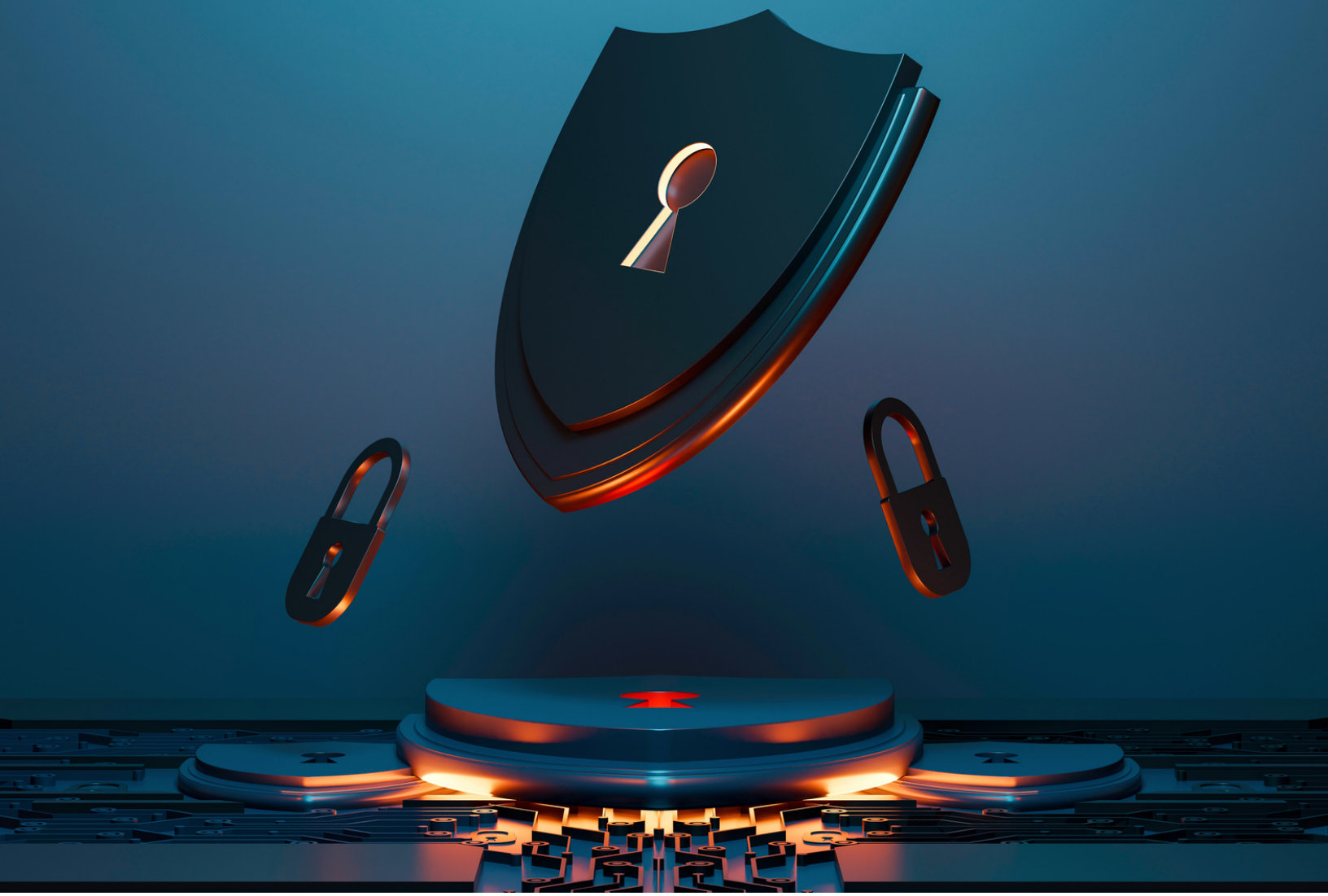
Outsmarting Generative AI Cyberattacks



The XDR Advantage

A new wave of AI-backed ransomware is upon us. Is your security ready? See why XDR is your best bet for future-proofing against emerging attack vectors.

eset® Digital Security
Progress. Protected.

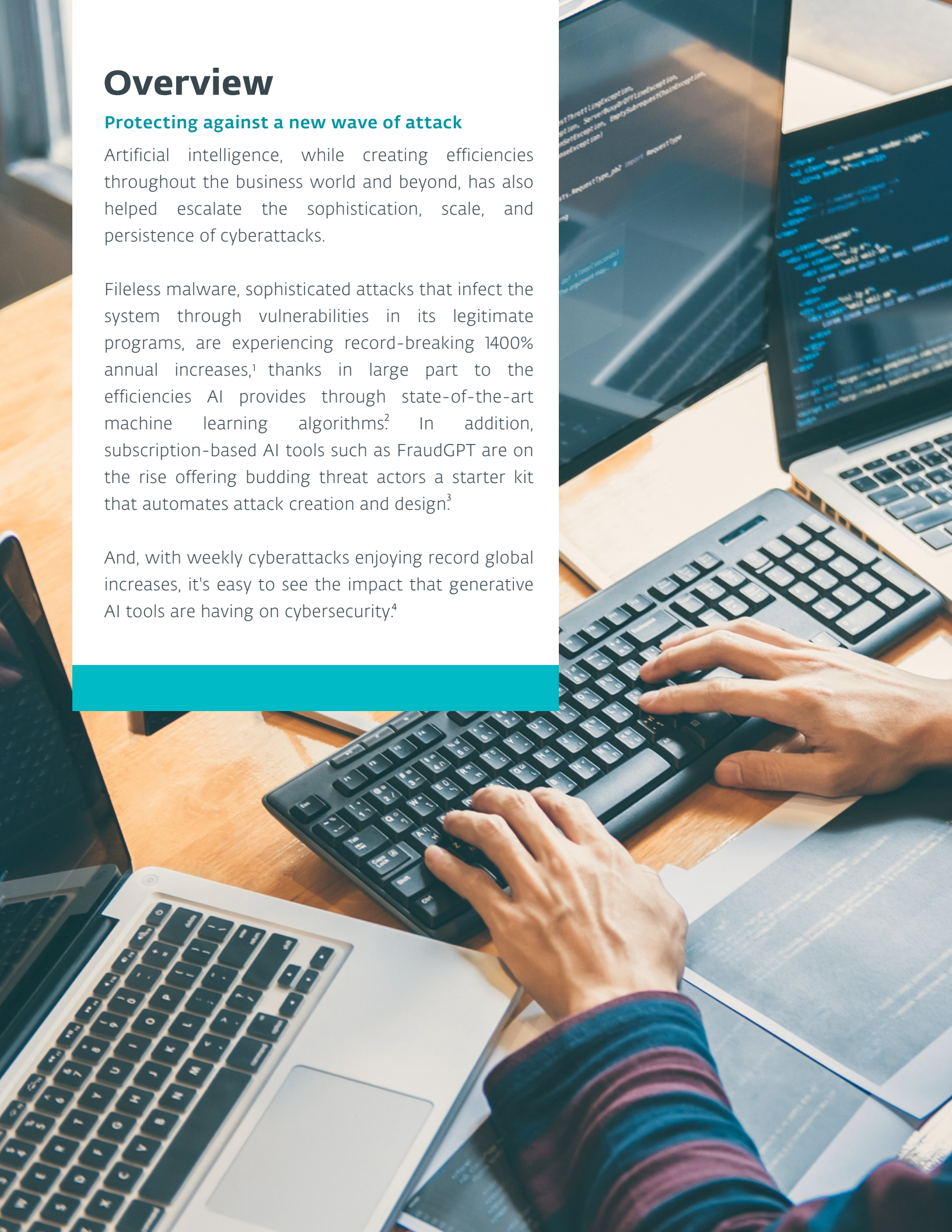
Overview

Protecting against a new wave of attack

Artificial intelligence, while creating efficiencies throughout the business world and beyond, has also helped escalate the sophistication, scale, and persistence of cyberattacks.

Fileless malware, sophisticated attacks that infect the system through vulnerabilities in its legitimate programs, are experiencing record-breaking 1400% annual increases,[1] thanks in large part to the efficiencies AI provides through state-of-the-art machine learning algorithms.[2] In addition, subscription-based AI tools such as FraudGPT are on the rise offering budding threat actors a starter kit that automates attack creation and design.[3]

And, with weekly cyberattacks enjoying record global increases, it's easy to see the impact that generative AI tools are having on cybersecurity.[4]



The Challenge

AI tools enable threat actors through a number of efficiencies including:

IMPROVED PHISHING SUCCESS RATES

Not only can AI accelerate the scale of attack through deployment automation but it helps attackers compose more credible-looking emails, websites, and social content to aid in the success rate. Typos and grammar, once telltale signs of phishing attempts, are now easily corrected on a mass scale with AI-powered content creation tools.

FASTER AND MORE EFFICIENT CODE CREATION

Cyberattacks are a numbers game for hackers and generative AI systems can produce fast and efficient code. Today's more sophisticated attacks utilize AI to write code that circumvents security controls including antivirus software, intrusion detection systems, and next-generation firewalls (NGFW).[5] Compounding the threat is the emergence of polymorphic code which uses built-in machine learning to mutate on deployment in order to evade detection.[6]

DATA MINING

AI tools can quickly mine publicly available data for information to aid in the attack including new vulnerabilities, exposed credentials, exploitable information on the target organization, and insight on how to launch sophisticated campaigns including vishing and deep fakes.

KEYSTROKE MONITORING

Groundbreaking AI systems are able to determine keystrokes through audio recordings with up to 95% accuracy rates.[7] Considering the ubiquity of microphones, cameras, and other audio recording devices that are connected to the network, this threat has the potential to negate basic password controls and identity.

Security Through Simplicity

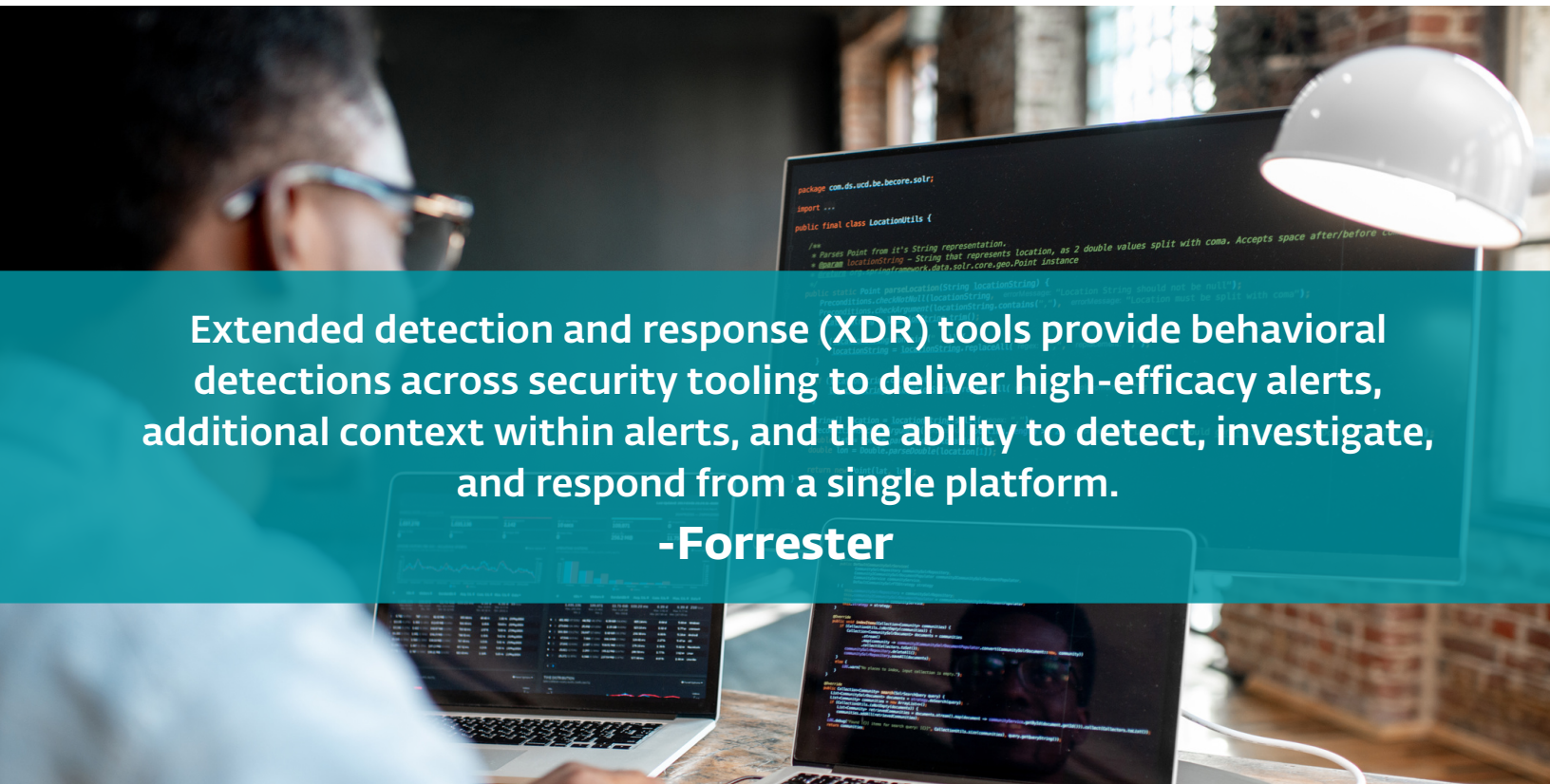
XDR offers a comprehensive view beyond the endpoint

A multi-layered security approach has been long touted as the best practice to protect against cyber threats. With the understanding that there is no cybersecurity "silver bullet," organizations have adopted various solutions, each with its own security specialty and focus area, to ward off intrusions.

However, understanding the full scale of an attack meant aggregating information from these systems to show the full picture which is a challenge as most of them existed in silos, especially when sourced from a number of security vendors. As organizations grow in scale, even systems such as information and event management systems (SIEM) struggle to provide the context necessary to sift through the noise and adequately respond.

XDR (Extended detection and response) was born out of this challenge. XDR solutions correlate threat data from traditionally siloed systems including endpoints, network analysis and visibility (NAV), email, cloud workload, and others to provide a holistic overview of the entire technology stack. SOC teams, heavily burdened with the task of interpreting events, are now empowered with deeper intelligence of threats that they can leverage for faster incident response, more acute threat hunting, and insight for improved detection.

XDR embodies the future of cybersecurity on multiple fronts, serving as a formidable response to the escalating sophistication of threat actors and their evolving toolkit.



Extended detection and response (XDR) tools provide behavioral detections across security tooling to deliver high-efficacy alerts, additional context within alerts, and the ability to detect, investigate, and respond from a single platform.

-Forrester

Native XDR: Streamlined Intelligence

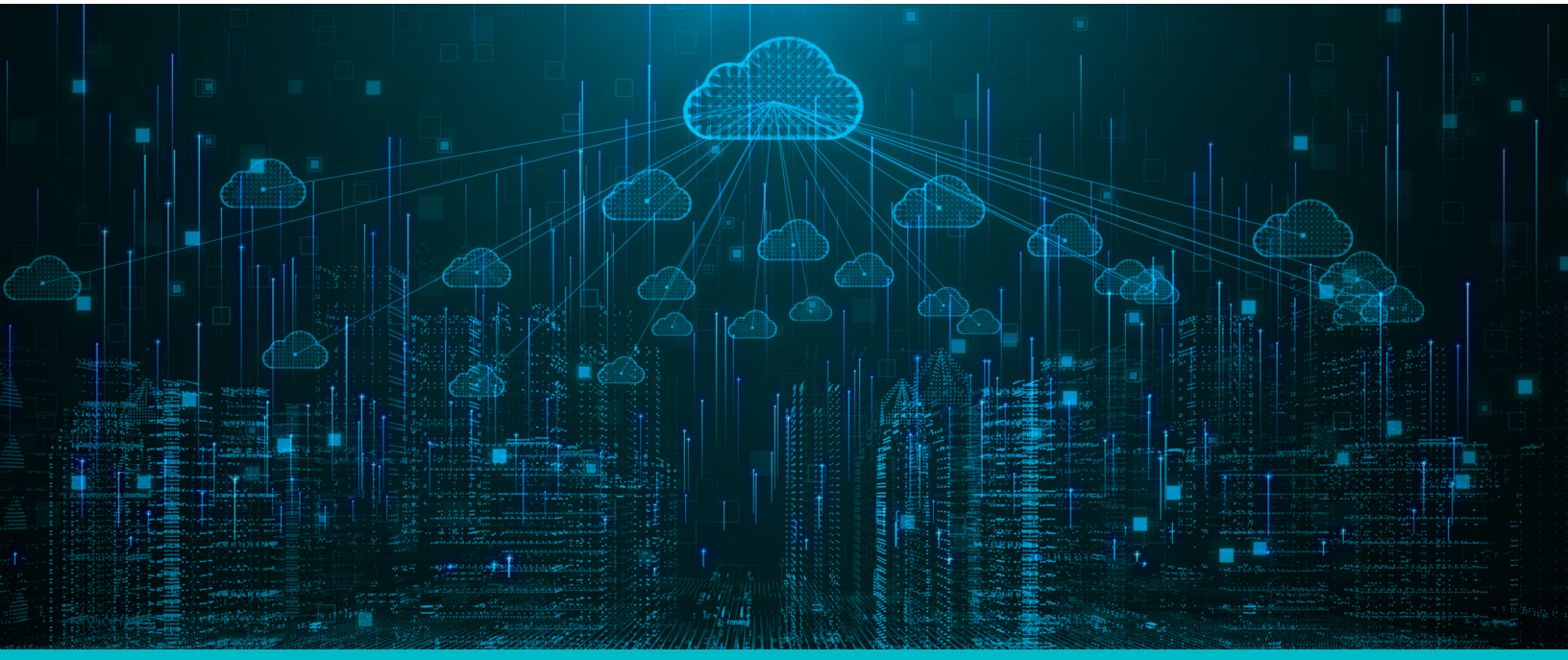
There are generally two types of XDR strategies: open (or hybrid) XDR which integrates telemetry from various third-party vendors via API, and native XDR which utilizes security tools from a single vendor. While there are pros and cons to both, a native XDR approach offers ease of deployment and management and streamlined intelligence from all areas of the security ecosystem. Where API integrations can cause complexity that increases the potential for false positives, integration failures, and misconfigurations, native XDR is becoming a popular strategy to avoid complications.

Consolidation is Key

Security consolidation is a growing trend among CISOs looking to streamline their security posture to relieve alert fatigue, control agent sprawl, and fill vulnerability gaps caused by misconfiguration, patch management, and training. Recent surveys show that 96% of CISOs plan to consolidate and 63% listed XDR as their strategy to do so. In fact, Gartner recently predicted that native XDR strategies will be used by 40% of enterprises by the end of 2027 to reduce the number of security vendors they have in place.[8]

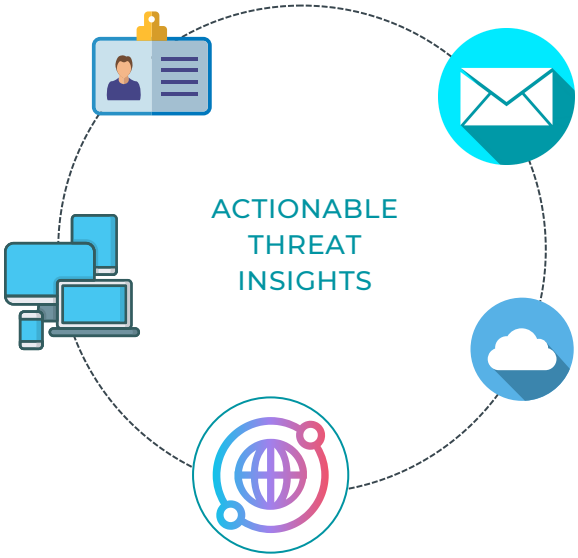
63%

OF CISOS LISTED XDR AS THEIR CONSOLIDATION STRATEGY



4 Ways XDR Outsmarts Generative AI Tools

1 Removes Hiding Spots



XDR is made stronger with the more intelligent inputs feeding it. Aggregating threat data across all areas of the technology stack from network to email to cloud to endpoint means that malware has fewer places to hide. Real-time telemetry shows actionable insights across the entire ecosystem exposing intrusion points and suspicious behavior even where systems overlap with each other. Native XDR solutions from a trusted security expert offer a streamlined approach to ensure a multi-layered security posture that works seamlessly together, providing actionable insight from one convenient platform.

2 Measurable Reduction in Time-to-Detect and Time-to-Remediate

Time is one of the most crucial assets in the fight against cyberattacks. Early detection is crucial to threat remediation yet on average it can take over 200 days to detect a security incident and another 75 to contain. These numbers are increasing with the proliferation of fileless malware and Living off the Land (LOTL) attacks in which native, legitimate system tools are hijacked to advance the attack.

XDR is the organization's best bet to reduce both time-to-detect and time-to-remediate. A built-in automatic incident creator vastly reduces the amount of time spent analyzing all data collected by XDR. This key feature automatically records attack behaviors in the incident report to focus admin efforts in time of need.

3 Enables Threat Hunting

Fileless attacks are extremely challenging to detect using traditional AV scanning techniques. Intelligent threat hunting is the crucial antidote. Leveraging the comprehensive view of the entire technology ecosystem offered by the XDR platform, threat hunters seek out subtle irregularities to uncover intrusions within seemingly innocuous interactions.

XDR streamlines the process, allowing security teams to effortlessly search for threats without the need for intricate query construction. In addition, XDR platforms that are powered by AI aggregate the security telemetry and continuously monitor activity to find and alert on these sophisticated attacks.

Leave it to the Experts

Managed Detection and Response (MDR) is becoming a popular choice for companies of all sizes. This add-on service provides continuous monitoring of security telemetry by a team of experts to hunt the most sophisticated attacks.

4 Advanced Threat Intelligence

XDR systems offer deep knowledge of how attacks move throughout the network and how threats, on the whole, are evolving. This knowledge can be used to identify and fill existing security gaps and to build an improved playbook for faster detection and response. Taken one step further, XDR platforms that are backed by and combined with a vendor's global intelligence feed build an even greater advantage. Bolstered by a team of security experts with a global view of emerging threats, XDR platforms become more effective and provide deeper context.

REFERENCES Help Net Security | MDPI | VentureBeat | Infosecurity Magazine | Dark Reading | Cyberark | Analytics Vidhya | VentureBeat | Security Intelligence

QUOTE Forrester: The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q3 2023. Heath Mullins, Andras Cser, Jess Burn, Allie Mellen, Jeff Pollard, Brian Wrozek with Joseph Blankenship, Alexis Tatro, Michael Belden. July 21, 2023

Empowering Security

As threat sophistication increases the need for visibility into all areas of the organization, XDR empowers security teams to quickly and effectively identify anomalous behavior and breaches. It provides advanced threat hunting, risk assessment, incident response, and investigation and remediation capabilities.

Native XDR solutions offer a simplified path to security consolidation to reduce alert fatigue, agent sprawl, and integration vulnerabilities. The power of XDR can be further extended through optional MDR services and global intelligence feeds for actionable insight into the toughest threats.

About ESET

WHEN TECHNOLOGY ENABLES PROGRESS,
ESET IS HERE TO PROTECT IT.

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

CONTACT US

ESET North America
1 (844) 824-3738
www.eset.com

Digital Security
Progress. Protected.