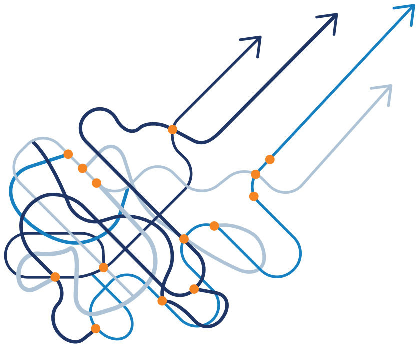
DYOPATH
Driving Your Organization's
PATH to IT Success

Guide Sheet: Advanced Security Services

At DYOPATH we work with the single purpose of helping our clients combat the ongoing increase of cyber threats, the growth in more complex IT environments, and the ever-increasing human capital shortages.



SIEM vs. EDR vs. MDR vs. XDR

Cyber threats are evolving faster and have become more malicious than ever. And now that "distributed workforce" has become the prevailing business model around the globe, organizations must do whatever it takes to defend their expanding networks. Few organizations have the expertise, experience, tools, and resources to manage and maintain an expensive Security Information & Event Management (SIEM) platform or to build their own Security Operations Center (SOC) capable of expert investigation and lightning-fast incident response around the clock.

As one of the largest privately held Managed Security Service Providers (MSSP's) in the country, DYOPATH employs the latest, most cutting-edge security orchestration technology available, powered by our best-in-class 24x7x365 SOC comprised of highly certified security analysts with a broad range of cyber expertise. DYOPATH's SOC-as-a-Service can be fully managed or co-managed with your IT personnel to give you peace of mind and "always on" 360-degree expert protection.

By monitoring every "event source" across your network, DYOPATH is able to identify and respond to threats and suspicious activity in real time, instantaneously extinguishing any risk of attack and/or breach of sensitive data such as medical records or payment information.

DYOPATH
Driving Your Organization's
PATH to IT Success

Mitigating Threats: SIEM vs. EDR vs. MDR vs. XDR

Security Incident & Event Management (SIEM)

SIEM solutions offer organizations the ability to collect, aggregate, analyze, and store logs of network traffic and event data derived from multiple sources, including network devices, endpoint security software, and intrusion prevention systems. However, unless your organization possesses the appropriate level of inhouse security expertise, SIEM solutions should never be self-managed. Rather, organizations should partner with an MSSP who understands every facet of cybersecurity, religiously adhering to the five pillars of the prevailing NIST framework: Identify, Protect, Detect, Respond & Recover.

Endpoint Threat Detection & Response (EDR)

Similar to SIEM in its purpose, EDR is an automated software designed to analyze data and identify threats. Installed on network endpoints (devices), EDR software collects and sends behavioral information to central databases to be analyzed in a relatively limited capacity.

Managed Detection & Response (MDR)

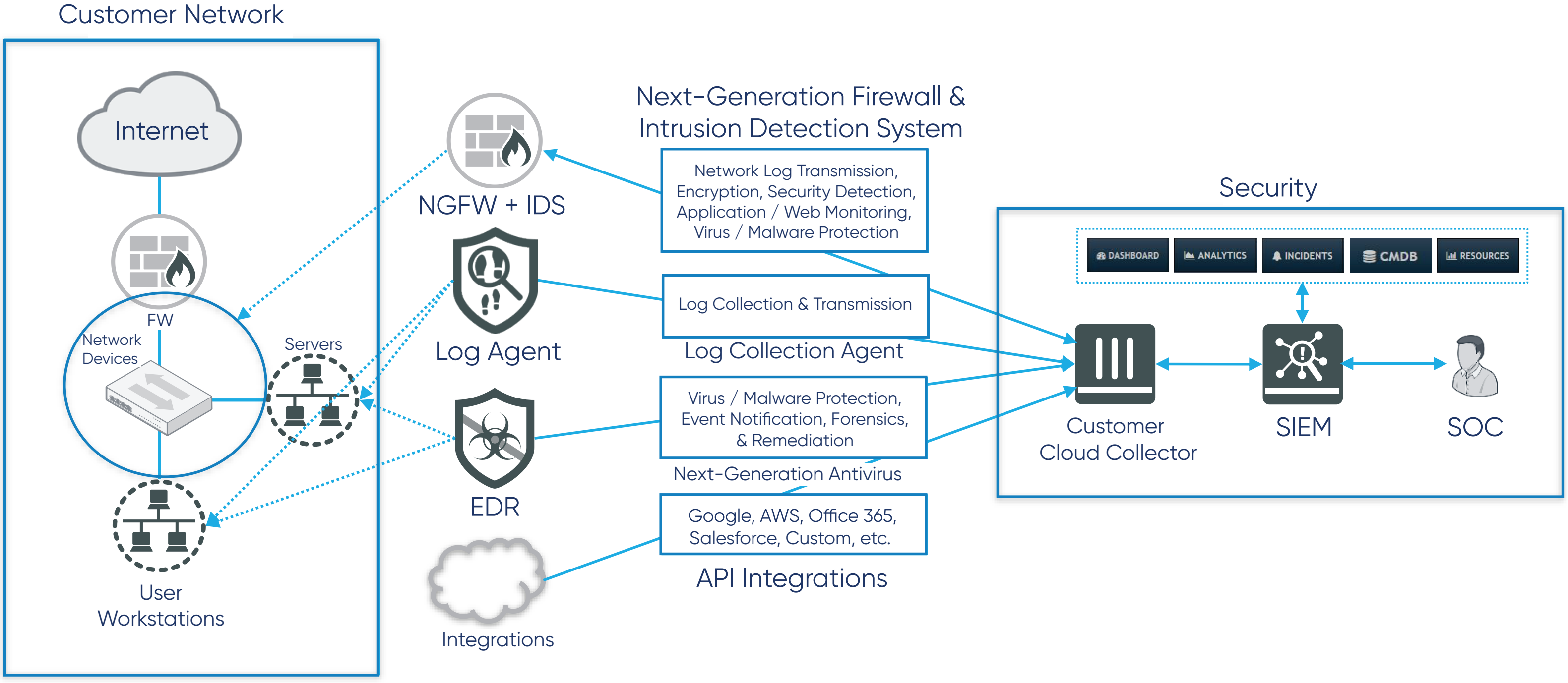
While the purpose of EDR is to detect and remediate threats, it requires the installation of sensors on endpoints to automate the detection & response process for further investigation. Unlike EDR, MDR is a 24x7 monitored cybersecurity service with actual staff on hand to detect, manage and remediate threats.

Extended Detection & Response (XDR)

Whereas EDR and MDR focus primarily on protecting endpoints, providing in-depth visibility and threat prevention for specific devices, XDR provides a much wider view, integrating security not just across endpoints, but across the entire network, cloud computing/workloads, email, and a multitude of other applications and solutions. XDR is a cross-layered detection & response process which includes the collection and automatic correlation of data across multiple security layers so security analysts can detect and respond to threats more quickly and efficiently.

DYOPATH XDR TOPOLOGY

DYOPATH
Driving Your Organization's
PATH to IT Success



Customer Network

Internet

FW

Network Devices

Servers

User Workstations

NGFW + IDS

Log Agent

EDR

Integrations

Next-Generation Firewall & Intrusion Detection System

Network Log Transmission, Encryption, Security Detection, Application / Web Monitoring, Virus / Malware Protection

Log Collection & Transmission

Log Collection Agent

Virus / Malware Protection, Event Notification, Forensics, & Remediation

Next-Generation Antivirus

Google, AWS, Office 365, Salesforce, Custom, etc.

API Integrations

Security

DASHBOARD | ANALYTICS | INCIDENTS | CMDB | RESOURCES

Customer Cloud Collector

SIEM

SOC

DYOPATH: Redefine Your SOC

Regardless of your organization's current security posture, there is one thing every IT professional must recognize: the cyber landscape is never static; rather, it continually evolves, creating new doorways for cybercriminals to infiltrate your company's network so they can seize upon your invaluable data by any means necessary.

Security Operations Centers must be adaptable and amenable to continuous improvement. From managing endpoints to investigating droves of "false positives" in real time to vulnerability scanning and advising on the latest updates and patches to triaging incidents to researching and mitigating threats and writing incident reports— the processes inherent to effective Security Operations will continue to grow and progress in proportion to the skyrocketing demands of today's threat landscape.

With IT departments lacking the personnel, time, and financial resources to build and maintain their own internal Security Operations Center, it is no wonder businesses around the globe continue to turn to DYOPATH; because we know that Security is a journey -- not a destination.

Contact DYOPATH Today for Your Advanced Security Questions

1.866.609.PATH

Texas Office:
13430 Northwest Fwy,
Suite 1000
Houston, TX, 77040

Illinois Office:
905 Parkview Blvd
Lombard, IL 60148

solutions@dyopath.com