to cloud, but similar threats remain. In other words, when moving to a cloud environment the attack types mirror the ones plaguing the on-premises world. Elements XDR Cloud Security helps you to detect vicious cloud attacks that pose a financial risk, as well as a threat to your continuous cloud-based business operations:

- **Credential compromise*:** For example, the leveraging of stolen credentials from the dark web to establish a backdoor, move laterally, and exfiltrate data.
- **Compromised workloads:** For example, enabling a resource-jacking attack, where the attacker launches a crypto mining attack on an existing cloud resource. We have detections for resources we expect might be involved in crypto mining.
- **Data exfiltration:** For example, an attacker phishes a user to access a cloud file storage application and exfiltrate data.

Cutting-edge Threat Research Based Detection Engine

High-quality cloud detections require continuous monitoring of the threat landscape. Our cutting-edge threat research, the experience of our Incident Response team in continuously battling against real-world attacks, and our advanced Machine Learning (ML) models are all used to constantly develop cloud detections for your Azure cloud environment. Our W/ Intelligence team of expert researchers combines expertise in cyber security, detection engineering, and data science to continuously develop our cloud detection capabilities. They research our product install base telemetry across millions of endpoints, as well as incidents response findings from real-world attacks and other current attack trends in the threat landscape, to identify new and evolving Tactics, Techniques, and Procedures (TTPs).

We constantly develop our protections based on the TTPs' potential impact. Our cloud detection engine uses logs to detect anomalies and suspicious actions, covering techniques ranging from Initial Access to Exfiltration. The detection engine then creates alerts based on a combination of low-risk events that collectively may be sinister, while using ML to reduce false positive alerts.

What is an Event Hub?

An Event Hub is a log collection and forwarding mechanism that collects logs and forwards them to WithSecure.

How much will an Event Hub cost?

There is a small cost associated with use of Event Hubs.
Please review the Associated Microsoft Costs for more details.

What is the data retention approach at WithSecure?

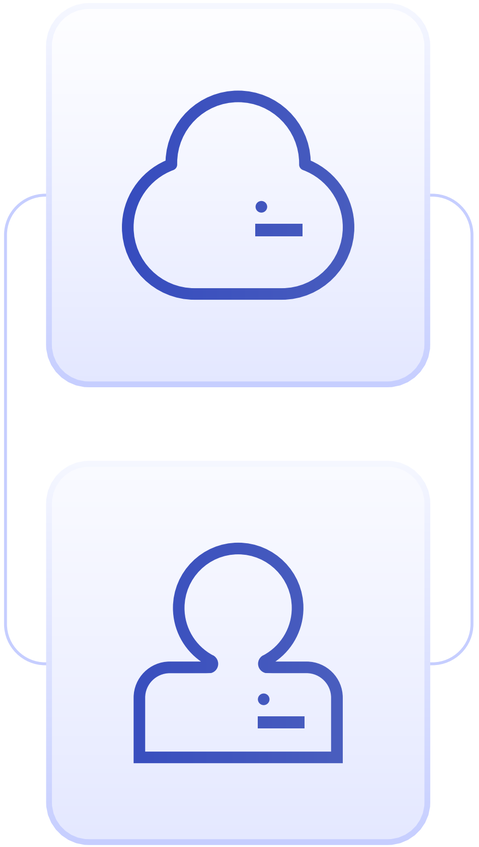
Data related to Broad Context Detections (BCDs) that are closed as confirmed or false positive is stored for the lifetime of the service.
Please review our privacy policy for more information.

* WithSecure Elements XDR Cloud Security BCDs for Azure make use of the Entra ID related BCD data from WithSecure Elements Identity Security.

Luminen™ GenAI – Your Investigation & Response Assistant

WithSecure's GenAI assistant Luminen™ blends the power of AI with the workflows of today's overwhelmed IT security teams. WithSecure Luminen is an Artificial Intelligence (AI) experience that leverages Large Language Models (LLMs) to provide Elements users with contextual and actionable guidance for their cyber security management tasks. It analyzes and provides natural language explanations of Broad Context Detections™ from WithSecure Elements XDR solutions, enriched with relevant external threat intelligence. Natively embedded into WithSecure™ Elements Cloud, Luminen supercharges IT teams with better situational awareness.

Detect and understand cloud attacks with the power of AI. Cloud Security is a new domain for many IT and security operators, but our Luminen GenAI assistant doesn't leave you to face the new challenges alone. Luminen empowers IT teams by assisting users of any experience level to better understand the context and impact of cloud detections. The assistant describes the cloud detections from XDR Cloud Security, including risk impact and recommended actions for remediation. The recommended actions from Luminen align with the industry's best practices, for example referencing the MITRE ATT&CK framework. Luminen also describes key cloud concepts in simple terms. The assistant provides outputs in multiple local languages and is automatically included with your Elements XDR Cloud Security license. With Luminen, you can easily turn cloud detections into concrete actions to improve your security posture.



Powerful Broad Context Detection™ Combines Cloud and Identity Events

Broad Context Detection™ (BCD) technology distinguishes real threat signals from the noise. Our proprietary Broad Context Detection (BCD) technology powers our detection capabilities across endpoints, identities, and cloud environments*. BCDs offer real-time behavioral, reputational, and big data analysis with machine learning to show you only relevant detections and their criticality. BCDs are natively designed for real-life, orchestrated, polymorphic attacks. By combining threat risk levels with information about affected resources and prevailing threat landscape, only the relevant detections and their criticality are shown. BCDs are visualized on a timeline that includes all impacted cloud resources, and relevant events, with their details, enabling you to better understand the scope of an attack. This allows you to detect the root causes of incidents and to take informed response actions quickly.

While the Elements EDR agent provides the best detection capabilities in traditional on-premise environments, public cloud environments require a different approach. Elements XDR Cloud Security consolidates suspicious events for your cloud resources together with Entra ID identity* related threat signals to form the full picture of a cloud attack. In other words, our Broad Context Detection logic is applied to both the cloud environment (Azure) and user identities (Entra ID) for producing synergistic Broad Context Detections in the cloud domain. Thus, the BCDs provide extensive coverage for cloud attacks, spanning across different stages — from compromise of the identities accessing the Azure cloud service to malicious activities targeting the Azure resources containing your sensitive company data. You can also configure tailored email notifications to be sent out for new cloud-related BCDs, to get alerted when suspicious activities are detected.

* Endpoint part of BCDs is covered by WithSecure Elements Endpoint Detection and Response (EDR), identity part (Entra ID) by WithSecure Elements Identity Security and cloud environments (Azure) by WithSecure Elements XDR Cloud Security.

Support your Cloud Transformation with Elements XDR

By choosing WithSecure Elements XDR, you gain visibility and detection capabilities across your workloads, both in the cloud and on-premise*. This makes your cloud transformation easier when you are moving from using on-premise endpoints to using the cloud or shifting to hybrid setups mixing both. Our unified agent and agentless approach ensure attacks are detected across on-premise endpoints and in the cloud environment. The latter includes both cloud-native resources and workloads in Azure as well as Virtual Machines in the cloud**. Get intelligent threat detection for the cloud era.

Protection, Detection, and Response for your Virtual Machines

WithSecure Elements Endpoint Security (EPP + EDR) agent can also be installed on your virtual machines running in the cloud**. Elements Endpoint Security provides advanced protection, detection, and response for your Virtual Machines (VMs), including workstations and servers. Elements EPP automatically blocks ransomware and malware on your VMs. Its advanced capabilities regularly score highly for the best protection in the industry. Elements EDR provides visibility into and detects sophisticated threats for your VMs, offering ready-made quick response actions and built-in guidance. Elements EDR uses our Broad Context Detection™ technology for event and context-based detections, with multi-faceted automated response options. It provides extensive visibility into your VMs for investigation, triaging, and responding to emerging threats. Elements Endpoint Security includes automated patch management. Our Elements Endpoint Security agent can be installed on your on-premise servers and computers as well as VMs, thus being able to cover the security of both your native and on-premise workloads.

Automated Response Actions

You need to have real-time visibility into what happens once an attacker gains access to your cloud environment, to react and take time-sensitive cloud response actions. This is possible with our Elements XDR. The core detection capabilities of Elements XDR Cloud Security are complemented with advanced automated response actions*** for Entra ID identities and your Virtual Machines in the cloud. These versatile quick response actions for the cloud domain help you to investigate, contain, and remediate attacks across your cloud environments. For example, you can detect potentially compromised user credentials and quickly respond by using automated quick response actions for Entra ID, like removing access, resetting passwords, or ending sessions to stop attackers in their tracks. Essentially, you can do more with less, easily align your response with minimal disruption, and significantly boost your productivity compared to working with command line or other remote management tools.

* WithSecure Elements Endpoint Security (EPP + EDR) covers on-premise endpoints, identity part (Entra ID) is covered by WithSecure Elements Identity Security and cloud environments (Azure) by WithSecure Elements XDR Cloud Security.

** Virtual machines in the cloud require purchasing a license for WithSecure Elements Endpoint Security, consisting of WithSecure Elements Endpoint Protection (EPP) and WithSecure Elements Endpoint Detection and Response (EDR).

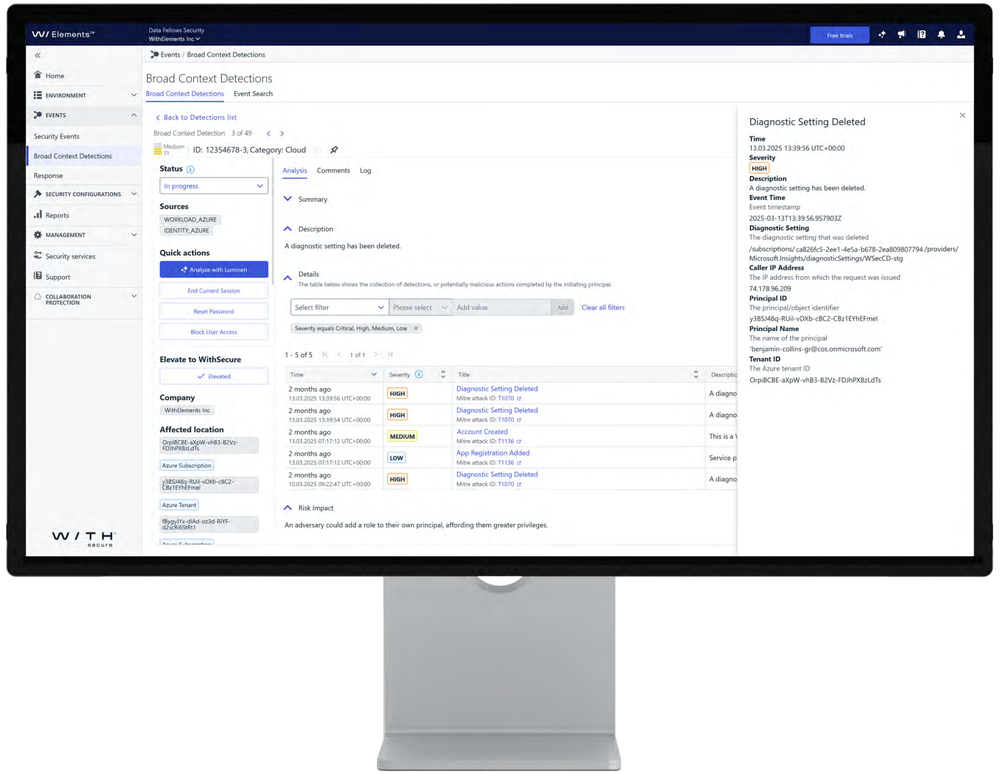
*** Currently, automated quick response actions are only available for Entra ID (requires WithSecure Elements Identity Security) or for Virtual Machines that can be protected by using WithSecure Elements Endpoint Security.

6. Detections for your key Azure Cloud resource types

Microsoft Azure cloud services currently included in the scope of detections:

- **Azure Key Vault:** Used to access sensitive keys and secrets to progress the attack.
- **Network Security Group:** Opened to exfiltrate sensitive data.
- **Azure Virtual Machine:** Used to run harmful code during initialization and in cryptojacking attacks, where attackers use an organization's resources and money to finance their crypto-mining activities.
- **Azure Storage:** Detects the modifications to setup scripts that run when an admin opens a cloud shell. This gives the attackers the privileges of an admin and the ability to execute their own code silently.

Please find a more detailed list of our detections in the WithSecure Elements XDR Cloud Security User Guide.



7. Technical Requirements

Supported systems

As Elements XDR Cloud Security is designed to protect Microsoft Azure as part of our Elements XDR solution, you need to have administrative rights to the relevant Azure tenants to set up your protection. After the initial setup, all you need is a modern web browser and Internet access to manage Elements XDR Cloud Security as part of Elements XDR.

Supported languages (Elements XDR Cloud Security)

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

Installation

You must be able to sign in as a Global Administrator on the Azure account to run the script in Azure Cloud Shell and have your tenant ID, subscription ID, and deployment location known and ready before you start the deployment. The subscription must be assigned to an Azure Management Group.

Elements License Requirements

WithSecure Elements XDR Cloud Security module must be purchased together with the following solutions:

- **WithSecure Elements Identity Security for Entra ID**, as Elements XDR Cloud Security is an add-on solution. Elements Identity Security provides Entra ID related data for providing understanding on what happens at the management level of Azure Cloud. Elements XDR Cloud Security complements this data at the subscription level of Azure Cloud, to give a complete picture of a cloud attack.
- **WithSecure Elements Endpoint Security** consisting of WithSecure Elements Endpoint Detection and Response (EDR) and WithSecure Elements Endpoint Protection (EPP).

Microsoft License Requirements

There are no Microsoft license requirements for Elements XDR Cloud Security.

Limitations

The customer is permitted to a total of 400 million events across one cloud module. If the number of processed events exceeds this limit, then a price adjustment may be required. When using WithSecure Elements Identity Security, automated quick response actions for identity can only be applied to Entra ID users; service principals are not in the scope of automated response actions currently.

Associated Microsoft Costs

WithSecure collects data using Standard Tier Event Hubs, which are created to each region where resources are deployed. The monthly cost is based on the number of Throughput Units (TU). The number of TUs depends on the number of events that generate load. Each Standard Tier Event Hub costs approximately €25 per month per Throughput Unit (TU). The costs that are associated with Event Hubs are described in the Microsoft Azure Event Hubs pricing web page. The cost per event received through the Event Hub is currently €0.026 per million events. Based on our historical data, monthly event volume varies depending on the size of the organization:

- Between 10 and 50 million for a company with 100 employees deployed to one region would be roughly 25 euros.
- Between 200-400 million for a company with 2500 employees deployed to three regions would be roughly 89 euros.

Please find more information on the topic from our XDR Cloud Security User Guide.

8. Overview of WithSecure™ Elements Cloud Platform

WithSecure™ Elements XDR Cloud Security 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 organization's Azure cloud resources.

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