kaspersky bring on the future

How to protect enterprises against complex cyberattacks

Have you ever lain awake at night, concerned that some kind of advanced cyberthreat might be lurking inside your infrastructure, just waiting for the right moment to steal your intellectual property or hold your enterprise or business for ransom?

If so, you have good reason. As their name suggests, advanced persistent threats (APTs) use sophisticated hacking techniques to gain access to your systems. Once they breach your defenses, they can stay undetected for months or even years, gaining higher-level access privileges, and harvesting and exfiltrating your data with potentially devastating results.

Who's at risk?

Unsurprisingly, it takes a significant amount of skill, effort and resources to mount an APT or targeted attack, with the result that their prime targets are often government sectors or large corporations with sensitive or proprietary data that justifies the investment.

But despite this, APTs are a method of attack that should be on the radar for businesses everywhere – with even medium-sized businesses potentially at risk.

APT attackers are, for example, increasingly targeting smaller companies that make up the supply chains of their ultimate targets. Because such companies are typically less well-defended, they can act as stepping stones to gain access to the larger organizations they work with.

As a result, whether you're a major enterprise or a smaller business that could potentially be exploited to target a larger organization, it's important to **understand the nature of the threats** you could be facing. This includes APTs and other targeted attacks – and the capabilities required to defend against these.

All sectors targeted

During the last two years, human-driven targeted attacks were observed in all sectors. In 2024, the IT and government sectors led with 14.7% and 13.8% respectively.

Source: Kaspersky Managed Detection and Response 2024 Analyst report

$4.88 million

The global average cost of a data breach in 2024 – marking a 10% increase over 2023 and the highest total ever. In the Middle East region, this indicator is significantly higher, reaching $8.75 million.

Source: IBM's 2024 Cost of a Data Breach Report

258 days

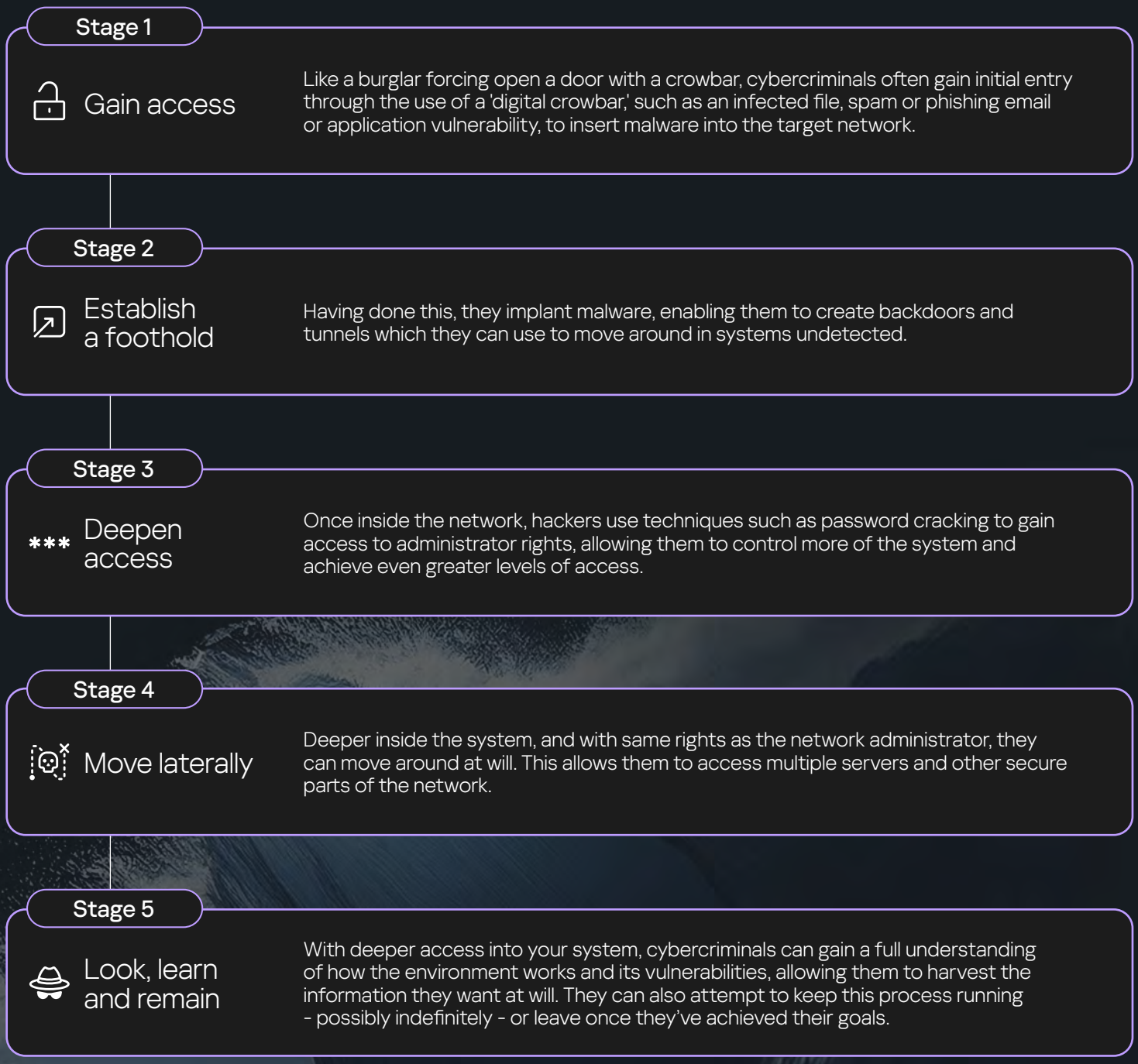
The time to identify and contain a breach. This extended recovery period not only exacerbates financial losses but also leaves organizations vulnerable to further attacks.

Source: IBM's 2024 Cost of a Data Breach Report

How do APTs work?

The whole point of an APT is to gain persistent or ongoing access to the target's IT and/or OT (operational technology) systems, which hackers generally achieve through a five-stage process.

Figure 1: Stages of an evolving APT



What are the potential consequences of falling victim to an APT attack?

Read the media coverage of any organization that has experienced a targeted attack and it will be clear that the effects can be both severe and long-lasting. While the immediate impacts typically include financial harm caused by loss of data and business disruption, longer-term effects can include damage to the organization's reputation, customer trust and potential legal proceedings.

Then of course there's the issue of repairing the damage to the organization's IT infrastructure, which often takes months or sometimes even years to complete. And, depending on which industry you're operating in, there can be sector-specific consequences as well.

Figure 2: Understanding the impact of APTs on business security

Finance

- Disruption to critical services
- Unauthorized transactions
- Cash-out attacks
- Legal consequences of identity theft

Government

- Potential effects of cyber-espionage
- Damage to critical infrastructure
- Disruption to e-government services
- Exposure of citizens' personal data

E-commerce

- Legal implications of account takeover via identity theft
- Fraudulent transactions
- Denial of IT services, revenue losses
- Potential fines under GDPR, PCI DSS, etc.

Transportation

- Operational disruption and shutdowns
- Supply chain delays and increased costs
- Threat to life
- Damage to critical infrastructure

Food

- Stock shortages and production shutdowns
- Compromised food quality
- Potential contamination with chemicals, toxins, etc.
- Need to fall back on manual operations

Healthcare

- Disruption to critical services
- Exposure of patients' personal data
- Undermined public trust
- Potential threat to life

IT and Telecom

- Loss of customers
- Loss of sales
- Unplanned network downtime
- Fixed and mobile service disruption

Industrial

- Environmental disasters
- Operational disruption
- Increases in unplanned downtime
- Cascading failures or system-wide blackouts

>2

high-severity incidents happen every day.

43%

of all high-severity incidents detected by Kaspersky in 2024 are human-driven targeted attacks (APTs).

Source: Kaspersky Managed Detection and Response 2024 Analyst report

What does this mean for your cyberdefences?

A major danger of APTs and other targeted attacks is that even when they've been discovered and the immediate threat appears to have passed, the hackers may have left multiple backdoors, allowing them to return again whenever they choose.

Another problem is that many traditional cyberdefenses, such as antivirus and firewalls, generally can't protect against these types of attacks.

From the short summary above of the steps involved in mounting an APT or a targeted attack, it should be clear that defending against these threats requires a multi-level approach – incorporating solutions capable of protecting endpoints, networks, cloud, email, internet access and more.

Not only will this help to prevent and reduce the risk of sophisticated attacks – it will also help minimize the disruption and costs of these kinds of incidents should they occur.

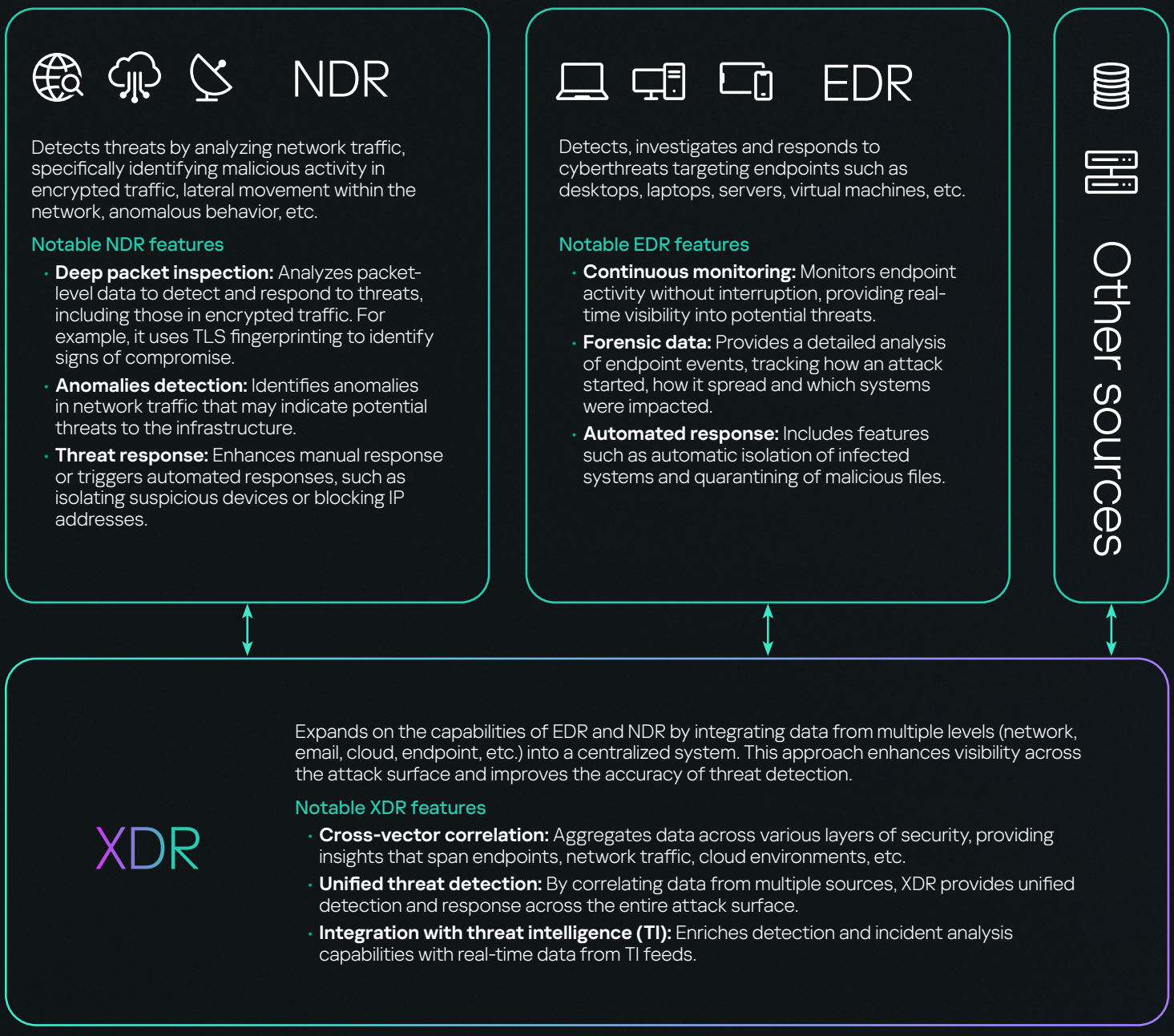
So what kinds of solutions does this involve and how should you be looking to deploy them?

How to protect enterprises against complex cyberattacks

While an endpoint protection platform (EPP) on its own won't protect against targeted attacks, it will provide a vital source of data to be used in the analysis of new, ongoing or historical attacks. As a result, it should be used as part of a suite of solutions that also includes:

- Endpoint detection and response (EDR) – Provides endpoint protection and visibility at the device level, identifies and responds to threats on workstations, servers, etc.
- Network detection and response (NDR) – Monitors and analyzes network traffic, detects anomalies and responds to potential threats at the network level.
- Extended detection and response (XDR) – Integrates EDR, NDR and other security layers to enhance visibility and automate threat response.

Figure 3: EDR, NDR, XDR: How does it work?



In 2024, the mean time to investigate and report high-severity incidents increased by 48%, indicating a rise in the average complexity of attacks compared to 2023. This is supported by the fact that the vast majority of triggered detection rules and IoAs were by specialized XDR tools, rather than OS logs as in previous years.

Source: Kaspersky Managed Detection and Response 2024 Analyst report

So which solution(s) should you choose?

Selecting the right solution(s) depends on your organization's specific needs, infrastructure and threat landscape:

- Choose EDR if traditional endpoint protection tools are no longer sufficient and you need more advanced protection against cyberthreats (such as malware, ransomware, phishing and more) targeting endpoints.
- Choose NDR if network-based threats are your primary concern and you need advanced capabilities to analyze and respond to network traffic anomalies.
- Choose XDR if you want comprehensive protection across multiple vectors and the ability to correlate threats across your entire IT infrastructure.
- Better still, combine EDR, NDR and XDR into a single security ecosystem to provide comprehensive defense against an extensive range of evasive and advanced cyberthreats.

Figure 4: EDR, NDR, XDR – who's it best for?

Cybersecurity solution	What organization is it best for?
EDR	• Organizations that prioritize endpoint protection and need real-time insights into endpoint activity. • Organizations with many distributed endpoints, such as financial institutions or healthcare providers, who will benefit greatly from EDR's ability to detect and respond to endpoint-based threats in real time.
NDR	• Organizations that rely heavily on network traffic and need advanced capabilities for detecting network-based threats. • Companies with a dedicated IT security team or highly regulated businesses such as data centers, service providers or government agencies, can benefit from NDR's ability to detect and respond to network-based threats.
XDR	• Organizations that require a unified security platform with comprehensive threat detection and response capabilities across their entire IT infrastructure. • Large organizations with complex IT environments that need a comprehensive approach to security. For example, a multinational enterprise with on-premises data centers and cloud environments would benefit from XDR's ability to provide unified threat detection across multiple platforms, while also reducing operational complexity by centralizing incident response.

Kaspersky Anti Targeted Attack

How Kaspersky can help

Kaspersky Anti Targeted Attack (KATA) delivers comprehensive anti-APT protection against complex cyberthreats. It helps organizations:

- Swiftly detect, analyze and respond to targeted attacks.
- Enable robust security across all key attack entry points, including networks, emails, the web and endpoints.
- Safeguard critical assets.
- Ensure compliance with industry regulations.

The above is made possible by leveraging the powerful NDR and EDR technologies available within the three tiers of Kaspersky Anti Targeted Attack.

The three KATA tiers offer protection against advanced persistent threats (APT) ranging from essential and advanced NDR to native XDR.

- KATA: Serves as an essential NDR solution and offers basic features to detect and respond to cyberthreats.
- KATA NDR Enhanced: Builds on the foundational features of the KATA tier, offering advanced NDR capabilities.
- KATA Ultra: Combines NDR and EDR capabilities to deliver native XDR functionality. It secures multiple threat entry points, including networks, web, email, endpoints, servers and virtual machines.

Figure 5: Kaspersky Anti Targeted Attack. A flexible choice.

Comparison criteria	KATA	KATA NDR Enhanced	KATA Ultra
Description	Essential NDR	Advanced NDR	NDR+EDR (Native XDR)
Essential NDR functionality	•	•	•
Advanced Sandboxing	•	•	•
Kaspersky Threat Intelligence and MITRE ATT&CK enrichment	•	•	•
Enhanced NDR functionality		•	•
Expert EDR functionality			•
Native XDR capabilities			•

Choose from essential or advanced level NDR functionality, or opt-in for the combined NDR and EDR solution for native XDR scenarios, safeguarding you against the most sophisticated cyberthreats – all in a single platform. At KATA Ultra tier, you get full-fledged, all-in-one APT protection and visibility across your entire IT infrastructure.

Why choose Kaspersky Anti Targeted Attack

Full visibility across your IT infrastructure

Provides a full stack of unique technologies to eliminate blind spots and control all potential threat entry points, including network, web, endpoints and email – all within a single unified platform.

Protection enriched by global threat intelligence

Enriches threat analysis and response through direct access to Kaspersky Private Security Network's global reputation database, Kaspersky Threat Intelligence and mapping to the MITRE ATT&CK framework.

Independently tested and proven technologies

Uses innovative technologies for advanced ML-driven threat detection, in-depth investigations and rapid incident response, which is recognized by leading analytical agencies and trusted by major clients worldwide.

Kaspersky Anti Targeted Attack

Learn more

Kaspersky Anti Targeted Attack video presentation

Watch now

The advanced threat predictions

Read now

www.kaspersky.com