Why do I need XDR?

A comprehensive guide to XDR – what it is and why the modern threat landscape calls for more comprehensive security.

Introduction

In the ever-evolving realm of cyber security, organizations face a constantly shifting threat landscape.

Advanced attacks have become more sophisticated, targeting vulnerabilities with precision and persistence.

Over the next few pages, we will:

- Lay out the intricacies of these threats
- Explore how Extended Detection and Response (XDR) emerges as a robust solution
- Demonstrate the natural progression from traditional Endpoint Detection and Response (EDR) systems towards XDR

In numbers :

Use of stolen credentials has become the most popular entry point for breaches.

90%

of organizations reported at least one identity-related incident in the last 12 months.

71%

spike in cyberattacks caused by exploiting identity

32%

Europe makes up 32% of global incidents

26%

Europe also experiences the most ransomware attacks globally (26%).

IBM's Cost of a Data Breach Report 2023 by Ponemon
(24 July 2023)

Stolen or compromised credentials (15%) and **Phishing** (16%) were the two most common initial attack vectors in 2023.

Breaches that initiated with stolen or compromised credentials took **the longest to resolve – nearly 11 months** (328 days) to identify and contain (overall mean time of 277 days).

Gartner says:

"By 2025, 50% of midmarket security buyers will leverage extended detection and response (XDR) to drive consolidation of workspace security technologies such as endpoint and cloud application security, and identity".

Gartner Top Trends in Cybersecurity 2022, 18 Feb 2022

Chapter 1: Current threat landscape

The modern-day threat landscape is constantly evolving. Cyber attacks are becoming more and more sophisticated and this is leading to increased complexity.

The rise of ransomware, phishing, and zero-day exploits.

Here are some of our W/Intelligence's recent findings:

- There are emerging signals that the ransomware industry peaked in scale in the second half of 2023 (H2) and ransomware productivity is starting to level off.
- Ransomware numbers and payments were still higher in the first half (H1) of 2024 than H1 2022, and H1 2023.
- Since 2022, Small / Medium sized businesses are increasingly posted to ransomware data leak sites as a proportion of all victims.

We explore:

Real-world case studies of high-profile breaches (THR)

> **"There are positive signals that ransomware productivity is waning, however the industry and western authorities must keep applying pressure and imposing cost on ransomware actors wherever possible."**
>
> **Tim West,** Director, Threat Intelligence & Outreach, WithSecure

Chapter 2: What is XDR?

Unlike traditional security tools that operate in silos, XDR offers a unified platform that provides unparalleled visibility into the security posture of an organization's entire IT and cloud infrastructure. By using a cloud-based data lake to aggregate and then AI and machine learning models to correlate and analyze vast amounts of data in real time, XDR enables security teams to swiftly detect, investigate, and respond to advanced threats across multiple attack vectors.

Modern attacks no longer start purely from malware on an endpoint, they stem from an attacker using an **identity** to gain access to business data.

XDR is a unified solution to protect modern IT estates by minimizing impact of attacks with:

- Advanced preventive controls
- AI-powered tooling, and access to flexible, round-the-clock expert services

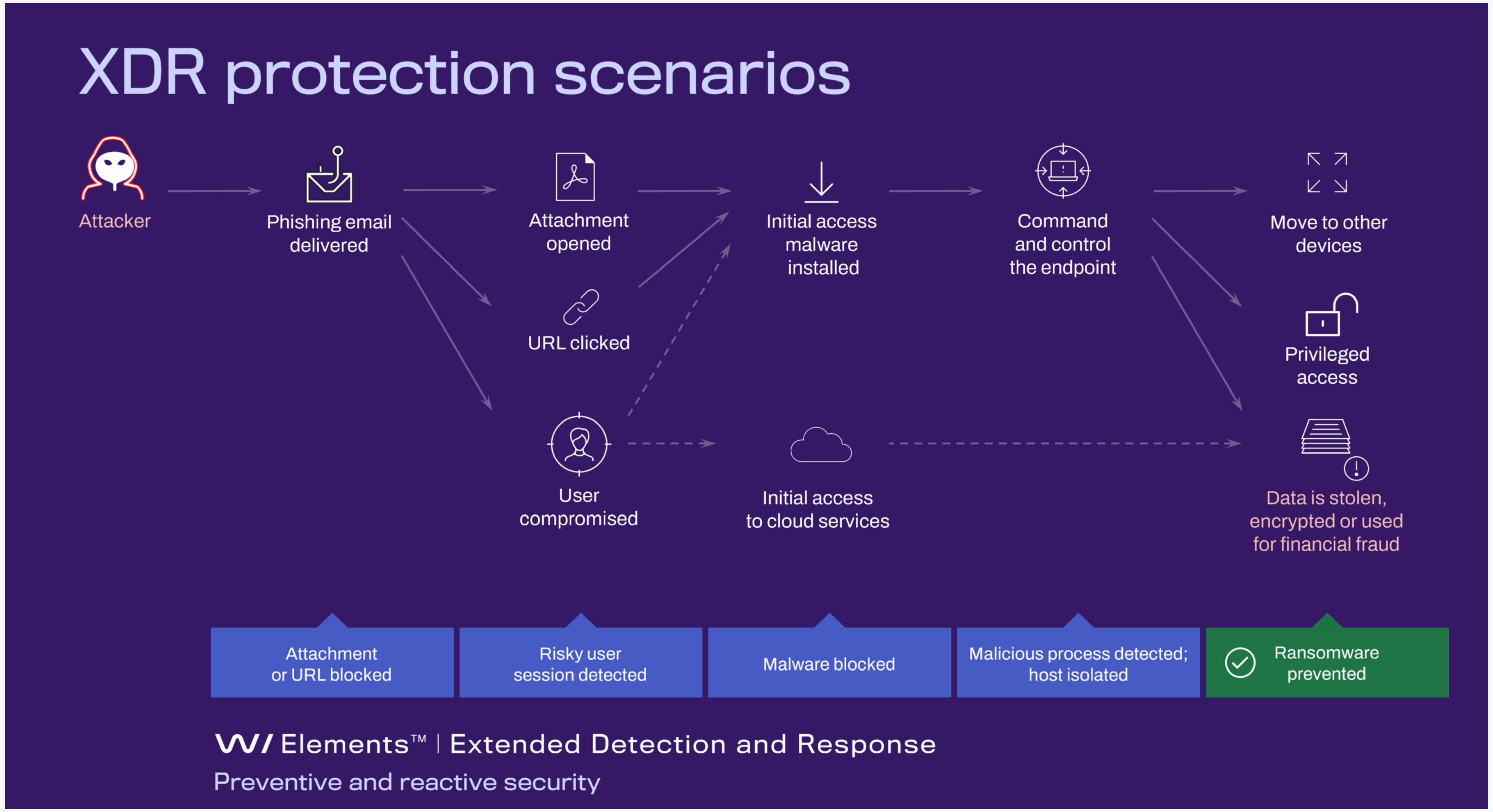
The modern IT estate – XDR is the evolution of EDR.

Traditional EDR tools do not provide the visibility beyond the endpoint. Instead, IT estates are now sprawling across cloud-hosted applications and emails.

Given **security skills are scarce,** having more tools doesn't necessarily mean you have the best security if you don't use them properly.

Chapter 3: How an attack happens

How we can help:



XDR protection scenarios

Attacker

Phishing email delivered

Attachment opened

URL clicked

User compromised

Initial access malware installed

Initial access to cloud services

Command and control the endpoint

Move to other devices

Privileged access

Data is stolen, encrypted or used for financial fraud

Attachment or URL blocked

Risky user session detected

Malware blocked

Malicious process detected; host isolated

Ransomware prevented

Elements™ | Extended Detection and Response

Preventive and reactive security

Modern day techniques used by threat actors include:

Social engineering

Malware

Exploit kits

Chapter 4: What is the difference between EDR and XDR?

EDR solutions focus on detecting and responding to threats for endpoints, whereas 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.

Chapter 5: How XDR addresses cyber security challenges

The fundamentals of XDR and its components

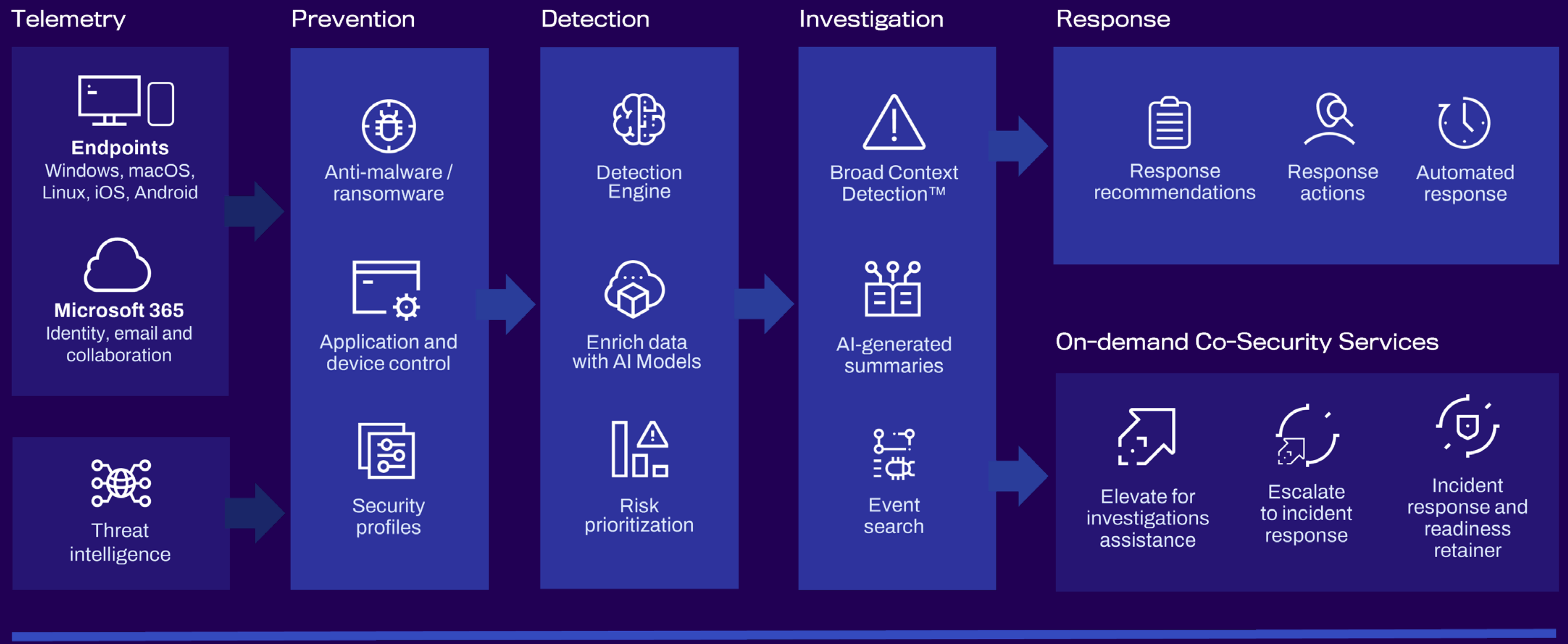
Detect modern environments and use a range of data sources

Prevention, detection and response capabilities

“incidents” are presented in one place, so have prioritized lists of work to be done

“Incidents” are easy to understand with actionable next steps

WithSecure Elements XDR in operation



Telemetry

Endpoints
Windows, macOS, Linux, iOS, Android

Microsoft 365
Identity, email and collaboration

Threat intelligence

Prevention

Anti-malware / ransomware

Application and device control

Security profiles

Detection

Detection Engine

Enrich data with AI Models

Risk prioritization

Investigation

Broad Context Detection™

AI-generated summaries

Event search

Response

Response recommendations

Response actions

Automated response

On-demand Co-Security Services

Elevate for investigations assistance

Escalate to incident response

Incident response and readiness retainer

Configuration, monitoring, investigation and response

Self-managed, partner managed, co-monitored or fully managed by WithSecure

Chapter 6: Identity Security within XDR

WithSecure Elements Identity Security, a module of Elements XDR, is designed to detect and respond to identity-based threats. This is achieved by alerting you to potentially compromised users and providing an understanding of the malicious activity and how to response [completed within the Microsoft 365 environment and third-party single sign-on services].

Key actions:

- Minimize time to detect identity-based attacks.
- Increase visibility into identity-related attacks and potentially compromised credentials that could turn into a data breach
- Protect your organization against stolen credentials – currently the most popular entry point for breaches – by getting an alert and allowing you to respond quickly when suspicious activity occurs. This minimizes the impact before any business-critical data is stolen.

Numbers :

71%

spike in cyberattacks caused by exploiting identity – reported by 90% of organizations.

7

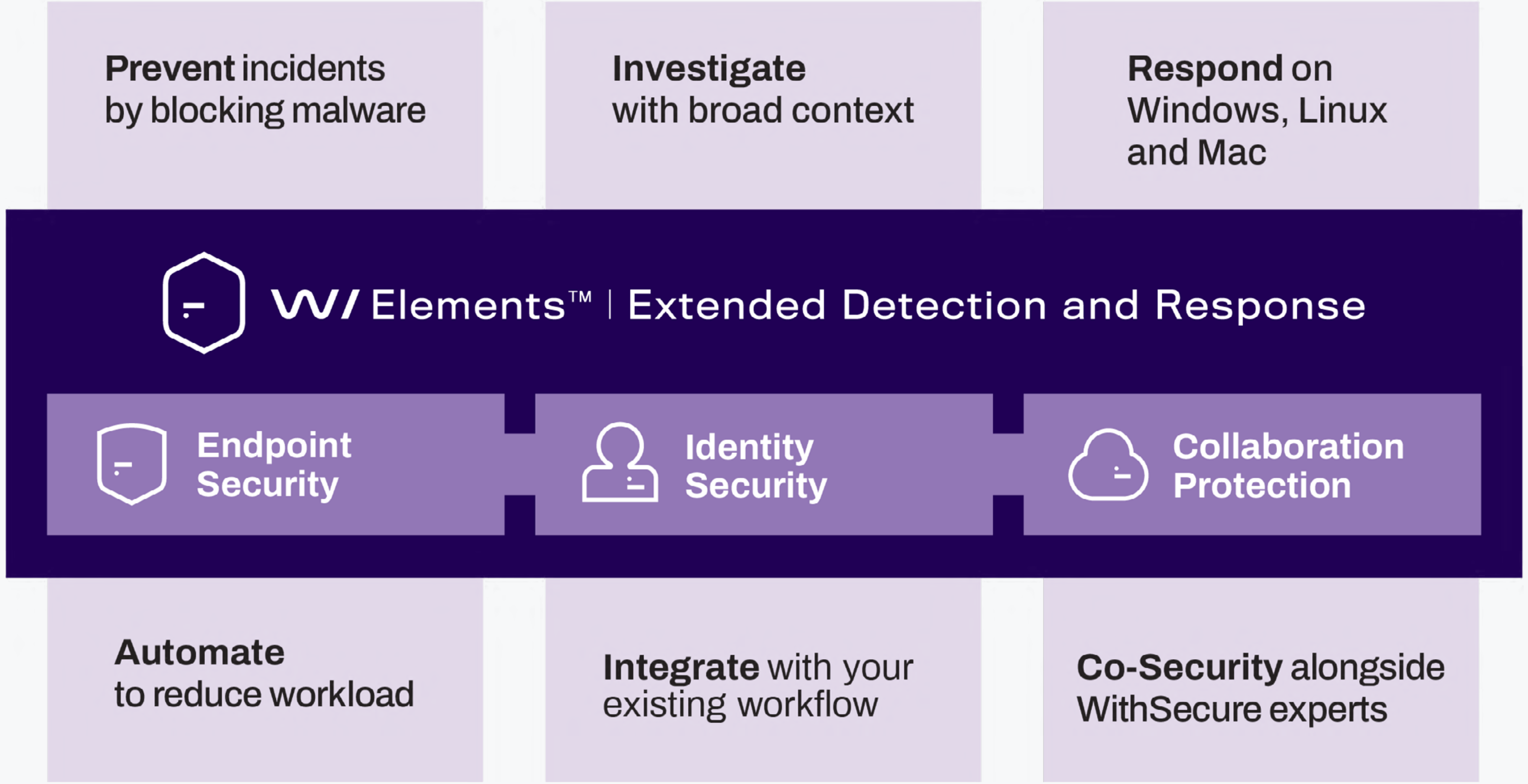
Attacks directly targeting Entra ID identities are on the rise based on our recent incident response engagements – 7 cases in the last 6 months, compared to 1 in the same period last year.

Chapter 7: How Elements works

WithSecure Elements XDR broadens visibility into attacks to enable earlier identification and faster response across your modern IT estate (endpoints, identities, email, and other cloud-based collaboration tools) by employing configurable, automatic preventive controls to block ransomware and fileless attacks before they cause a major incident.

Key actions:

- Gain visibility and protect your organization against modern threats.
- Monitor, investigate, prioritize and respond to threats across endpoints, identities, email and other collaboration tools.
- Augment your team with flexible, round-the-clock services.


Prevent incidents by blocking malware
Investigate with broad context
Respond on Windows, Linux and Mac
W/ Elements™ | Extended Detection and Response
Endpoint Security
Identity Security
Collaboration Protection
Automate to reduce workload
Integrate with your existing workflow
Co-Security alongside WithSecure experts

WithSecure™ Elements Endpoint Security

provides continuous protection for your endpoint devices - whether they are Windows, Mac, Linux or Mobile. Together, they offer comprehensive visibility into the security of your devices in the Elements Security Center, meaning that your Security Administrators can immediately see anything that needs attention.

WithSecure Elements Identity Security

is an identity threat detection solution. It protects organizations against identity-based attacks by detecting potentially compromised Microsoft Entra ID identities that are used by attackers to access Microsoft 365 or other cloud-based services.

WithSecure™ Elements Collaboration Protection

provides an overview of your security status within Microsoft 365. Elements Collaboration Protection secures the complete Microsoft 365 environment, covering Exchange, SharePoint, OneDrive, and Teams. The solution adds an extra layer of protection to Microsoft 365 native security capabilities, addressing advanced cyber threats such as malware, ransomware, compromised accounts, phishing and targeted attacks.

Chapter 8: AI in XDR

Embedded, award-winning AI

WithSecure has been using multiple machine learning models to support detection capabilities for nearly a decade. WithSecure's advanced adaptive AI engine acts as the core of Elements XDR to enrich collected events with additional information and suppress events based on normal baseline behavior. The newest addition implements clustering techniques to take the verdicts of similar incidents into the incident risk scoring. Elements Agent embeds on-device AI capabilities, developed as part of Project Blackfin, WithSecure's AI research, which was received an AI Excellence award for collective intelligence techniques such as swarm intelligence and multi-agent reinforcement learning.

New Generative AI experience

WithSecure Elements XDR includes a new AI experience called Luminen that adds Generative AI powered capabilities to help unskilled and overworked analysts by providing an easy to understand, human language summary of new activities. The new AI experience provides natural language explanations for Broad Context Detection™ with relevant threat intelligence and multi-lingual summary reports. WithSecure's customer-centric approach to the introduction of Generative AI only takes new algorithms into use whenever they are ready to meet our high quality and strict privacy standards.

Co-creation

Our XDR solution was created with help from our brilliant partners. Together, we plot the roadmap of our products so they work for everyone.

The future

If you'd like to be a part of that roadmap, get in touch today:

https://www.withsecure.com/en/trials-and-demos/epp-edr-trial