Definitive Guide to XDR:

Current Threats, Challenges & Solutions

ESET Cybersecurity
Progress. Protected.

Navigating XDR

Extended detection and response (XDR) is no longer a future-forward concept—it's an indispensable part of the organization's security stack. This guide is designed to help security professionals, IT leaders, and decision-makers make informed choices about XDR solutions.

Here's what you'll learn:

- The evolving threat landscape driving XDR adoption
- How XDR delivers visibility, speed, and integrated response
- 9 essential capabilities to demand from modern platforms
- What a solid XDR solution entails
- What to ask vendors
- How ESET delivers XDR and MDR in a unified ecosystem

Whether you're upgrading existing infrastructure or launching your first XDR deployment, this paper arms you with the insights, checklists, and evaluation strategies needed to secure your environment—efficiently and at scale.

Current Threats

To understand the value of XDR, it's essential to begin with the threats that continue to pressure organizations worldwide. A handful of threats have emerged as especially dangerous in the last couple years and have become increasingly difficult to manage without advanced, integrated detection capabilities. These **threats** don't just demand better visibility; they **require cross-domain correlation**, **behavioral analytics**, and **real-time contextual awareness**. In short, they simply demand XDR.

RANSOMWARE ATTACKS 3.0

Ransomware attacks have evolved over the course of the half-decade. Many modern operations now employ double or even triple extortion tactics combining encryption, data theft, and threats to third parties connected to the victim to maximize pressure and increase the likelihood of payment.

These campaigns can be preceded by long dwell times, even months long, during which threat actors quietly escalate privileges and exfiltrate sensitive data.

The average cost of a data breach was

$4.45 million

Source: *IBM, Cost of a Data Breach Report, 2025*

Typically, this involves exploitation of legitimate credentials, moving laterally with precision, and evading siloed tools—making fusion of telemetry across domains critical for detection. Moreover, attackers are increasingly able to exploit gaps in response—not because detections are missing, but because they're often ignored or overlooked by defenders.

The evolution continues with **ESET's recent discovery of PromptLock**, the first known **ransomware powered by generative AI**. It uses a local language model to autonomously generate malicious scripts, adapting its behavior based on prompts—without needing skilled developers. This marks a turning point: AI can now assist threat actors in crafting dynamic, cross-platform attacks. As AI-generated malware becomes more viable, XDR platforms must evolve to detect non-deterministic, behavior-driven threats in real time.

LIVING-OFF-THE-LAND AND POST-COMPROMISE TACTICS

Abuse of legitimate admin tools is one of the most persistent challenges that defenders need to face. These tools include PowerShell, PsExec, Windows Management Instrumentation (WMI), and AdFind. Known collectively as living-off-the-land (LOTL) tools, these allow adversaries to operate within the bounds of what appears to be normal administrator behavior.

In recent years, Microsoft has reported several cases of attacks abusing remote monitoring and management (RMM) tools such as BeyondTrust Remote Support and SimpleHelp—further expanding the scope of LOTL to include trusted third-party

platforms used by IT teams themselves (Microsoft Security). Attackers are capable of abusing legitimate tools and features within a target system to carry out malicious activity.

Some events, like dumping of the Local Security Authority Subsystem Service (LSASS) process, can trigger high-severity alerts due to their known threat profile. Others may appear benign in isolation, generating only low-severity or informational alerts. However, when correlated with identity access, lateral movement, or anomaly patterns, their true risk becomes clear. This is **where mature XDR solutions excel**: **exposing malicious intent through context**. Whether it's a flood of low-priority signals or subtle activity, it's the correlation that transforms noise into actionable insight.

DATA EXFILTRATION AND EXPOSURE

It's not surprising that data theft is often the final goal, not just a side effect. Exfiltrating sensitive data—whether financial records, intellectual property, source code, or customer information—from legitimate cloud storage platforms such as Dropbox, Google Drive, or OneDrive, continues to be a highly prevalent tactic among threat actors.

However, not all data exposure stems from external threat actors; misconfigurations, insider errors, or poor access controls can also lead to significant breaches. Misconfigurations in SaaS platforms or public cloud storage, insider negligence, or compromised service accounts can lead to high-impact leaks. XDR can identify these risks by **detecting anomalies in data flow and user behavior**, particularly when outbound traffic patterns deviate from normal baselines.

SUPPLY-CHAIN AND IDENTITY INTEGRATION RISKS

The modern supply chain is digital and deeply interconnected—encompassing vendors, SaaS platforms, APIs, and federated identity systems. Compromises no longer come just from software packages; they now emerge from misconfigured OAuth permissions, compromised third-party integrations, and identity providers (IdPs), which have become the new beachheads.

Recent high-profile incidents have shown how attackers exploit SSO misconfigurations, vulnerable CI/CD pipelines, or access tokens to infiltrate otherwise secure environments. Without **visibility across cloud**, **endpoint**, **and identity telemetry**, these indirect paths to compromise can remain undetected.

IDENTITY-BASED ATTACKS AND SESSION HIJACKING

Attackers know that identity is a valuable perimeter. Compromised credentials are involved in the vast majority of breaches, and multi-factor authentication (MFA) seems to be no longer a guaranteed defense. Adversaries are nowadays exploiting MFA fatigue, session token theft, and cookie replay attacks to gain and maintain access.

Once inside, they often operate under valid user sessions, making them nearly invisible to some tools—the tactic commonly known as living-off-the-land (LOTL).

80%

of breaches

involve identity-based techniques.

Source: *Verizon: 2025 Data Breach Investigations Report*

XDR excels here by **tracking how identities are used across systems**, **correlating behavior with known baselines**, **and surfacing high-risk anomalies**—even when the user is authenticated.

ACCESS-AS-A-SERVICE AND INITIAL ACCESS BROKERS (IABS)

The professionalization of cybercrime has given rise to access-as-a-service (AaaS), where initial access brokers (IABs) sell footholds into networks to ransomware gangs and other threat actors. These access points are often acquired months in advance and sit dormant until monetized.

The earlier that defenders can spot these initial compromises, the better. These incidents are often marked by strange authentication events, dormant admin accounts being reactivated, or reconnaissance from the command line. XDR enables **early threat hunting** and investigation, fusing low-signal events into high-confidence incidents.

CLOUD-NATIVE AND API-BASED ATTACK PATHS

Modern infrastructure is dynamic and cloud-native—built on containers, microservices, APIs, and serverless functions. Unfortunately, this agility comes with blind spots.

Adversaries are exploiting cloud workload vulnerabilities, misconfigured APIs, over-permissioned roles, and cloud identity mismanagement to traverse networks without touching endpoints.

The detection perimeter has shifted and without visibility across cloud telemetry, network activity, and endpoint logs, defenders miss the full picture. XDR fills that gap by linking signals from AWS, Azure, GCP, and SaaS platforms to on-premises activity, surfacing threats that live in the seams.

Today's threats are sophisticated not just in technical design, but in their ability to **exploit fragmentation in security tooling**. Attackers count on blind spots between siloed systems—whether endpoint, cloud, identity, or network.

79%

of organizations

experienced at least one cloud-related security incident in the past year.

Source: *Cloud Security Alliance: Top Threats to Cloud Computing 2024 Report*

The threats covered here, from stealthy ransomware and identity abuse to cloud native breaches and third-party risks, underscore the **urgent need for integrated**, **cross domain detection and response**.

XDR isn't just a tool. It's a response to how attackers operate today. The sections ahead explore how XDR delivers on this promise, what to look for in a solution, and how organizations can deploy it effectively to close the gaps and reclaim the advantage.

How Can XDR Help You?

While monitoring low-level events on endpoints might sound like background noise to busy security teams, it's time to take a broader view. In today's landscape, where identity misuse, cloud compromise, and AI-accelerated attacks dominate the headlines, the **right telemetry** can make or break your defenses. XDR isn't just about surfacing alerts—it's about enabling visibility, decision-making, and decisive response across your digital estate.

KEY BENEFITS

Organizations deploying XDR for the first time are often surprised by the sheer number and diversity of events that begin triggering detections. This initial visibility can become a turning point—exposing poor identity hygiene, cloud misconfigurations, shadow SaaS use, and threats that had quietly evaded earlier controls. The first wave of XDR deployment often brings **two immediate benefits**: **better visibility** into gaps in security architecture and **faster identification** of previously undetected threats.

34%

of tech leaders

worldwide prioritize cloud security in their cybersecurity investments.

Source: *Statista: Cybersecurity Investment Priorities For Tech Leaders Worldwide In 2025*

In the first section, we explored threats that are notoriously difficult to catch without extended detection. With a modern XDR approach, organizations gain confidence tackling challenges like ransomware, destructive malware, supply-chain attacks, and insider threats. Just as important is the ability to detect abuse of legitimate tools—whether it's a cloud storage service being used for exfiltration, or a trusted identity provider being hijacked as a point of entry.

Today's XDR platforms go beyond SIEM-style correlation by incorporating behavioral analytics, real-time context enrichment, MITRE ATT&CK mappings, and increasingly, AI driven pattern recognition to surface early signs of compromise. These are features that Forrester identified as key differentiators in its 2025 Security Analytics Platforms report.

By referencing tactics and techniques from the ATT&CK framework, defenders can more accurately emulate adversaries and proactively **tune** their **coverage**. As new methods—like token theft, cloud role escalation, and lateral movement across IdPs—emerge, XDR evolves in lockstep.

XDR also empowers modern **threat hunting**, enabling analysts to **formulate hypotheses** and **search across endpoints**, **cloud environments**, **identities**, **and network flows**. With the help of GenAI-based summarization and visualizations, threat hunters can more quickly pivot from weak signals to full attack narratives. Hunting has become not only more effective but more accessible to broader teams, regardless of experience level.

> **"By 2026, more than 80% of organizations will have consolidated endpoint management teams and tools into a centralized team utilizing a single UEM platform, up from about half in early 2022."**

Gartner: *Consolidate Endpoint Management Teams, Tools and Strategies to Reduce Cost and Optimize Operations, Tom Cipolla, Sean Bankston. [3 July 2024] ID: G00778293*

Today, **AI within XDR** has shifted from passive correlation to active augmentation—helping **prioritize high-risk detections**, **summarize attack chains**, and even **propose response steps**. Gartner notes that modern XDR platforms increasingly rely on machine learning for dynamic baselining and GenAI for alert contextualization. This reduces analyst load and accelerates triage. Once a threat is uncovered, today's XDR systems offer built-in response automation, triggering playbooks that can isolate a host, revoke a token, disable a user, or alert human responders.

This speeds up containment and reduces dwell time, especially during off-hours. And with process correlation, XDR helps incident responders trace alerts back to the initial point of compromise, often pinpointing open authorization abuse, third-party access, or software supply-chain issues as root causes.

Modern XDR doesn't operate in a vacuum. It integrates tightly with cloud workload protection platforms (CWPPs), SaaS security tools, SIEMs, and even CI/CD systems, providing a unified picture of modern infrastructure.

For defenders tasked with securing sprawling, hybrid environments, XDR becomes a connective tissue for collaboration and shared context.

DEMONSTRATING XDR'S VALUE

The focus has firmly shifted from proving that you "have XDR" to demonstrating the measurable value it delivers. This includes not just mean time to detect or respond (MTTD/MTTR), but also a reduced blast radius of breaches, faster cross-team triage, and clearer insights into where risk accumulates. The ability to reduce tooling overhead—by fusing detection, investigation, and automation into a single platform—has become a powerful factor in budget-conscious decision-making.

52%

of security teams

plan to increase XDR investment.

Source: *Cloud Security Alliance: Top Threats to Cloud Computing 2024 Report*

What to Look for in XDR

UNDERSTANDING THE EVOLUTION OF XDR

When XDR first entered the market, it was hailed as a means to unify alert signals from disparate security tools and reduce the burden on SOC teams. Early offerings focused on correlation—pulling EDR, email, and network alerts into a single console. But today's expectations have evolved.

Modern XDR platforms are expected not only to correlate signals but also to **analyze behavior**, **automate response**, and **map attacks** across hybrid environments. As threat actors shift toward identity compromise, cloud abuse, and AI-enhanced evasion, the scope of XDR must expand to cover endpoints, identities, SaaS apps, CI/CD pipelines, and more.

This evolution means that buyers must rethink what "good XDR" looks like. The criteria for evaluation have changed—from merely aggregating alerts to delivering investigation support, attack surface visibility, and adaptive response capabilities. The next sections walk you through eight essential technical capabilities and one strategic aspect you should expect from an XDR solution.

9 KEY THINGS TO EXPECT FROM A MATURE XDR SOLUTION

DETECTION

At its core, XDR must spot threats that other tools miss. That means going beyond signature or IoC matching and embracing behavioral analytics, identity telemetry, and cloud-native signals. **Look for platforms that** not only correlate events across endpoints, workloads, users, and SaaS apps, but also **track and reconstruct entire attack chains** as unified incidents.

This deeper level of correlation, a core strength of ESET Inspect, enables security teams to understand how individual events connect across time and systems. It's precisely this capability that sets ESET apart in the recent MITRE ATT&CK Evaluations, where ESET Inspect demonstrated exceptional visibility and context-building across the multiple stages of the attacks.

The best XDR solutions detect techniques such as token abuse, credential stuffing, lateral movement via identity providers (IdPs), and activity tied to known MITRE ATT&CK tactics.

They also prey on the fatigue of potential victims for using MFA, where attackers manipulate users into approving repeated authentication requests. Detection should also integrate with **threat intelligence** and apply machine learning to suppress noise while preserving fidelity.

As AI adoption accelerates across both defensive tooling and enterprise workflows, security leaders must walk a fine line between innovation and oversight—especially as misuse, data leakage, and unintended exposure become growing concerns. Meanwhile, attackers are beginning to experiment with AI, though its integration into their tactics remains emergent.

According to the 2025 IBM Cost of a Data Breach Report, 97% of organizations that experienced AI-related security incidents lacked adequate access control, with many attacks originating from third-party tools or shadow AI. Yet, those embracing AI for detection and automation see significantly lower breach costs—confirming that strategic **AI adoption in XDR** can drive both **efficacy and efficiency**.

RESPONSE

Detection is only half the equation—response is where XDR delivers operational value. Look for platforms that support **native response actions** across multiple surfaces: isolating hosts, disabling users, revoking tokens, and integrating with firewalls or CASBs to contain cloud-based threats.

61% of security practitioners

think there are too many threat intelligence data feeds.

Source: *TechRadar: Security overload is leaving admins with too much alert data to comprehend - which makes things even more dangerous*

Effective XDR also includes playbook-driven automation and integrates with IT service management tools for coordinated response. Customizable response policies and role-based access are crucial for ensuring appropriate actions without overstepping.

BALANCE

Noise remains a critical pain point. A mature XDR platform should strike the right balance between visibility and actionability. It should use severity scores, risk-based prioritization, and behavioral baselining to prevent alert fatigue while ensuring that real threats are never buried.

Custom tuning, **exclusions**, and the ability to **provide context around alerts**—showing root cause, impacted assets, and kill chain progression—helps analysts triage and act both faster and more effectively.

TRANSPARENCY

Analysts need to understand why a detection occurred and what logic led to an alert. **Transparent rule logic**, **detection mapping** to MITRE ATT&CK, and clearly **surfaced telemetry** paths are now expected from any leading XDR product.

53%
of cloud alerts

are irrelevant, leading to reactive response modes.

Source: *TechRadar: Security overload is leaving admins with too much alert data to comprehend – which makes things even more dangerous*

The ideal solution would be to look for platforms that offer query access to raw data, detection explanations, and severity scoring. Bonus points go to solutions that allow rule creation or modification using open standards like SIGMA or support integration into analytics pipelines via APIs.

CUSTOMIZATION

Every environment is different. Knowing what's normal for yours is crucial. Tuning XDR according to your circumstances is what makes it a powerful solution. An XDR platform should allow analysts to define custom detection logic, automate responses based on their playbooks, and tailor views to role-specific needs.

Custom indicators, **detection rules**, **hunting queries**, and dashboard widgets all contribute to better situational awareness so that your organization's defenders can achieve the desired balance between risk and noise. Support of user and entity behavior analytics (UEBA) tuned to highlight abnormal behavior specific to your baseline is a must.

INTEGRATION

Modern XDR cannot exist in a silo. The best platforms integrate with a broad ecosystem of third-party tools—firewalls, EPPs, SIEMs, IAMs, ticketing systems, and threat intel providers. Integration should be **easy to configure** and supported by robust APIs.

While some solutions emphasize native integration where many vendors typically offer both endpoint security and cloud-based reputation and detection systems, many security teams prefer best-of-breed interoperability. What matters most is **seamless data flow**, enrichment, and response across your existing investments.

MULTIPLATFORM COVERAGE

XDR must cover more than endpoints. It should bring visibility into Windows, macOS, Linux, and mobile—while also ingesting telemetry from cloud platforms (AWS, Azure, GCP), SaaS apps (M365, Google Workspace, Salesforce), and identity systems (Okta, AAD, Ping). Look for support for container workloads, CI/CD pipelines, and network telemetry. The ability to trace **lateral movement** across cloud, **identity**, and **endpoint surfaces** is a must in today's attack landscape.

SERVICES

Not all organizations have the resources to fully staff a SOC. Leading XDR vendors offer managed services (MxDR) as part of their solution, ranging from monitoring and triage to guided response, threat hunting, and beyond.

Even without fully outsourcing detection, onboarding support, tuning assistance, and continuous optimization services can accelerate time to value. **Service maturity** can be a major differentiator between vendors so be sure to determine whether the vendor provides more than just a product:

- Deployment and optimization services
- Managed detection and response services, including threat hunting
- Security health checks
- A partner or local office in your region
- Technical support in local languages

VENDOR

Finally, evaluate the vendor behind the XDR: market presence, product roadmap transparency, integration velocity, and customer support all matter. Third-party validation and tests such as MITRE ATT&CK® Evaluations or Endpoint Prevention & Response (EPR) Test, peer reviews, and other analyst reports can help separate mature vendors from those still catching up.

XDR is a strategic investment and therefore it's in your best interest to make sure that the **vendor's vision aligns with your architecture**, **security priorities**, and **operational constraints**. You can do this by asking about their roadmap, commitment to open standards, update frequency, and performance in independent evaluations like the ATT&CK Evaluations or Forrester Wave.

Buyer's Checklist

As XDR matures into a central pillar of modern SecOps, choosing the right platform goes far beyond comparing features. This checklist helps buyers assess not only capabilities, but also operational impact, vendor maturity, and ecosystem fit.

DETECTION & COVERAGE

- ☐ Supports behavioral analytics and correlated multi-domain detections
- ☐ Includes identity, cloud, and SaaS telemetry (beyond endpoints)
- ☐ Detects sophisticated threats: token theft, lateral movement, MFA fatigue, etc.
- ☐ Integrates with threat intel for enriched detection
- ☐ Maps to MITRE ATT&CK with details on how the action or technique was performed

INVESTIGATION & RESPONSE

- ☐ Offers a centralized investigation view with attack storylines or timelines
- ☐ Enables cross-domain response actions to coordinate host isolation, token revocation
- ☐ Includes customizable automated playbooks
- ☐ Integrates with ITSM tools for incident ticketing and workflow
- ☐ Reduces MTTR through pre-built response logic and context-rich alerts

CUSTOMIZATION & TRANSPARENCY

- ☐ Allows rule editing, hunting queries, and detection tuning
- ☐ Supports open standards (e.g., SIGMA, STIX, OpenTelemetry)
- ☐ Offers full transparency into alert logic and scoring
- ☐ Role-based access to views, rules, and dashboards
- ☐ Enables a transparent feedback loop to fine-tune performance

INTEGRATION & SCALABILITY

- ☐ Connects via APIs to firewalls, IAM, SIEM, and other tooling
- ☐ Supports hybrid/multi-cloud infrastructure and remote assets
- ☐ Flexible enough to accommodate vendor-native or best-of-breed technology stacks
- ☐ Enables modular expansion (e.g., cloud workloads, OT, containers)
- ☐ Built to scale across multiple business units or locations

SERVICES & VENDOR RELIABILITY

- ☐ Offers onboarding, tuning, and continuous optimization services
- ☐ Includes access to local technical support and partner presence
- ☐ Provides access to threat hunting or MxDR (if needed)
- ☐ Clear roadmap and regular product updates
- ☐ Validated by third-party tests (ATT&CK Evaluations, Forrester Wave, peer reviews)

MUST-HAVE

- ☐ Correlated detection across endpoint, cloud, and identity
- ☐ Automated, customizable response playbooks
- ☐ Integration via open APIs
- ☐ Transparent detection logic
- ☐ Precise mapping to MITRE ATT&CK techniques
- ☐ Local language support or regional service partners

NICE-TO-HAVE

- ☐ GenAI-powered hunting assistants
- ☐ Built-in modules for executive reporting
- ☐ Threat actor attribution tagging
- ☐ Native support for OT/IoT telemetry

AVOIDING VENDOR OVERPROMISING

In a crowded and fast-moving space like XDR, it's easy to be swayed by polished demos and bold claims. Insist on vendor proof points: third-party evaluations (like ATT&CK® Evaluations), customer case studies, and realistic deployment timelines.

Ask whether a feature is generally available, in early access, or just on the roadmap. **Clarity upfront avoids disappointment post-purchase**.

KEY QUESTIONS FOR AN XDR REQUEST FOR PROPOSALS

- Which data sources are natively integrated, and which require custom connectors?
- How does your platform support detection of identity-based threats?
- What types of response actions are automated out of the box?
- How are detection rules tuned and updated over time?
- Can you demonstrate MITRE ATT&CK mapping and recent evaluation results?
- What services are included in onboarding and optimization?
- Is support available in our region and language?

The XDR market will continue to evolve, but the principles of visibility, integration, and operational efficiency will remain at the core of any strong security program.

Use this checklist above not just to compare vendors, but also to **define the value you expect** from your next-generation detection and response platform.

Schedule an XDR Demo

Empower Your XDR with ESET

Using behavioral analytics across the endpoint, network, cloud, email, and other layers is a defining framework for ESET's approach and methodology. It enables spotting suspicious activity and stopping attackers before they can make an impact. To make this possible, ESET leverages its industry-leading technology solutions such as XDR.

ESET Inspect, our XDR-enabling solution, provides risk managers and incident responders with outstanding visibility into threats. It allows them to perform fast and in depth **root cause analysis**, and immediately respond to incidents. Paired with the time-tested preventive power of ESET's endpoint protection products, **ESET Inspect is a cloud-delivered**, **XDR-enabling solution** that can:

- Detect advanced persistent threats
- Stop in-memory threats
- Block zero-day threats
- Protect against ransomware
- Prevent company policy violations

THE ESET DIFFERENCE

Complete prevention, detection & response

ESET Inspect enables quick analysis and remediation of any security issue in your network. ESET's underlying multilayered security, in which every single layer sends data to ESET Inspect, analyzes vast amounts of data in real time to detect threats.

Solution from a security-first vendor

ESET has been fighting cyberthreats for more than 35 years. As a science-based company, it has long been at the leading ➔ edge of developments like AI, cloud technology, and now XDR.

Prevention is better than cure

ESET's approach to XDR is tightly connected to its multi-award-winning prevention products. Thanks to our commitment to developing high-quality detection technology, ESET prevention technology is world leading.

Detailed network visibility

With transparent detection rules (ESET Inspect has 1620 and counting), indicators of compromise (IoC), and search capability, an in-depth review of

➔ your network will allow you to identify suspicious behavior.

Ready to start working now

ESET's solution works out of the box and is powerful enough to allow granular modification by experienced threat hunters.

Flexibility of deployment

We let you decide how to deploy your security solution: ESET Inspect can run on your own server or in the cloud, allowing you to tune your setup according to your TCO targets and hardware capacity.

MITRE ATT&CK®

ESET Inspect references its detections to the MITRE ATT&CK® framework, which – with just one click – provides you with comprehensive information about even the most complex threats. ESET is a top independent cybersecurity software company and in the top 10 out of more than 350 contributors to ATT&CK.

➔ **Reputation system**

Extensive filtering enables security engineers to remove known good applications from consideration, based on ESET's robust reputation system. The ESET system contains a database of hundreds of millions of benign files to ensure security teams spend their time on unknown – and potentially malicious – files, not on false positives.

Automation & customization

Easily tune ESET Inspect to the level of detail and automation you need. Choose your level of desired interaction, and the type and amount of data to be stored, during the initial setup and with the help of preset user profiles, and then let Learning Mode map your organization's environment and suggest exclusions to false positives where needed.

BENEFITS OF ESET'S XDR SOLUTION

Organizations now require greater visibility into endpoints, devices, and networks to protect their profits and reputation from emerging threats, employee risks, and unwanted applications.

ESET Inspect, which is a part of ESET PROTECT, is a cloud-based, XDR-enabling solution that delivers unique behavior and reputation-based detection, providing **real-time feedback** to security teams, **using global threat intelligence** from ESET LiveGrid®.

ESET Inspect monitors authentication events, cloud role escalations, and SaaS access patterns to detect lateral movement, OAuth abuse, and token misuse. Combined with identity correlation and anomaly detection, this makes the ESET PROTECT platform **capable of addressing today's most evasive identity-based threats**.

Organizations can benefit from this solution thanks to:

Expertise

Detection and response from a trusted, research-based, security-first vendor with over 35 years of experience on the cutting edge of digital security.

Flexibility

Works out of the box and is powerful enough for experienced threat hunters, offering granular controls for optimal tailoring to each user's environment.

Quality

Tight integration with ESET's multilayered prevention products, built on award winning technology with industry-wide recognition.

Transparency

Transparent detection rules ensure detailed visibility across multiple layers, including email, networks, and servers.

FROM XDR TO MDR: SECURE AND STREAMLINED

ESET XDR delivers transparent, behavior-based detection, advanced threat hunting, and fast incident investigation across endpoints, email, SaaS, and identity layers. For organizations wanting to focus on core operations, ESET offers **ESET PROTECT MDR**, a 24/7 managed service that **pairs this powerful XDR engine with expert-led monitoring**, threat hunting, incident response, and remediation support.

Transitioning from self-managed XDR to ESET's MDR is straightforward: the same technology—ESET Inspect—is integrated into your environment, and then ESET's global team takes over detection management, alert triaging, and automated response tasks. Clients benefit from **industry-leading 6-minute MTTR**, proactive threat hunting, and access to **threat intelligence across over 100 million global endpoints**—all without hiring in-house cybersecurity staff.

With ESET MDR, teams remain in control via the ESET PROTECT console, but enjoy the added advantage of continuous service, optimized detection tuning, local language support, and compliance-ready reporting. The result? Strong security posture delivered as a fully managed service.

This MDR model is particularly effective against stealthy techniques like identity abuse and LOTL attacks, where adversaries operate under valid credentials or use built-in tools like PowerShell and WMI to evade detection.

ESET experts analyze deviations from user and system baselines to surface such threats early—before lateral movement or privilege escalation occurs.

Within MDR, visibility is driven by **endpoint and email telemetry** from ESET's security solutions, enabling precise detection of misuse of legitimate tools and stealthy attacker techniques. For organizations adopting ESET's broader Managed Cybersecurity offering, this coverage **can be extended across additional perimeters**—including identity, network, and cloud services—helping eliminate blind spots and enabling high confidence response actions without overwhelming internal teams with noise or false positives.

22% of tech leaders

worldwide prioritize cyber managed services in their cybersecurity investments.

Source: *Statista: Cybersecurity Investment Priorities For Tech Leaders Worldwide In 2025*

Conclusion

The promise of XDR lies not in flashy acronyms but in tangible outcomes: reduced dwell time, broader visibility, and smarter, faster decisions. As threat actors weaponize identities, cloud misconfigurations, and SaaS integrations, the ability to correlate across domains and automate response is no longer optional.

This guide has explored both the shifting threat landscape and what modern buyers should demand from an XDR platform—**visibility**, **integration**, **transparency**, and **support**. ESET's XDR and MDR offerings respond directly to these needs, enabling security teams to scale capabilities without scaling headcount. Whether self-managed or fully outsourced, the path forward is clear: make detection and response extensible, adaptive, and centered on what matters most—cyber resilience.

Schedule an XDR Demo

XDR CUSTOMER CASE STUDY

Kohlpharma

Kohlpharma is one of Europe's top pharmaceutical importers, based in Germany. Since 1979, it's helped lower healthcare costs by supplying affordable branded medications, backed by advanced logistics and a strong focus on cybersecurity. The company employs 800 people and plays a key role in ensuring timely access to medications across Germany.

As a critical infrastructure provider, Kohlpharma needed a security solution to protect its automated logistics systems from cyber threats—requiring both anti-malware and advanced endpoint detection and response (EDR) tools. They were increasingly targeted, and the stakes were high: any disruption could result in multi-million dollar losses and erode trust with patients and partners.

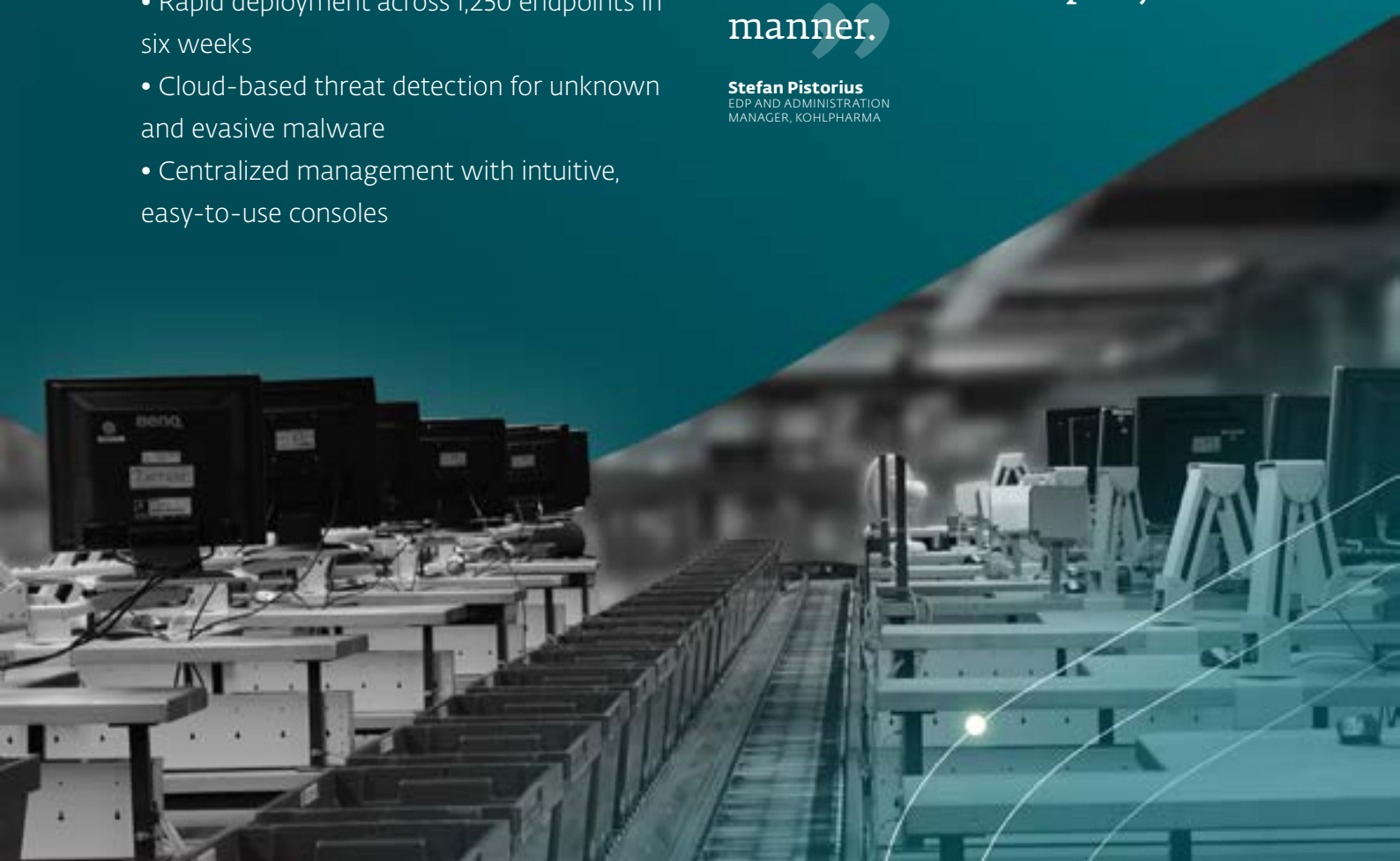
ESET delivered a layered security setup including ESET PROTECT Entry, LiveGuard Advanced, and Inspect. The full rollout across 1,250 endpoints was completed in just six weeks, with seamless collaboration and fast implementation. ESET's strong detection rates, transparent communication, and cost-benefit advantage made it the clear choice.

KEY BENEFITS

- Advanced & robust protection for critical infrastructure and automated systems
- Rapid deployment across 1,250 endpoints in six weeks
- Cloud-based threat detection for unknown and evasive malware
- Centralized management with intuitive, easy-to-use consoles

> "A complex IT security solution must work properly and yet be easy to use. ESET masters this balance in an exemplary manner."

Stefan Pistorius
EDP AND ADMINISTRATION MANAGER, KOHLPHARMA



This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach.** We combine the power of AI and human expertise to make protection easy and effective.

Experience **best-in-class** protection thanks to our in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers.

ESET protects your business so it can unlock the full potential of technology. Progress. Protected.

Schedule an XDR Demo

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

eset
Cybersecurity
Progress. Protected.