WithSecure™ Elements Identity Security

Gain visibility into identity-based attacks

November 2024

DISCLAIMERS:

1) This document describes the General Availability version of the product and is this applicable January 2025 onwards

2) The key differences between the Early Access and General Availability versions are the addition of response capability and business email compromise detection.

Introduction

WithSecure™ Elements Identity Security is an Identity Threat Detection and Response (ITDR) solution. It protects organizations against identity-based attacks by detecting potentially compromised Microsoft Entra ID identities and enables analysts to respond to threats quickly, to minimize their business impact. As part of the Elements XDR family of products, Identity Security prevents major impact from credential theft and attacks against identity and access management infrastructure.

Attacker goals have not changed, they are still trying to cause disruption and steal information. However, attacks are focusing decreasingly on deploying payloads to endpoints, and more on abusing identities (user and entity) and their privileges. WithSecure's incident response team is seeing an increasing trend in identity-focused attacks. A recent report* revealed that stolen credentials have become the most popular entry point for breaches and breaches initiated with stolen or compromised credentials took the longest time to identify and contain.

From 2023 to 2024, there has been a 71% increase in attacks based on stolen or compromised user credentials. Data breaches that were initiated with stolen or compromised credentials took the longest to resolve out of various attack vectors – nearly 10 months.***

As modern IT environments sprawl beyond on-premises, you need more than basic security hygiene to stay protected. While still useful in securing endpoints, traditional Endpoint Detection and Response (EDR) tools cannot provide visibility into identities and cloud services that can be accessed from anywhere. Use of cloud-based Entra ID identities by remote workers and authentication to third-party tools increase the attack surface – and often there's no endpoint device to attack or to defend as part of these processes.

Identities have become a new, lucrative attack vector, especially in the case of Microsoft Entra ID as the most used cloud-based Identity and Access Management (IAM) service. Entra ID plays a central role for Microsoft 365, as it also includes multi-factor authentication and conditional access. It is used by most organizations that utilize cloud-based Microsoft 365 services.

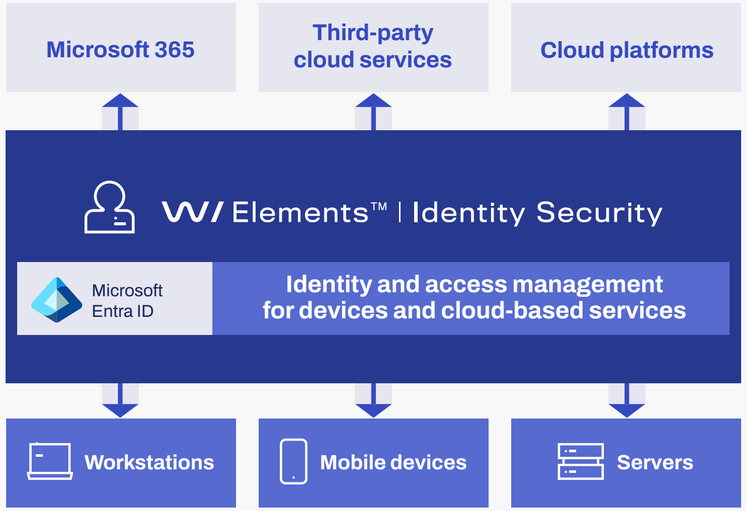
* IBM Cost of a Data Breach Report 2024
** IBM X-Force Threat Intelligence Index 2024

WithSecure™ Elements Identity Security allows you to detect and respond to identity-based attacks by highlighting potentially compromised user credentials, so analysts can take action to protect their organization. Credentials are often collected by attackers through either phishing email campaigns or by baiting administrators to accept non-standard authentication flows into their organization. Elements Identity Security extends your detection capabilities to identity-based attacks beyond endpoints, to secure your user credentials.

Once Elements Identity Security detects an attack, it makes your next steps in responding easy. All activity detected from a potentially compromised user is aggregated together into a Broad Context Detection™ (BCD), so that the investigation can easily happen in one central place within the WithSecure Elements Cloud platform. With Elements Identity Security, you can respond to identity threats quickly and easily to minimize disruption, for example by removing access, resetting passwords or ending sessions to stop attackers in their tracks.

The detection coverage for Entra ID spans a range of the latest attack scenarios including business email compromise, where an attacker gains unauthorized access to a company email, which can then be used to steal data or fraudulently obtain funds. In addition to a broad range of techniques, the MITRE attack phases of Initial Access, Persistence, Privilege Escalation, Defense Evasion and Credential Access are covered.

The service also combines native alerts from Microsoft Entra ID Protection* together with the other activity captured by WithSecure's Elements Identity Security and aggregates this data. This enables customers to have a comprehensive view of recent actions performed by suspected or compromised accounts from a single pane-of-glass.



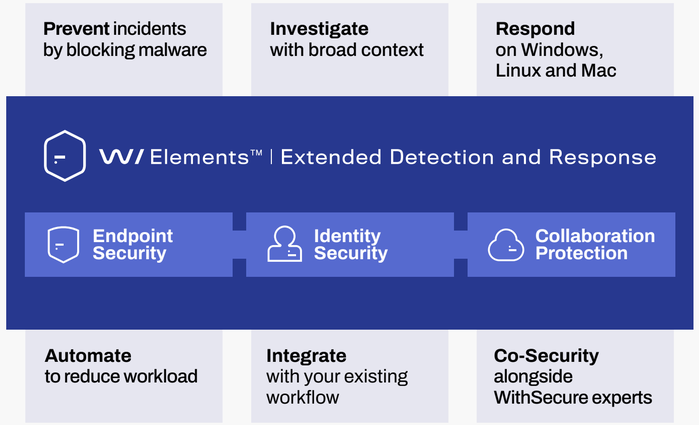
*Requires also a separate license for Microsoft Entra ID Protection that is a product that alerts for risky sign-ins (part of Microsoft bundle licenses like Entra ID P1 and above).

Part of WithSecure™ Elements XDR

WithSecure™ Elements Identity Security is a module of WithSecure™ Elements Extended Detection and Response (XDR) and 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 to different parts of the attack across cloud platforms, identities and email. Recognizing attacks early not only gives you a head start in reacting but also saves costs by reducing the repercussions that follow from compromises.

Elements XDR is part of our complete Elements Cloud platform that includes wide range of tools and capabilities that are delivered from the cloud to provide exposure management, automated patch management, dynamic threat intelligence and continuous behavioral analytics. Users of Elements Cloud can easily gain access to WithSecure's expertise with our flexible Co-Security Services that offer help for working with complex detections or widespread major incidents, for example.



What is the difference between EDR and XDR?

EDR solutions focus on detecting and responding to threats for endpoints, whereas WithSecure Elements XDR is a more extensive, unified solution to protect modern IT estates. It minimizes the impact of attacks by automated advanced preventative controls that keep incident volumes and lower-level attacks at bay. AI-powered tooling enables fast detection, investigation and response to threats in broader context – across endpoints, identities, emails and other cloud-based collaboration services. WithSecure Elements Identity Security is an ITDR solution to protect organizations against identity-based attacks as part of Elements XDR. WithSecure Elements Endpoint Detection and Response (EDR) also belongs to our Elements XDR offering, as part of our Endpoint Security solution that combines Elements EDR and Elements EPP (Endpoint Protection).

How does the pricing for Elements Identity Security work?

The price is based on the number of Entra ID user accounts, so all users in each* tenant should be added. You can get XDR with protection for Identities without needing to invest in Microsoft Entra ID's most expensive subscriptions like P1 and P2, thanks to Elements Identity Security. We offer a bundled price for Elements Identity Security together with Elements Endpoint Security (EPP + EDR).

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. This trend is likely to continue until there is wide adoption of ITDR tooling, making attacks so difficult that the attackers must look for new methods. The rise in identity-related attacks doesn't diminish the importance of guarding against endpoint threats. Ransomware remains a significant threat to many organizations. For more detailed information, please refer to our latest Threat Intelligence Reports.

* The solution is compatible with multiple tenants.

Why WithSecure™ Elements Identity Security?

Protect your most targeted assets: your users. Identity is the layer between your endpoints, cloud services, and the platforms your organization utilizes. Endpoint protection, detection and response capabilities protect your devices, but you need Elements Identity Security as the next extension to protect your modern IT environment.

Based on real-life attacks from our Incident Response team

Secure your organization's remote workforce by utilizing detection logic created from real attacks targeting identities.

Prevent the use of stolen credentials

Detect compromised credentials and identity-based attacks by gaining visibility beyond the endpoint.

Detect Business Email Compromise

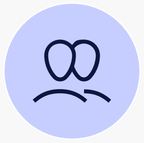
Proven detection for the techniques that are the costliest to organizations.

Act fast to minimize impact

Use our Entra ID Response capabilities to end sessions and disable user access.

Investigate in broad context

All activity detected from a potentially compromised user is aggregated together so that the investigation into suspicious activity can be performed from one central place.



Flexible services

Do more with limited resources by easily managing Elements XDR and accessing flexible services whenever needed to augment your own team.

Benefits

Protect your remote workforce

Traditional EDR solutions don’t protect all assets accessed by your remote workforce. Cloud services are becoming increasingly common in modern IT environments and those often rely on Entra ID, thanks to using features like Single Sign-On (SSO). With Elements Identity Security, you can extend detection capabilities beyond endpoints to cover identities and respond to identity-based threats swiftly.

Investigate with Broad Context Detection™

Broad Context Detections™ (BCDs) reduce alert fatigue by automatically aggregating relevant events, scoring the overall severity, and enabling investigations from one consolidated view. Suspicious activity performed by users can be investigated through a comprehensive view of recent actions that have been undertaken by suspected compromised accounts. With BCDs, you can look at attacks on a timeline to find patterns, view relevant events, and act swiftly – with recommendations from us. Real-time behavioral, reputational, and big data analysis are used alongside machine learning to place detections in context while taking risk levels and the importance of each affected host into account.

Our several detection mechanisms create high-fidelity alerts. We use a combination of signs in risk scoring and in other detections to identify actions that an attacker would use after getting initial access. These signs include actions like creating application registrations, adding credentials to service principles and adding service principles with similar names to Microsoft to disguise actions. Combining these types of signs reduces false positives, as we can be more confident that the BCD is malicious if it contains multiple suspicious detections.

Detect and respond to identity-based attacks

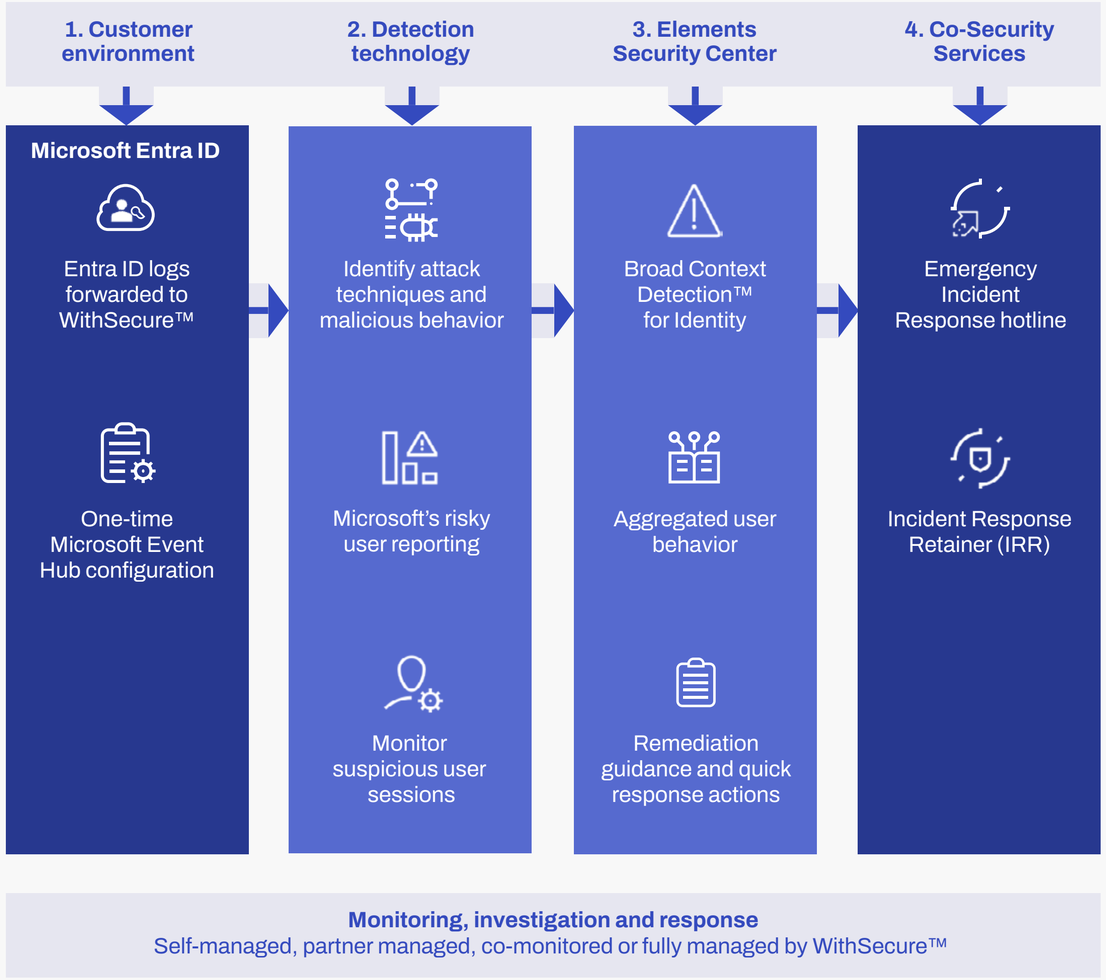
Protect against the risk in identity-based attacks by having visibility of compromised user credentials. Credentials are often stolen using phishing email campaigns that harvest credentials from false websites that bait administrators to accept non-standard authentication flows in their organization. Utilize user-centric alerts to investigate all suspicious activity detected from a potentially compromised user. By getting alerted, you can quickly respond when suspicious activity occurs, allowing you to minimize the impact of attacks before any business-critical data is stolen. Each Broad Context Detection™ includes remediation guidance and quick response actions, making it easy to act fast.

GenAI Luminen™

Use our helpful Elements Cloud platform AI assistant to understand identity-based attacks and key concepts (availability of assistant for Identity Security solution planned for H1/2025*). Luminen™ GenAI analyses and provides natural language explanations of Broad Context Detections™ from WithSecure Elements XDR, enriched with relevant external threat intelligence data. It empowers IT teams by immediately assisting users of any experience level to better understand the context and impact of the detections, allowing them to focus on what matters the most.

* Plans are subject to change.

How it works



1. There is a one-time Microsoft Event Hub configuration to capture Entra ID logs from the customer's environment*. The onboarding is configured in three parts: initially creating the tenant in the Elements Security Center; then deploying the infrastructure to the Microsoft tenant; and finally adding the connection string back into the Elements Security Center, so that data collection can begin.

2. Microsoft Entra ID logs are sent to WithSecure via a customer-hosted Microsoft Event Hub. WithSecure's detection technology identifies attack techniques and malicious behavior by using Microsoft's risky user reporting and by monitoring suspicious user sessions.
   - Logs collected are sign-in and audit logs, non-interactive user sign-in logs, service principal sign-in logs, managed identity sign-in logs, Microsoft risky alerts and events from users and service principles**.

3. In the Elements Security Center, identity related detections are aggregated into potential incidents. Broad Context Detection™ for Identity will appear as a method to understand aggregated user behavior. Each Broad Context Detection™ includes remediation guidance and quick response actions.

4. Often, the next step in an investigation is to confirm the activity is expected and legitimate. Therefore, usually the partner should contact the end user to validate the activity in the organization's context. However, monitoring, investigation and response can be either self-managed or partner managed. In case needed, there are also additional Co-Security Services for incident response available from WithSecure, for example our guaranteed Incident Response Retainer (IRR) service. We also offer a 24/7/365 emergency Incident Response support hotline.

* There is also a one-time onboarding for the response capability, which grants consent from the customer tenant to a WithSecure Elements Azure Response Application. This connection will be used by the Elements Platform to issue response jobs in the customer tenant.
** More information about what data is collected and its purpose can be found in the Elements Privacy Policy.

Prevent major impact from credential theft with our technology

Extensive Detection Coverage

Identity related attack detection coverage for Microsoft Entra ID spans a range of MITRE ATT&CK phases. These include Initial Access, Persistence, Privilege Escalation, Defense Evasion and Credential Access. The detection coverage spans a range of the latest attack scenarios, for example business email compromise, where an attacker gains unauthorized access to a company email which can be used to steal data or fraudulently obtain funds. Elements Identity Security can also detect scenarios like suspected compromised accounts, the use of stolen credentials, suspicious identity and access activity, or atypical travel.

Session cookies and tokens can be stolen by a malicious AitM (Adversary-in-the-Middle) website for reuse in a session takeover attack. The circumstances under which these cookies and tokens, like location and device, are reused can be traceable properties of the session activity. This can then be used for detection of suspicious activity. Our solution tracks the device metadata and location of session activity, among other types of data, allowing us to rate the likelihood of a malicious session.

Risk Factors for Determining Sign-in Protection

WithSecure uses numerous factors to determine the risks of a sign-in event:

- **Geolocation** – We cover a range of impossible travel anomalies from successful and unsuccessful logins.
- **Brute-force** – There can be hundreds of failed logins for impossible travel use cases. To reduce noise, these are aggregated together and used to determine the ultimate risk of the sign-in, rather than alerting the user to individual brute-force attempts.
- **OAuth Protocol anomalies** – We identify anomalies in the OAuth sign-in events, which could be new resources, applications or clients.
- **Device Metadata** – Differences in devices and their metadata can indicate a compromised session and therefore, will increase the risk of the sign-in.
- **MFA (Multifactor Authentication)** – We use MFA metadata to assess how suspicious a sign-in event is.
- **Unknown principal** – If the principal has not been used in a sign-in event for the organization, this will increase the overall risk score of the event.

Extensive Visibility via Entra ID Integration

WithSecure Elements Identity Security integrates with Microsoft Entra ID (previously known as Azure AD) as the most widely used cloud-based Identity and Access Management (IAM) service. Entra ID is mandatory for cloud-based Microsoft 365 services, and it can be used for authentication across third-party cloud services. Elements Identity Security captures relevant identity-based Entra ID events, including sign-in and audit logs, and combines them with native alerts from Microsoft Entra ID Protection (if this Microsoft product is in use). With the combination of these two types of identity-based events, you have extensive visibility into identity-based attacks.

Impossible Travel

Impossible or atypical travel is detected by the solution. This works by detecting cases where physical travel for long distance is not possible in a given time between logins.

Business Email Compromise

Business Email Compromise (BEC) is a type of identity attack where perpetrators impersonate an internal user by first stealing their credentials. This enables them to then send an email to trick other individuals from within the same organization to send money or divulge sensitive information. WithSecure has built detections based on real Business Email Compromise incident response cases where Microsoft Outlook client data was used.

Minimizing Noise

Due to the probabilistic nature of sign-in events, there is always a delicate balance between over-alerting and missed detections. In developing the product, we have carefully fine-tuned our detections and built noise suppression mechanisms as part of the engine. Those mechanisms include aspects like:

- Suppressing alerts on repeat principals in a short timeframe (histograms)
- Aggregating activity together to determine a risk score based on user activity, rather than single sign-in events
- Looking at behaviour across the organization to reduce anomalies with impossible travel (although the use of organizational VPN can be an issue here, we mitigate this issue using common company login metadata statistics).

Identity Response

Response is an important part of preventing major impact from attacks and therefore, a critical component of Elements Identity Security. The available quick response actions work by a direct integration between Elements Cloud and your Entra ID instance. The response actions include:

1. End current session
2. Reset password
3. Block user access.

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, usually 15 euros per month, please review the Associated Microsoft Costs for more details.

What is the data retention approach at WithSecure?

Data related to Broad Context Detections (BCDs) is stored for the lifetime of the service. Please review our privacy policy for more information.

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 Identity Security 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 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.

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

Supported languages
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
Elements Identity Security requires a subscription to WithSecure Elements Endpoint Security, which includes Endpoint Protection (EPP) and Endpoint Detection and Response (EDR) capabilities.

Microsoft License Requirements
There are no Microsoft license requirements for Identity Security. If the customer has a P2 license for Entra ID, we offer a detection logic to utilize risk reports from Microsoft Entra ID Protection and to disable conditional access (a feature which requires a P2 license).

Microsoft Permissions
The following privileged roles within the Entra ID tenant are required for response capability:
- Graph API permission: User.ReadWrite.All
- Azure privileged role: User Administrator.

While WithSecure has implemented measures to reduce this risk, the permissions mentioned above have elevated privileges that attackers could exploit. Potential impacts include:

a) Creation of new user accounts to maintain unauthorized access within the environment

b) Denial of Service (DoS) attacks targeting administrators and Entra ID users

c) Unauthorized access to sensitive data, such as names, email addresses, and job titles.

Limitations
Note that the customer is permitted 200 million events across Entra ID log sources each month. If the number of processed events exceeds this limit, then a price adjustment may be required. During the deployment, the customer will execute a script that configures Azure alerts for when the Microsoft Event Hub(s) reaches full capacity. The customer is responsible for ensuring the Event Hubs do not reach full capacity, because this will impact service delivery, as WithSecure will no longer receive all events from the customer's tenant. Please raise a ticket to WithSecure Customer Care, if such alerts are received from Azure.

Associated Microsoft Costs
The Microsoft Event Hub configuration that is deployed uses Standard Tier Event Hubs. The monthly cost is based on the number of Throughput Units (TU). The number of TUs depends on the load. Standard Tier Event Hubs cost 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, the monthly event volume ranges from 6 million to 300 million events. Please find more information on the topic from our Identity Security User Guide.

WithSecure™ Elements – Reduce cyber risk, complexity and inefficiency

WithSecure™ Elements Identity 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. 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 remote workforce against the rise in attacks targeting identities.

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 NASDAQ OMX Helsinki Ltd.