Open XDR

Unified Visibility Across Your Security Tools

Unify telemetry across your environment in a single overlay without rip and replace—backed by 24×7 Security Operations and expert-led threat hunting.

Most organizations already have security tools in place.

The challenge isn't lack of tools—it's the time, expertise, and correlation required to connect the dots before threats slip through. Security data lives in silos of OEM's product, alerts pile up, and teams struggle to quickly determine what actually matters.

Tools generate signals. Open XDR correlates, normalizes, and enriches them to create contextual alarms no single manufacturer can—then applies expert human analysis to turn that context into clarity.

Our Approach

Open XDR works with your existing security stack, enriching telemetry across the silos and bringing it together into single operational layer.

Open XDR correlates activity across your tools—adding expert-led threat hunting and investigation to your environment. The result is unified visibility, clearer investigations, and reduced dwell time, so your team can respond faster and more efficiently.

What Open XDR Delivers

Unified Visibility

Gain a single, contextual view of security activity across your environment—without rebuilding your stack.

Cross-Tool Correlation

Open XDR correlates and enriches telemetry across tools to reveal meaningful patterns and attacker behavior.

By correlating activity across endpoints, networks, and infrastructure signals, Open XDR reduces noise and accelerates investigations for your team—turning raw signals into actionable insight.

24x7 Expert Threat Hunting

Experienced security analysts continuously monitor and hunt for threats, escalating what truly matters to your team.

KEY BENEFITS

- **Unified Security Visibility**
  A single operational layer that correlates and enriches telemetry across your existing security tools.
- **24x7 Expert Threat Hunting**
  Continuous monitoring and human-led threat hunting surfaces threats your team can act on.
- **Faster, Confident Response**
  Cross-tool correlation delivers clearer investigations and accelerates your team's ability to respond decisively.
- **Stronger Security Posture**
  Continuous external and internal attack surface monitoring improves exposure awareness as environments change.
- **Lower Operating Overhead**
  No need to deploy a SIEM or staff and train a SOC.

> *No rip and replace.*
>
> *Just better outcomes from the tools you already use.*

CONTACT US

Our experts don't just triage alerts—they:

- Hunt for anomalous signals across your infrastructure
- Identify threats earlier in the attack chain and escalate to your team
- Investigate suspicious behavior across systems

This is AI-assisted, human-led detection—not just automated alerts.

Continuous Attack Surface Awareness

Open XDR includes continuous external and attack surface monitoring, extending security posture visibility across:

- Externally exposed assets (ESPM)
- Internal network-connected infrastructure (NSPM)

This monitoring helps identify risky exposures by not only scanning for CVEs, but also identifying exploits.

Add XDR Value Without Rip and Replace

Open XDR is ideal for:

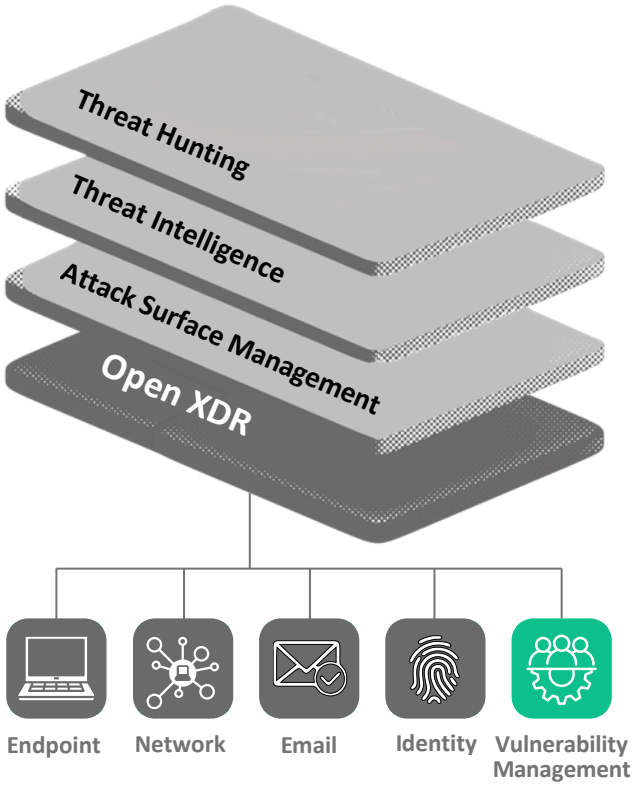
- Organizations that have invested in security tools but have limited internal bandwidth
- Teams overwhelmed by alerts and unclear investigations
- Organizations that want expert threat hunting without building a SOC
- Security teams seeking faster clarity—not more tools

A Single Operational Layer

Open XDR delivers unified visibility across security tools in your environment—backed by 24×7 security operations and expert-led threat hunting:

- Correlates and enriches alerts from the telemetry generated by your security tools
- Applies expert human threat hunting and investigation
- Reduces noise and surfaces actionable insights to your team faster

Enhance Your Existing Stack



Open XDR Features

Global SaaS Platform	
Secure, High Availability, Role-based Access	✓
24x7 Security Operations & Threat Hunting	✓
Up to aggregate of 60 MB of data per IP address per day	✓
Up to aggregate of 5 MB of data per email address per day (each IP address includes 2 email addresses)	✓
30 days hot storage for raw event data	✓
1 year hot storage for alerts, incident, and agent data	✓
M365/GWP Cloud Connector	✓
Network, Cloud Sensor	✓
Active & Passive Asset Discovery (NTA/UEBA)	✓