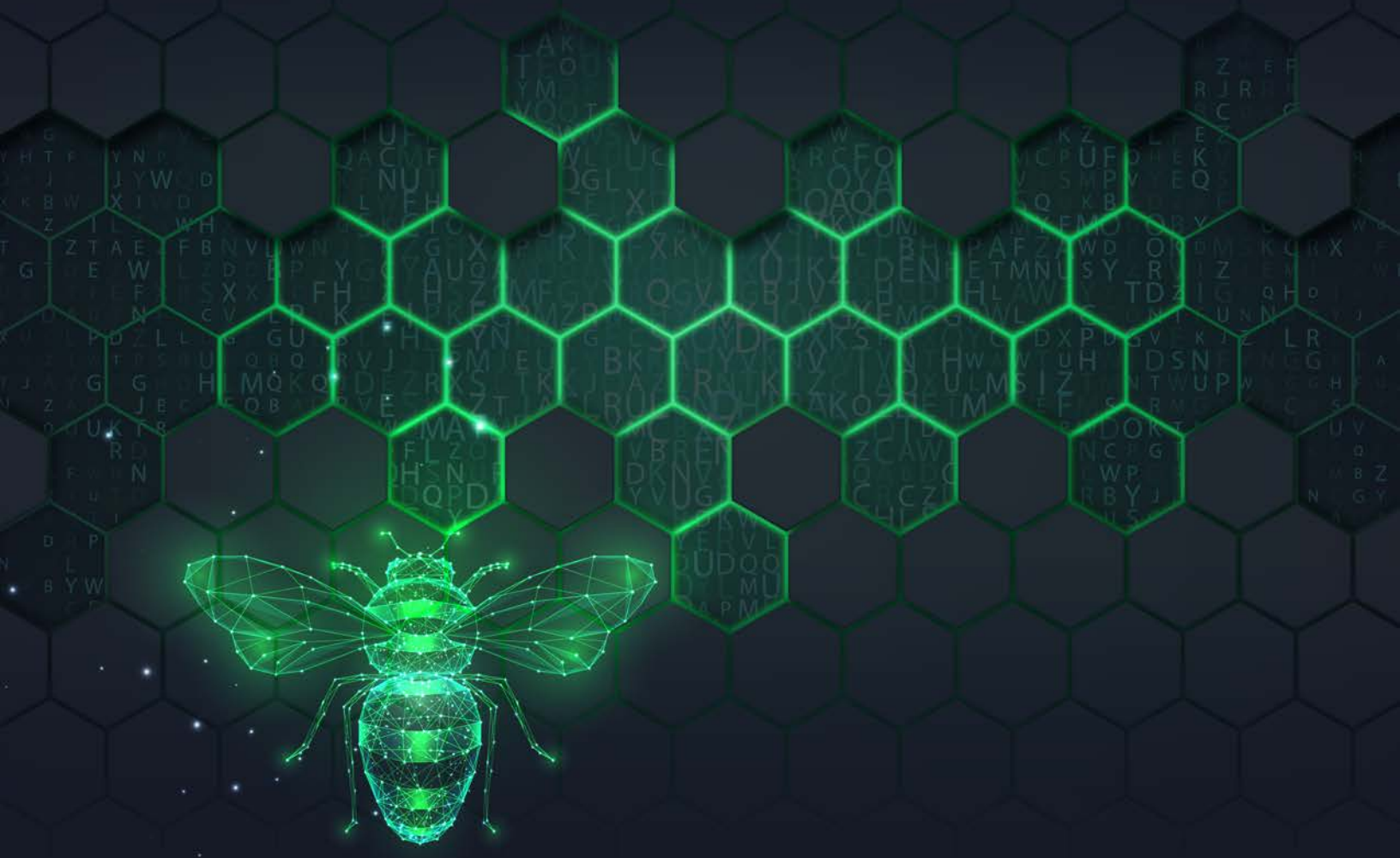
Understanding XDR

Beyond the Buzzwords



Netsurion®

Content

Are Current Cybersecurity Stacks Effective?

With the recent shift in the threat landscape, companies need to take a more proactive approach to cybersecurity. Legacy SIEM solutions are falling out of favor and open platforms that can bring a modern, AI-driven security analytics capability to the data generated by their existing tools are in demand.

Customers have turned to advanced threat detection, prevention and response tools that make better use of their existing security technology stack and allow for proactive approaches to cybersecurity including threat hunting, deep machine learning and automated threat response. This new technology has been labeled Extended Detection and Response (XDR). However, this also increases the complexity of the task at hand – first because the sophistication of the threats themselves, and second because this requires highly skilled and capable human cybersecurity resources to make use of XDR platforms.

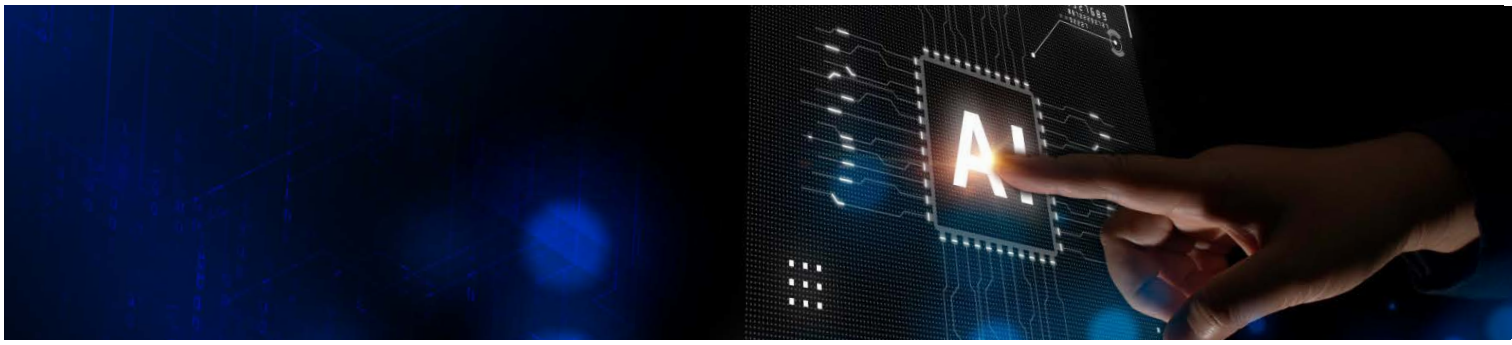
Managed detection and response (MDR) providers can make more effective use of XDR platforms for their customers by offering an MDR service in a fully managed or co-managed fashion. Smaller organizations without the budget or skilled personnel have the option to off-load their security operations fully or partially to a professional and highly capable security team that can act as an extension of their own team. Netsurion's MDR service combines a cutting-edge security platform with a 24x7 Security Operations Center (SOC) team for the ultimate protection against sophisticated, never-seen-before cybersecurity threats.

This whitepaper provides the information needed by security managers to understand what the critical components of an effective XDR platform are. It also dives into why it makes sense for small and mid-size companies to adopt an MDR service like Netsurion instead of trying to operationalize a SOC themselves.

What is XDR and Where Did It Come From?

Extended Detection and Response (XDR) is a security solution that provides comprehensive visibility, threat detection, analysis, and highly automated response across all your cloud, hybrid, and on-premises data center resources. XDR tools create a unified security analysis environment across all the different security tools an organization has deployed. Open XDR solutions also support an open standard by being able to accommodate and use security telemetry from disparate vendors, unifying the signals and streamlining response operations. The benefits of modern XDR solutions fall into three major categories, including AI-driven correlation at scale, improving operational efficiency, and addressing skills gaps.

Thwart Advanced Threats with Machine Learning



Threat actors today have become extremely sophisticated and are operating as for-profit businesses. They are continuously testing against the most widely deployed security defense tools to bypass existing security solutions in place. This results in more sophisticated and targeted attacks, multi-stage attacks, ransomware, polymorphic malware, social engineering, phishing, and file-less malware reaching unsuspecting users.

In the face of these threats, XDR platforms are replacing Security Information and Event Management (SIEM) correlation by bringing modern AI-driven threat detection, big-data repositories, and streaming analytics to the cybersecurity arena. The amount of data generated by IT environments has grown by orders of magnitude, and the compute and analytics power required to effectively analyze this data has increased at the same rate. XDR solutions can pull together and make sense of Endpoint Protection, Host-based Intrusion Detection, User & Entity Behavior Analytics (UEBA), and several other sources of data deployed for security alerting across the enterprise today.

Eliminate Noise and Alert Fatigue

One of the biggest challenges in cybersecurity today is being able to efficiently identify and respond to crucial security alerts generated by the plethora of tools deployed, and to be able to separate the important alerts from the irrelevant noise. Network sensors create numerous alerts – false positives – that must be analyzed before being deemed low priority. Incident response teams struggle to selectively pick what alert they will address and what they will ignore. Occasionally the decision is the wrong one, resulting in a headline-worthy data breach.

This is where XDR can help. Because they are leveraging advanced detection and prioritization techniques that can be applied across vast amounts of incoming data in real time, XDR platforms can help identify the important incidents that a security analyst must look at immediately. This helps prevent alert fatigue and results in a lower probability that an important cybersecurity incident will be missed or overlooked.

Close the Cybersecurity Skills Gap

Many organizations have, or are considering building a security operations capability by deploying a SIEM solution. However, standing up a Security Operations Center (SOC) is very expensive and requires specialized skills to maximize the value of technology with malware analysis, forensics, security analytics, etc. These skill sets are not always readily available and can't be easily trained because cyber skills cover a wide range of disciplines. They are also expensive and in high demand, which means that not every organization can afford to have in-house staff that can really get the best results from these Endpoint Detection and Response (EDR) tools. Endpoint Protection and Application Control are crucial to XDR to because over 70 percent of data breaches occur through compromised endpoints. Some organizations have built out incident response or security operations teams but don't have the budget to staff these beyond standard work hours and workdays.

Critical Components of an Effective XDR Platform

Security Information and Event Management (SIEM)

While the cybersecurity rhetoric would have you believe "SIEM is Dead", a SIEM solution continues to be a foundational component of a broader XDR platform. SIEM solutions collect, standardize, and store the disparate data that XDR needs to perform correlation. This includes log data, but also network, user, and cloud events. Recently, SIEM solutions have been tasked to provide the dashboarding and reporting needs of the SOC and for demonstrating compliance with regulatory mandates. In modern security programs, SIEM is largely now being deployed as a Software-as-a-Service (SaaS) rather than the heavy lift on-premises model of the past. And modern SIEMs are using big data technologies to handle the volume of data today.

Vulnerability Management

Vulnerability management and assessment scans are needed to continuously track the attack surface and ensure that the infrastructure, systems, and software applications running business operations are not exposed to cyber criminals. This capability is usually resource intensive, occupying a lot of time from security analysts because vulnerability scans tend to throw off a very large number of alerts, most of which are not relevant. Effective vulnerability management solutions can apply several layers of context to weed out irrelevant alerts and prioritize the small number of true, high-impact areas of risk in the organization's IT environment.

Endpoint (Threat) Detection and Response

EDR and EPP are crucial sources of information for XDR because over 70 percent of data breaches occur through compromised endpoints. These include desktops, servers, laptops, and more recently, mobile devices. Zero-day threats, APTs, ransomware and other nefarious vectors all reside on the endpoint. The endpoint protection component needs to be proactive and predict the incidence of file-based, file-less, and polymorphic malicious software. Over the last few years, deep machine learning and AI-based detection have emerged to protect against sophisticated endpoint threats.

Host-based Intrusion Detection

Managed IDS capability from Netsurion provides an early warning regarding attackers attempting to access your systems and sensitive data. Our SOC continuously tunes and configures the Host-based IDS (HIDS) capability and then prioritizes alerts for your further investigation. There is no expensive hardware or software to install or manage. Accelerate your cybersecurity and threat visibility with a managed IDS capability that provides single-pane-of-glass coverage.

Threat Intelligence

Threat intelligence is contextual data that helps the security analyst understand a threat actor's motives, targets, techniques, and attack patterns. The AI-driven analysis of security events with this contextual threat intelligence enables SOC teams to make faster, better-informed decisions that are backed by data and ultimately move the security team's behavior from reactive to proactive when battling malicious threats actors.

Threat Hunting

Threat hunting is a proactive security search across company resources including cloud assets, endpoints, networks, and user accounts to complement threat detection and uncover threats such as APTs and multi-stage attacks. This approach is gaining traction as a security technique but is still a largely manual exercise requiring specialized knowledge and skills. Security teams systematically perform threat hunting by aligning with the MITRE ATT&CK® Adversarial Tactics and Techniques framework to organize their effort. Because it requires a specialized skill set and could be time consuming, many organizations, especially smaller companies with limited resources, are unable to develop proactive threat hunting on their own.

Automated Response and Guided Remediation

As can be imagined, effective automated response is a core capability of any XDR platform. In fact, the highly automated response capability is largely responsible for delivering the benefits described earlier – removing inefficiencies in the security process and overcoming cybersecurity budget and staffing hurdles. Automated response to security incidents involves performing a routine set of tasks (like data collection, isolation, and alerting) by following a set script, thereby reducing the Mean Time to Recovery (MTTR) and eliminating human error. After the mundane activities are completed, skilled security staff can then step in and perform the higher order security analysis and remediation tasks to mitigate any adverse effects of the cyber incident.

Bring in “Managed” to Reduce Complexity and Cost

Managed Detection and Response (MDR) is a managed cybersecurity service backed by various technologies and a modern SIEM, EDR, or XDR platform to provide a range of threat detection and response capabilities to mitigate damage caused by cyber attacks that evade prevention controls. The layers of technology employed, and vigilance and expertise of the staff, determine how truly effective an MDR provider can be. For small-to-medium-sized businesses (SMBs), combining the technology spend of a security platform and an MDR service results in a dramatic reduction in the overall complexity and cost of their security program.

This is where Netsurion Managed Threat Protection comes in to provide a fully functional SOC-as-a-Service MDR solution that combines the critical components of XDR with a highly skilled team of security analysts. Netsurion Managed Threat Protection elegantly combines and balances the people-process-technology triad to elevate your security posture to predict, prevent, detect, and respond to security threats across your entire IT environment. Netsurion MDR, coupled with SOC-as-a-Service, makes sophisticated 24x7 security monitoring a reality.

Predict

Anticipate cyber incidents via actionable threat intelligence

Prevent

Block malicious activity before damage is done

Detect

Identify suspicious activity via continuous monitoring

Respond

Rapidly contain the impact and resume operations

Explore Netsurion's Managed Open XDR platform

It is no longer an option for companies to take a passive-reactive approach to cybersecurity. Enterprises of all sizes are ripe targets for hackers because they have smaller budgets and are unable to invest in the latest security defenses – technology or staff.

The combination of a sophisticated threat detection and response platform with a 24x7 highly skilled SOC staff is an extremely attractive option for many organizations. Gaining improved protection, visibility, and incident response capabilities without adding more headcount and tools allows companies to utilize their limited capital and resources better and focus on their core business.

Netsurion Managed Open XDR platform brings together several crucial components of effective cybersecurity. Delivered as a managed service leveraging the latest security technologies, Netsurion's customers can extend their security teams, enhance threat detection and response, improve forensic investigations and compliance reporting, all while reducing their cybersecurity spend.

A Market Leader in Cybersecurity

Netsurion has delivered consistent managed cybersecurity leadership for over 10 years. In third-party evaluations, Netsurion receives high marks for both its XDR platform and its SOC service. Netsurion Managed XDR has been recognized by industry analysts and media as a top solution in MDR, XDR, and SOC-as-a-Service.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's Managed Detection and Response includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.


Netsurion®