



**SPHERE**  
to you

# Evolution | VUM to Exposure Management

Bernd Länge, AXSOS AG

Jan Kolloch, Sales Engineer, WithSecure

**WITH**<sup>®</sup>  
secure

PARTNER RESTRICTED

# Threat Landscape

# Pain points of today's attack surface

**Hybrid  
environment  
with fuzzy  
borders**

Lack of visibility across cloud  
and on-premises environments

**Identities as  
the weak link**

Powerful attack acceleration points,  
easily phished and stolen

**Dynamic  
threat  
landscape**

Constant threat landscape changes  
and AI-enabled cyber attacks

# Organizations face many challenging questions

What is my external attack surface?

What risks is my organization causing to the supply chain?

What shadow IT do I have in my environment?

Are there risks in users' identities that make those easy to breach?

How can I keep my business risk low with limited resources?

What is the business context of the identified exposure?

# Solution Overview

# WithSecure™ Elements Exposure Management (XM)

**A continuous proactive solution to predict and prevent breaches against your company's assets and business operations.**

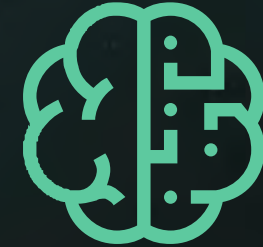
# Proactive security approach



**Know what makes  
up your attack  
surface**



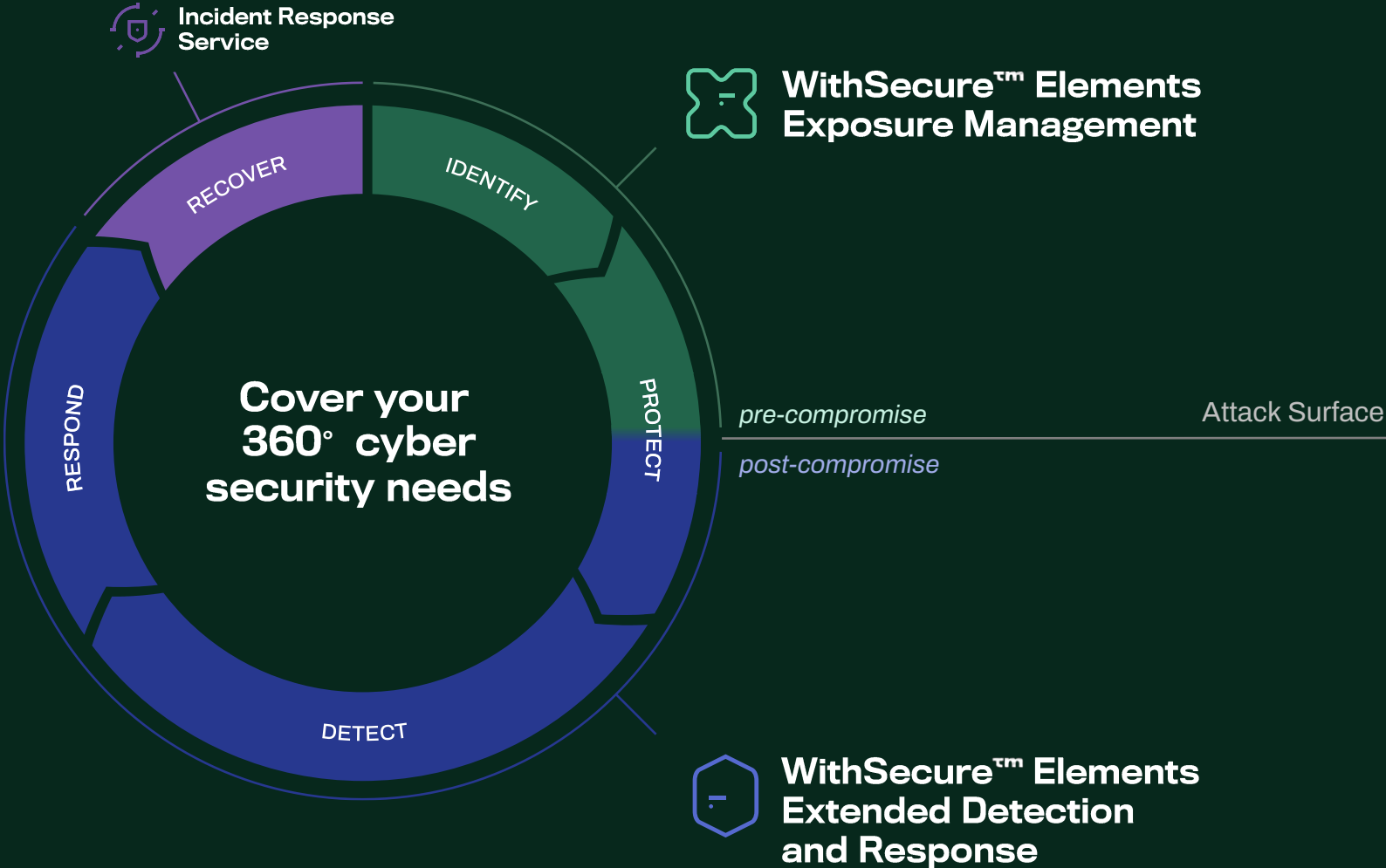
**Know what to prioritize  
when remediating  
exposures**



**Have the right tools,  
people and means to  
remediate successfully**

# Elements XM & XDR

is the foundational combination for addressing the pre- and post-compromise mid-market cyber security needs.

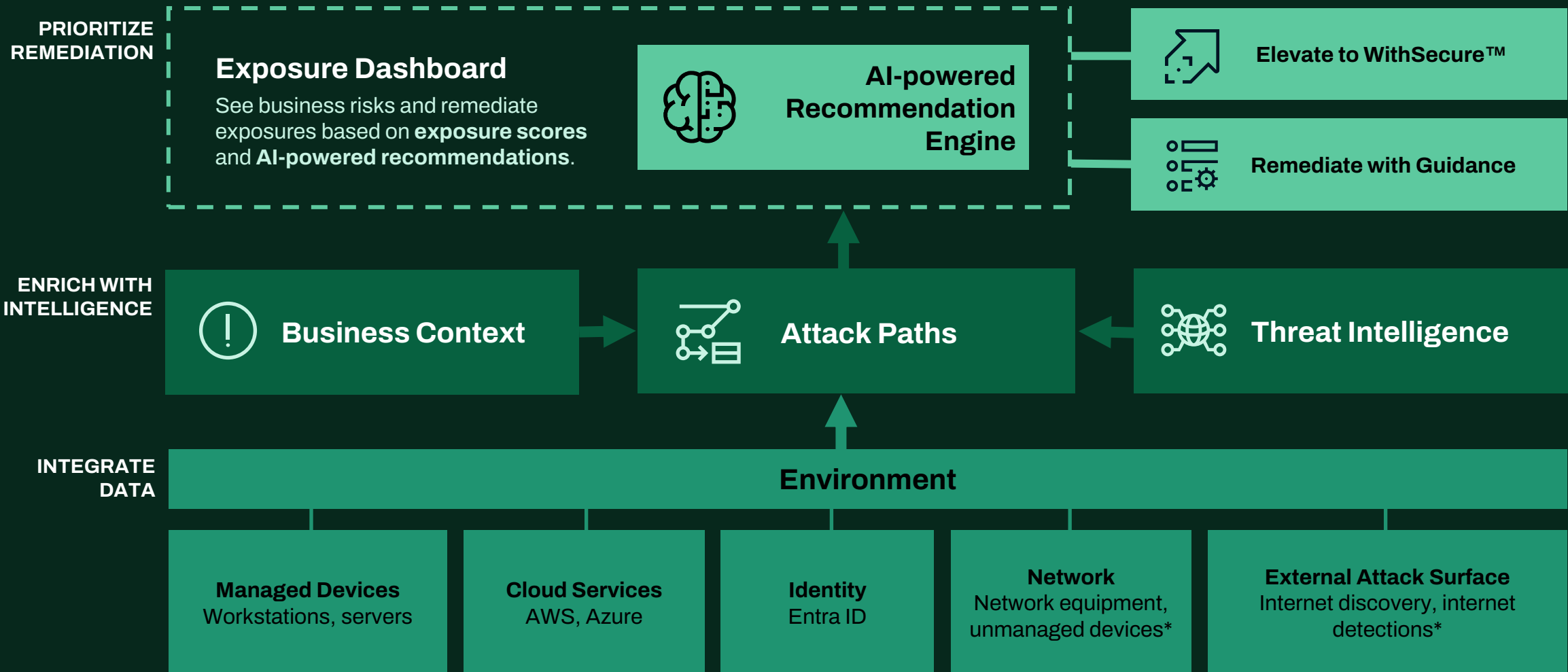


**Note:** Figure adapted from [NIST cyber security framework](#). We offer additional Incident Response services to cover the "Recover" area of NIST.



# WithSecure™ Elements Exposure Management

Continuous assessment of threat exposure, using the attacker's view of your environment.



# Key outcomes:

## DISCOVER

Discover your digital perimeter and identify the most **critical assets** and **identities**

## PRIORITIZE

Get actionable recommendations based on integrated data from **threat intelligence, attack paths** and **business context**

## ACT

Implement prioritized remediation actions to **reduce your attack surface** and **decrease your business risk level**

# How it works

External Attack Surface



External Attack Surface

⚠️ Open port

⚠️ Remote code execution vulnerability

⚠️ Stolen credentials

⚠️ Access rights misconfigurations

⚠️ Weak password

☁️ Collaboration Tool

☁️ CRM System

☁️ Task Tracker

☁️ Data Storage

☁️ HR Platform

External Attack Surface

 Task Tracker

 Collaboration Tool

 Data Storage

 CRM System

 HR Platform

External Attack Surface

Task Tracker

Collaboration Tool

Data Storage

CRM System

HR Platform

Productivity Tool

Files Converter

Messenger



External Attack Surface

Task Tracker

Collaboration Tool

Data Storage

CRM System

HR Platform

Files Converter

Productivity Tool

Messenger





External Attack Surface

High risk of compromise

High risk of sensitive data leakage

Task Tracker

Collaboration Tool

CRM System

Data Storage

HR Platform

Files Converter

Messenger

Productivity Tool



External Attack Surface

Collaboration Tool

CRM System

Task Tracker

Data Storage

HR Platform

Productivity Tool

Files Converter

Messenger

W / T H  
secure



# Key Features

# Exposure Dashboard

## Understand business risk and recommended actions

### 1. See how strong your attack surface is

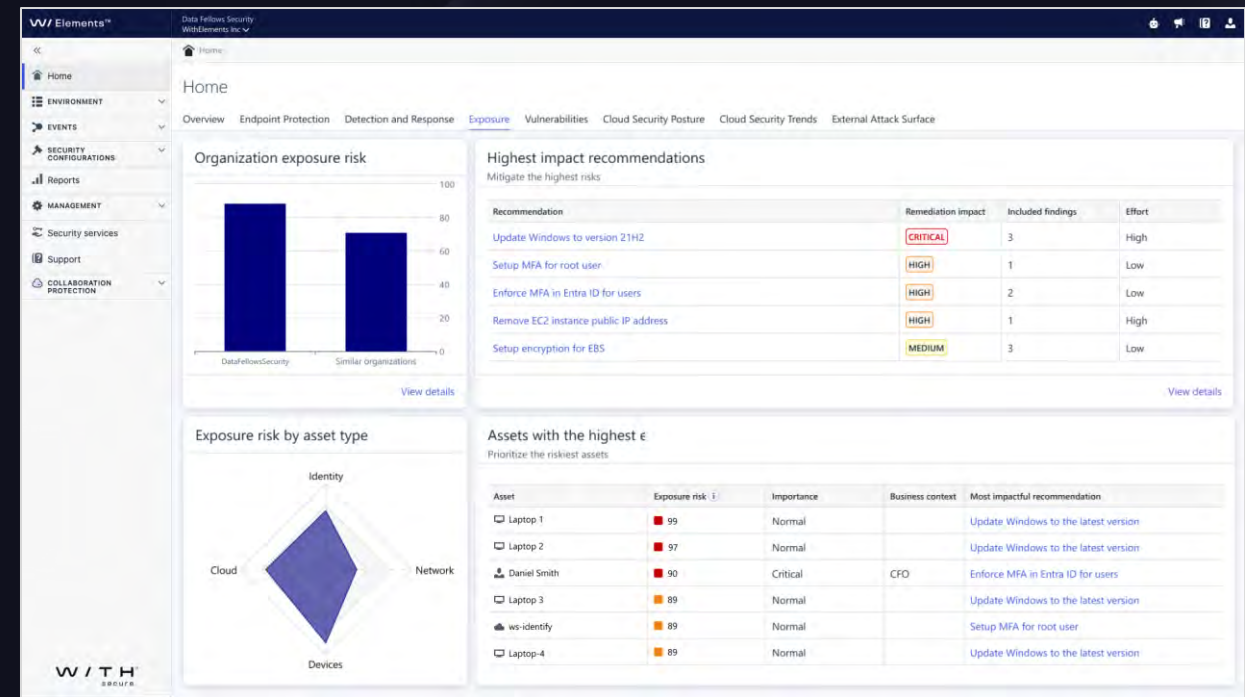
Exposure summary view gives you a risk-based overview of the identified weaknesses in your attack surface.

### 2. See the business-critical assets at risk

Use Exposure Score to start prioritizing the remediation from the assets causing the severest risk of exploitation.

### 3. Know the next actions to improve exposure

Get recommendations on what to solve first for quick and easy action, thanks to our AI-powered recommendation engine. No more alert fatigue.



Note: The UI views may undergo some improvements during the early access phase of the solution.

# Environment View

## Discover and manage your assets from a single view

Type	Name	Exposure risk	Online	Registration date	OS Name	Assigned profile	Status updated	Client version
Laptop 1	Laptop 1	99	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 2	Laptop 2	97	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 3	Laptop 3	89	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 4	Laptop 4	89	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 5	Laptop 5	88	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 6	Laptop 6	88	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 7	Laptop 7	88	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 8	Laptop 8	87	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 9	Laptop 9	85	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 10	Laptop 10	83	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 11	Laptop 11	82	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 12	Laptop 12	81	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 13	Laptop 13	81	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 14	Laptop 14	80	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 15	Laptop 15	78	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 16	Laptop 16	76	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 17	Laptop 17	75	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309
Laptop 18	Laptop 18	73	No	May 16, 2024	Windows 10	WithSecure™ Office (L...	May 16, 2024 5:42	22.4.47309

### 1. Centralized listing and management of assets per asset type:

- Onboard supported asset types like devices, network, identities and cloud
- List assets in a single view
- Manage and configure

### 2. Discover more assets

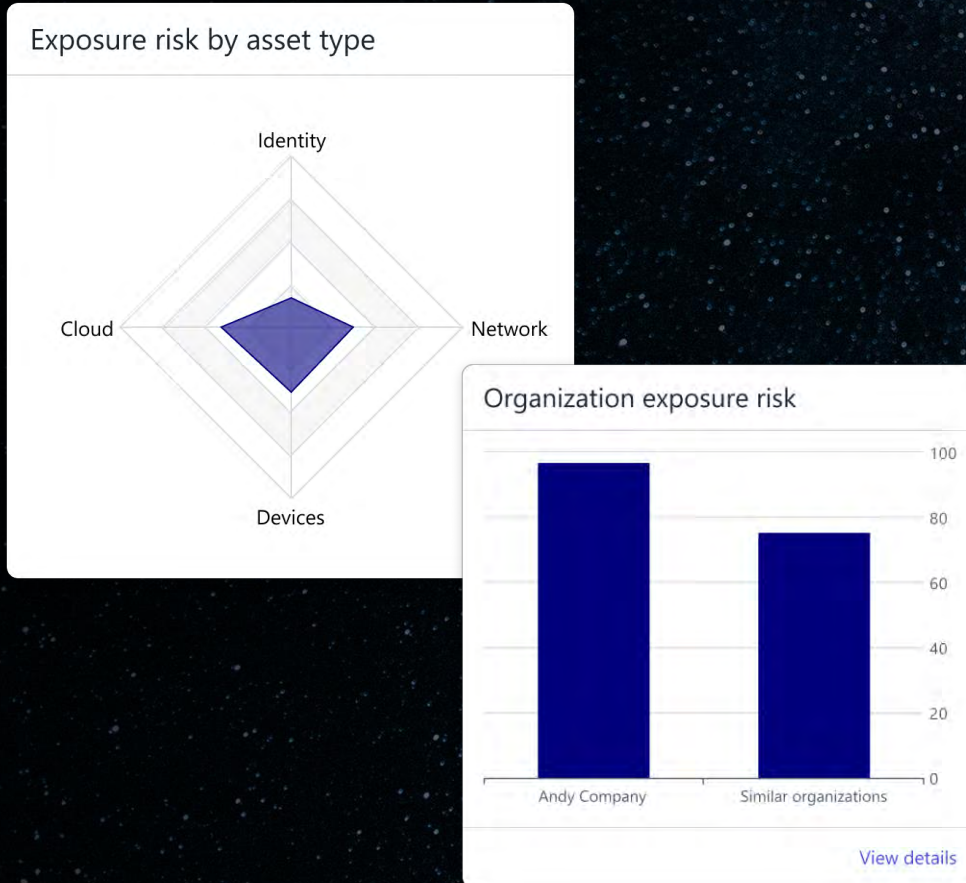
- For example: Unmanaged devices

### 3. Navigate and address risks related to a particular asset type

Note: The UI views may undergo some improvements during the early access phase of the solution.

# Exposure Score

See the exposure risk level of your company and assets



## Works on three levels:

1. The exposure score of a company represents relative business risk caused by the current state of the company's digital assets.
2. Calculated separately for each asset type to highlight where the issues are.
3. Each asset instance has an exposure score - calculated from various elements such as attack path mapping, criticality of the asset instance and threat intelligence.

Note: The UI views may undergo some improvements during the early access phase of the solution.

# Focus on what matters the most

## With Attack Paths, Business Context & Threat Intelligence

Recommendation	Remediation Impact	Effort	Place of fix	Affected asset	Included findings	Related findings type	Tags	ID	Generated on
ec-hardening	MEDIUM	High	Cspm	66	69	CSPM	exampletag test	7e3514a-fbce-4b	May 14, 2024 13:19 Over 3 days ago
T1530	MEDIUM	Medium	Cspm	5	10	CSPM	exampletag test	a6995833-e304-41	May 14, 2024 13:22 Over 3 days ago
T1548	MEDIUM	Medium	Cspm	1	2	CSPM	exampletag test	03c2850f-5965-4b	May 14, 2024 13:21 Over 3 days ago
Unauthorized access detected to subdomain	MEDIUM	High	Aum	1	1	MANUAL	exampletag test	380481c-c8e4-41	May 16, 2024 10:38 A day ago
CVE-2024-4671	MEDIUM	Low	Aum	1	1	MANUAL	exampletag test	d70b1db2-354c-4c	May 15, 2024 17:26 Over 2 days ago
Unauthorized access detected to subdomain	MEDIUM	Low	Aum	1	1	MANUAL	exampletag test	0ab8913-6a5d-43	May 15, 2024 17:42 Over 2 days ago
T1211	LOW	Medium	Cspm	2	2	CSPM	exampletag test	289706ce-8327-4a	May 14, 2024 13:22 Over 3 days ago
T1485	LOW	Low	Cspm	5	6	CSPM	exampletag test	f831204d-0939-4f	May 14, 2024 13:22 Over 3 days ago
T1496	LOW	Low	Cspm	2	2	CSPM	exampletag test	619578cc-7f68-4f	May 14, 2024 13:22 Over 3 days ago
Valid Accounts	LOW	Medium	Cspm	5	7	CSPM	exampletag test	0394969-845a-4a	May 16, 2024 16:10 A day ago
Exploit Public-Facing Application	LOW	Low	Cspm	1	1	CSPM	exampletag test	ab24e293-fa23-45	May 16, 2024 16:11 A day ago
Remediate identity breach of multiple users	LOW	MEDIUM	Identity	6	23	IDENTITYBREACH	exampletag test	ac990ee7-fc32-4cc	May 16, 2024 15:44 A day ago
T0879	LOW	High	Cspm	6	6	CSPM	exampletag test	6bd4f51d-c16b-4c	May 14, 2024 13:22 Over 3 days ago
T1078.004	LOW	Medium	Cspm	33	35	CSPM	exampletag test	40e6c903-a96d-47	May 14, 2024 13:21 Over 3 days ago
T1153	LOW	Medium	Cspm	2	2	CSPM	exampletag test	c37aa6f7-ea66-49f	May 14, 2024 13:22 Over 3 days ago
Remediate identity breach of multiple users	LOW	MEDIUM	Identity	6	23	IDENTITYBREACH	exampletag test	ac990ee7-fc32-4cc	May 16, 2024 15:44 A day ago
T0879	LOW	High	Cspm	6	6	CSPM	exampletag test	6bd4f51d-c16b-4c	May 14, 2024 13:22 Over 3 days ago
T1078.004	LOW	Medium	Cspm	33	35	CSPM	exampletag test	40e6c903-a96d-47	May 14, 2024 13:21 Over 3 days ago

Note: The UI views may undergo some improvements during the early access phase of the solution.

### Discover key elements for Exposure Score:

Ensure that you protect the path to the most critical assets by validating the **attack path**:

- Simulates the attack paths that an attacker could take to compromise a customer's estate (disrupt, recon, steal...).

### Flexibly manage your **business context** values:

- Each asset instance has a default business context value and optional context information.
- Business context information enables the tailoring of our recommendations to the customer's individual needs.

### Benefit from our unique **threat intelligence data**:

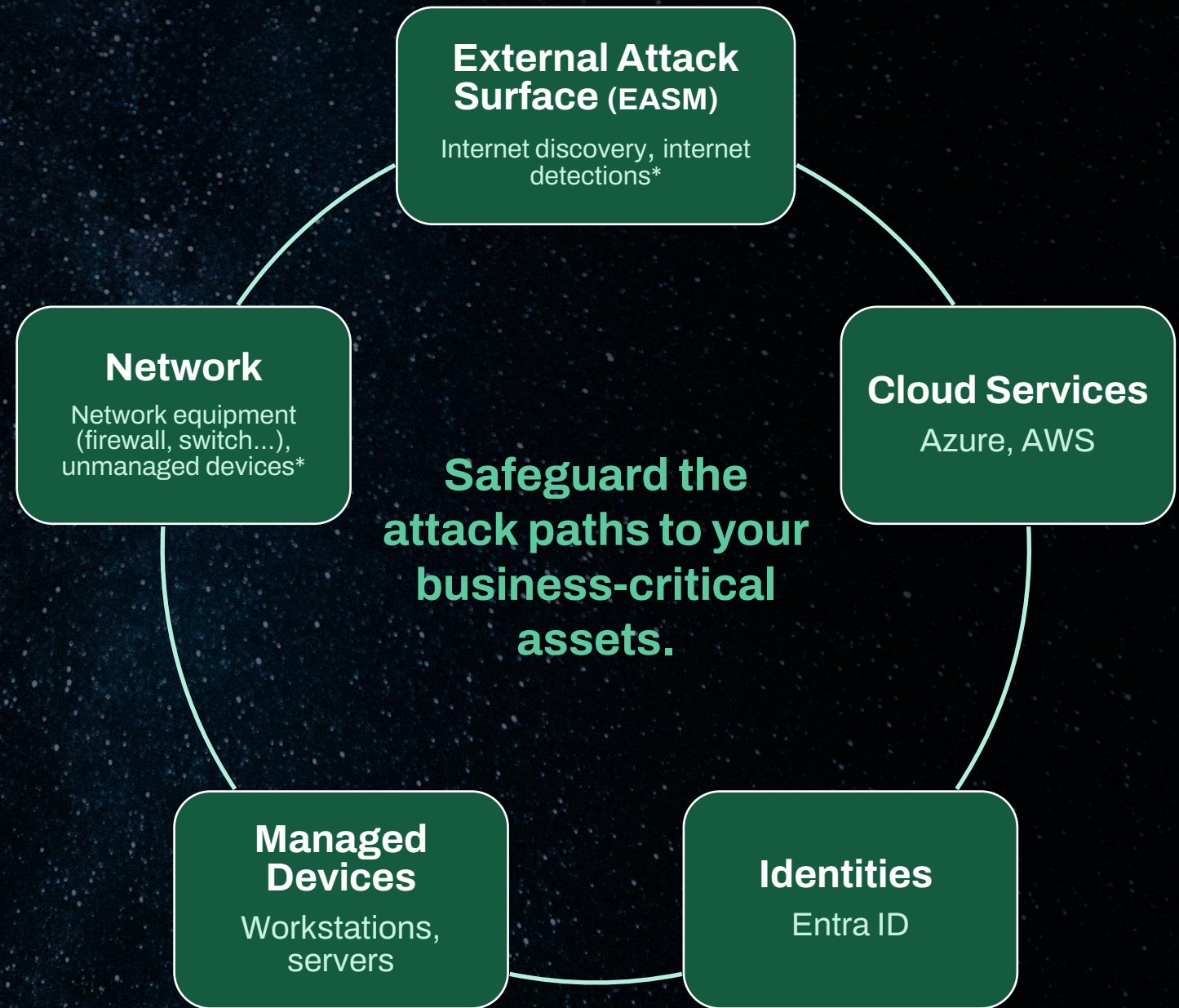
- Exposure scores are enriched with up-to-date threat intelligence data and anticipated breaches for better recommendations.



# Supported Assets

# 360° view of cyber risks

See your complete attack surface and remediate the highest-impact vulnerabilities that pose the most risk of intrusion to your organization efficiently from a unified view - thanks to our AI-powered recommendation technology.



\*Planned for GA version.

# Exposure for Identity Risk

## Use data on digital identities, tackle identity-based risks

Name	Email	Risk status	Importance	Business context	Location	UPN	Azure tenant	Last logged in device	Last logged in device status
Daniel Smith	daniel.smith@datafellow...	Risk	Normal		Finland	daniel.smith@datafellow...	DataFellow Tenant	Laptop 17 May 16, 2024 8:03	Managed
Emily Johnson	emily.johnson@datafellow...	No risk	Normal		Finland	emily.johnson@datafellow...	DataFellow Tenant	Laptop 3 May 16, 2024 8:03	Managed
Sophia Brown	sophia.brown@datafellow...	No risk	Normal		Finland	sophia.brown@datafellow...	DataFellow Tenant	Laptop 1 May 16, 2024 8:03	Managed
Liam Davis	liam.davis@datafellowsec...	No risk	Normal		Finland	liam.davis@datafellowsec...	DataFellow Tenant	Laptop 2 May 16, 2024 8:03	Managed
Olivia Wilson	olivia.wilson@datafellow...	No risk	Normal		Finland	olivia.wilson@datafellow...	DataFellow Tenant	Laptop 18 May 16, 2024 8:03	Managed
Noah Taylor	noah.taylor@datafellow...	No risk	Normal		Finland	noah.taylor@datafellow...	DataFellow Tenant	Laptop 5 May 16, 2024 8:03	Managed
Ava Anderson	ava.anderson@datafellow...	No risk	Normal		Finland	ava.anderson@datafellow...	DataFellow Tenant	Laptop 6 May 16, 2024 8:03	Managed
William Clark	william.clark@datafellow...	No risk	Normal		Finland	william.clark@datafellow...	DataFellow Tenant	Laptop 9 May 16, 2024 8:03	Managed
Isabella Scott	isabella.scott@datafellow...	No risk	Normal		Finland	isabella.scott@datafellow...	DataFellow Tenant	Laptop 8 May 16, 2024 8:03	Managed
James Lee	james.lee@datafellowsec...	No risk	Normal		Finland	james.lee@datafellowsec...	DataFellow Tenant	Laptop 11 May 16, 2024 8:03	Managed
Emma Hall	emma.hall@datafellowsec...	No risk	Normal		Finland	emma.hall@datafellowsec...	DataFellow Tenant	Laptop 13 May 16, 2024 8:03	Managed
Benjamin White	benjamin.white@datafello...	No risk	Normal		Finland	benjamin.white@datafello...	DataFellow Tenant	Laptop 7 May 16, 2024 8:03	Managed
Olivia Wilson	olivia.wilson@datafellow...	No risk	Normal		Finland	olivia.wilson@datafellow...	DataFellow Tenant	Laptop 18 May 16, 2024 8:03	Managed
Noah Taylor	noah.taylor@datafellow...	No risk	Normal		Finland	noah.taylor@datafellow...	DataFellow Tenant	Laptop 5 May 16, 2024 8:03	Managed

Note: The UI views may undergo some improvements during the early 'access' phase of the solution.

### Identity context for Elements

Entra ID data integrated with Elements to provide identity context to an incident

- **Covered assets:** Entra ID, hybrid.
- Human/Non-human

### Identity Attack Vectors

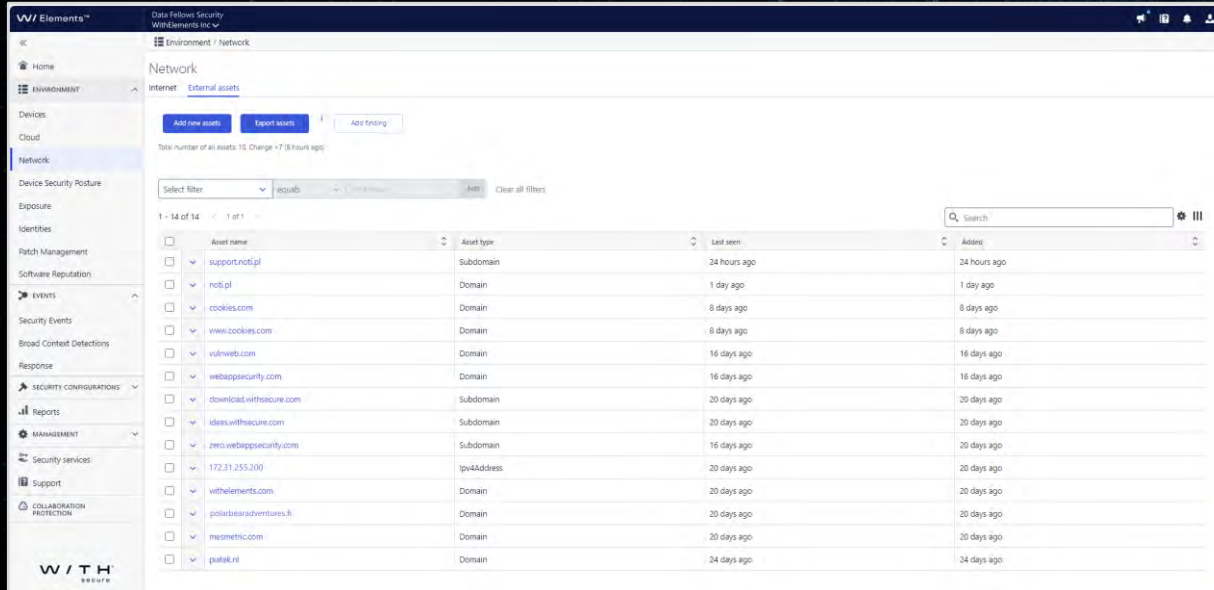
- Potential escalation of identity access rights
- Your part in supply chain breaches
- Employee security

### Exposure for Identity Risk

- Continuous assessment of identity-based risks
- Identity as part of potential attack paths
- Includes identity-related data in exposure assessment

# External Attack Surface (EASM)

## Protect your domains, IPs and public-facing assets



The screenshot displays the WTH Elements security dashboard. The main view is titled 'Network' and shows a list of 'External assets'. The table below contains the following data:

Asset name	Asset type	Last seen	Address
support.noki.pl	Subdomain	24 hours ago	24 hours ago
noki.pl	Domain	1 day ago	1 day ago
cookies.com	Domain	8 days ago	8 days ago
www.cookies.com	Domain	8 days ago	8 days ago
vulnweb.com	Domain	16 days ago	16 days ago
webappsecurity.com	Domain	16 days ago	16 days ago
download.withsecure.com	Subdomain	20 days ago	20 days ago
ideas.withsecure.com	Subdomain	20 days ago	20 days ago
zero.webappsecurity.com	Subdomain	16 days ago	20 days ago
172.31.255.200	Ipv4Address	20 days ago	20 days ago
withelements.com	Domain	20 days ago	20 days ago
polibearadventures.fi	Domain	20 days ago	20 days ago
mesmethic.com	Domain	20 days ago	20 days ago
psal&k.ru	Domain	24 days ago	24 days ago

Note: The UI views may undergo some improvements during the early access phase of the solution.

### Internet discovery

- Crawling and port mapping to collect data on public systems.
- Search the data based on location, top-level domain, pay-level domain, keywords, host name, and IP address.

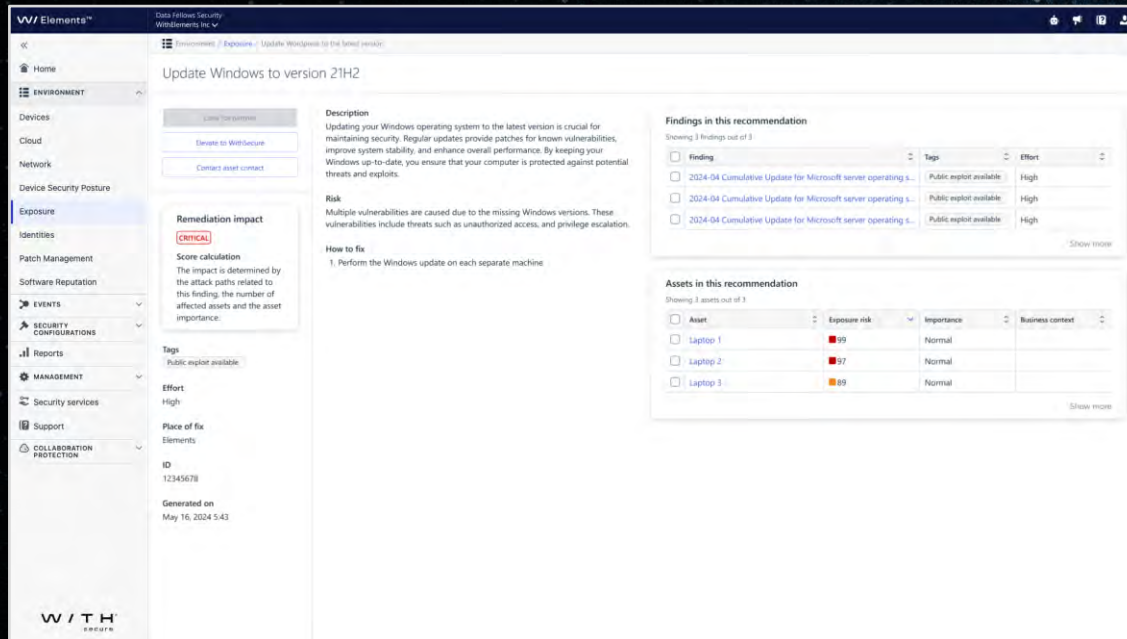
### Internet detections

- Domain takeovers
- Information disclosure from directory listing
- Continuous scope increase

# Remediate Exposures & Elevate Tough Cases

# Remediation

## Get actionable remediation guidance and track remediation



- Get unified instructions for remediation action, no matter the exposure type.
- Our actionable remediation guidance focuses on the top priority findings for you to work on.
- Communicate about the remediations for smooth collaboration.

Note: The UI views may undergo some improvements during the early access phase of the solution.

# Exposure Management Service

## Continuous Threat Exposure Management (CTEM)



### **Elevate** ON-DEMAND

Elevate tough cases in Exposure Management to WithSecure to get help with prioritization and validation.



### **Threat Hunting\*** 3-4 PER MONTH

Proactive Threat Hunting based on latest threat intelligence ensures that new and relevant findings are highlighted appropriately.



### **Exposure Review\*** PER QUARTER

Get the most out of your service through reoccurring Exposure reviews and summary of your security posture.

\* Planned for GA (General Availability) version of Elements Exposure Management. Services may have limited availability.



**SPHERE**  
to you



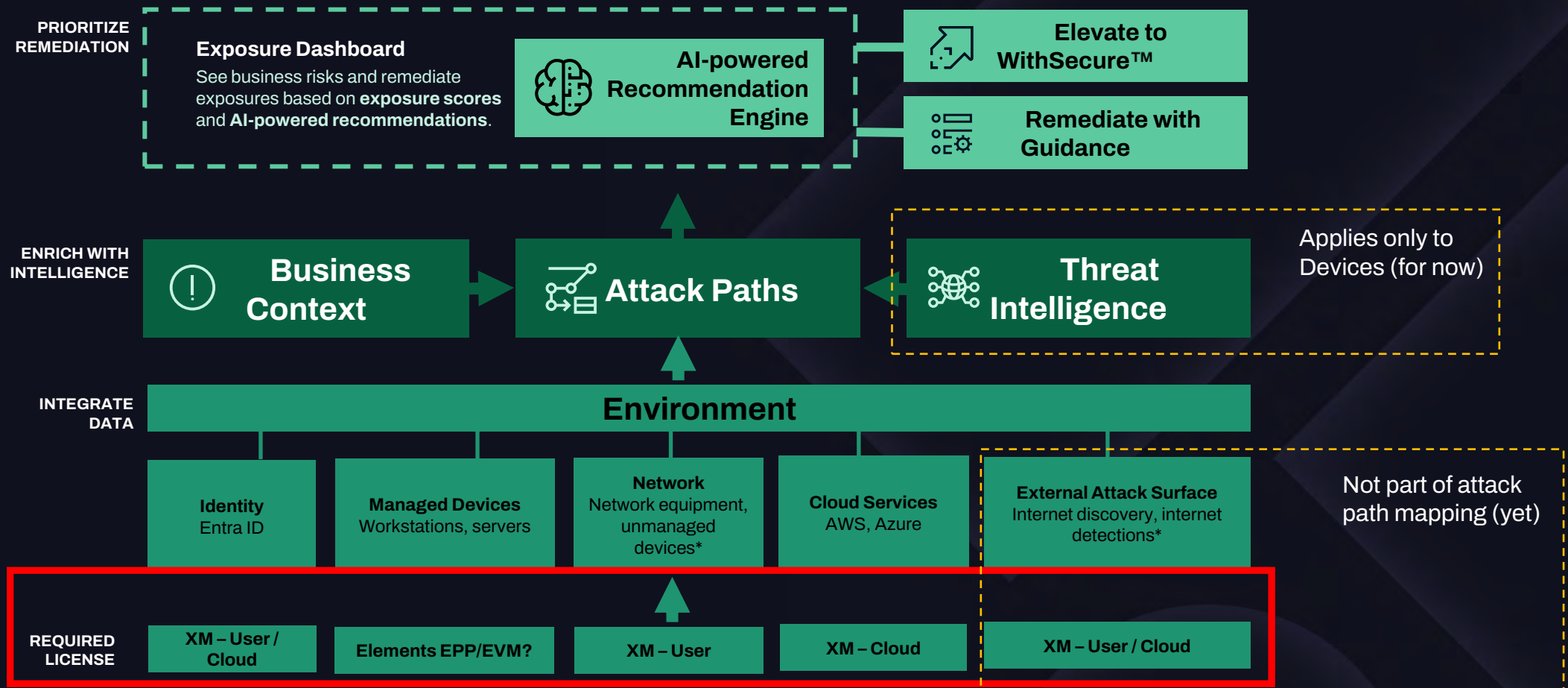
# Exposure Management: Available scanning methods

## External Attack Surface, Identity and Cloud platforms

## Managed Devices and network

External Attack Surface	Identity integrations	Cloud Integrations	Cloud Scan Node	Local Scan Node	Elements Agent
<b>Internet Discovery</b> Identify your organization's internet-facing systems	<b>Entra ID</b> Discover potential threats associated with all identities in Entra ID	<b>Azure</b> Assess the security and compliance posture of your Azure accounts	<b>Discovery scan</b> Identify and map all assets within internet	<b>Discovery scan</b> Identify and map all assets within your network	<b>Agent-based scan</b> Scan Windows workstations and servers automatically
<b>External assets</b> Identify and evaluate the security posture of all your externally exposed assets	<b>Account Breach</b> Breached account information	<b>AWS</b> Assess the security and compliance posture of your AWS accounts	<b>System scan</b> Scan all systems in internet that talk IP for vulnerabilities and misconfigurations	<b>System scan</b> Scan all internal systems that talk IP for vulnerabilities and misconfigurations	<b>Device service data</b> System configuration and login information
			<b>Web scan</b> Scan and test custom web applications for vulnerabilities	<b>Authenticated scan</b> Log into systems to gain more detailed vulnerability data	<b>Patch Management</b> System and 3rd party patch status and updates via Software Updater  <small>* Requires Elements Epp</small>
				<b>Web scan</b> Scan and test custom web applications for vulnerabilities	

# Exposure Management: Required licensing around available scanning methods



\* Planned for GA (General Availability) version.