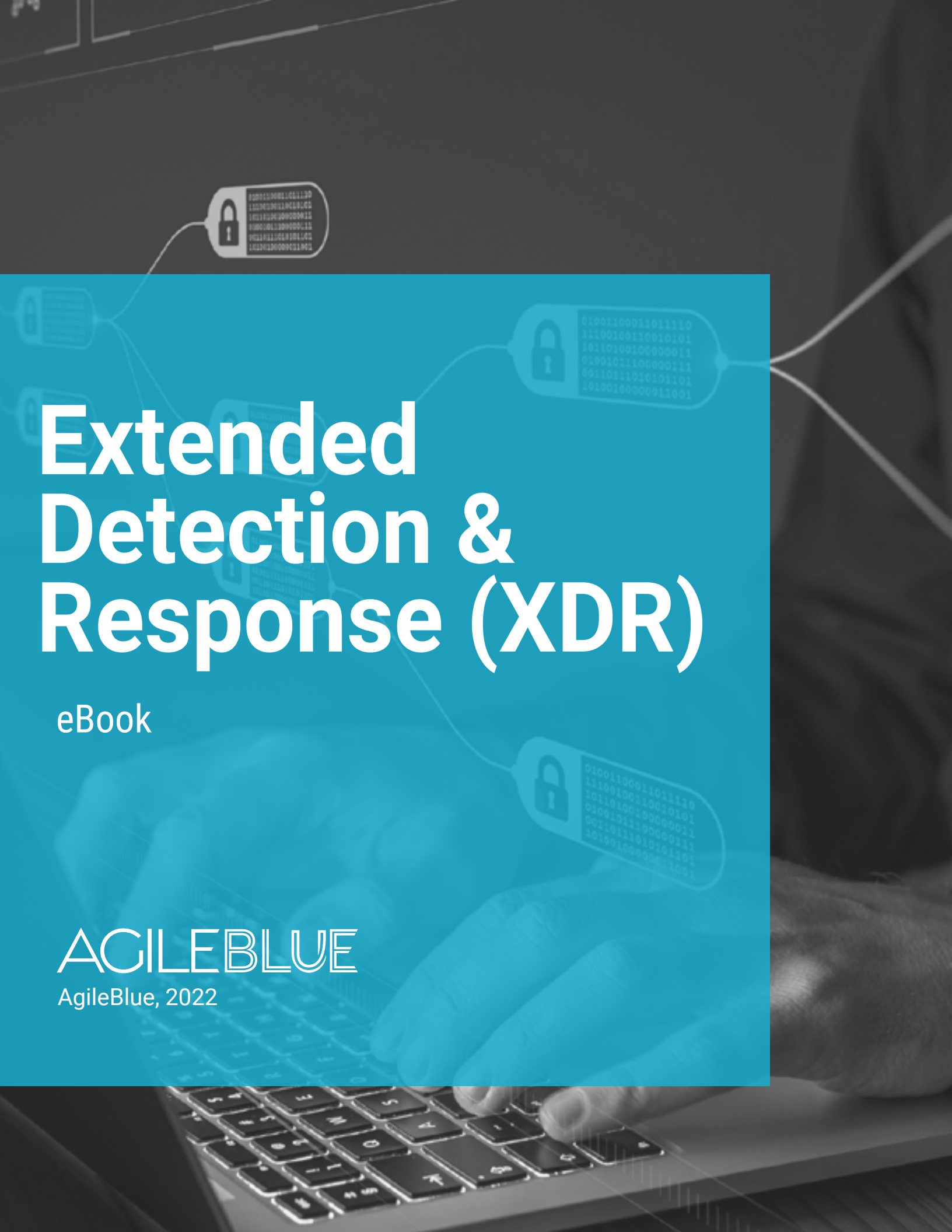


Extended Detection & Response (XDR)

eBook

AGILEBLUE

AgileBlue, 2022

WHAT IS EXTENDED DETECTION & RESPONSE?

The cybersecurity industry is known to create terms or other acronyms that rise and crash before it is truly understood. With solutions providers improving upon existing solutions, creating new concepts and methodologies for securing companies' infrastructures, it can be confusing to know which services are complementary verses which ones are redundant.

Terms for similar security solutions like MDR, EDR, and XDR leave organization leaders puzzled when addressing security issues. Knowing what separates one solution from another could ultimately save your company money, time, and risk.

EXTENDED DETECTION AND RESPONSE (XDR)

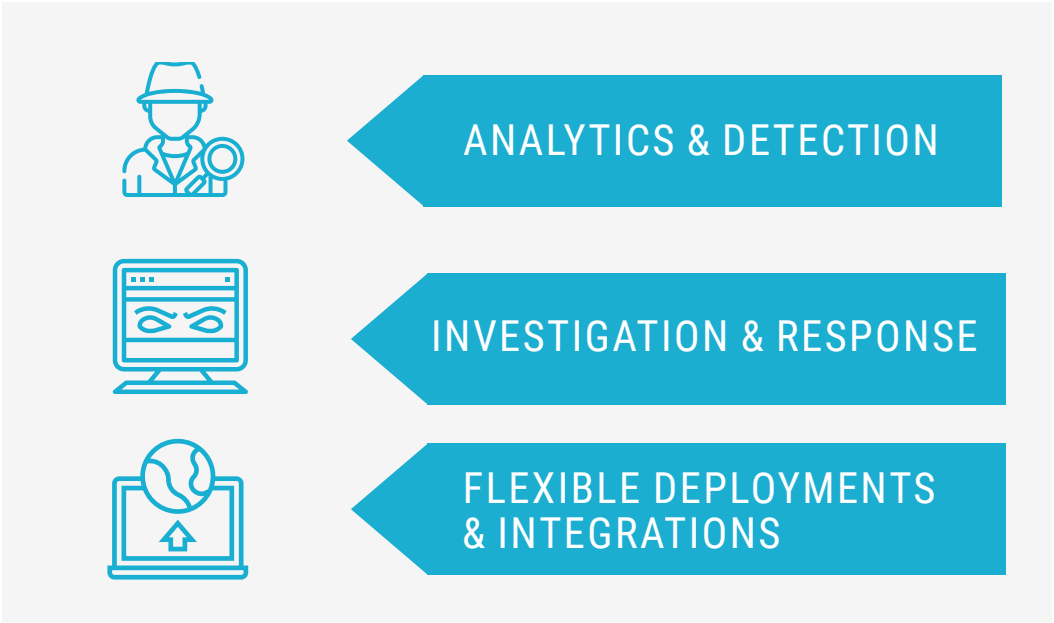
Extended Detection and Response (XDR) is a SaaS-based, vendor-specific, customizable security solution that performs monitoring, detection, and response that integrates multiple security products into a cohesive security operations system (SOC).

XDR is the evolution of end-point detection and response (EDR) and network traffic analysis (NTA). EDR, created to provide perimeter-wide protection for systems, was an advancement on existing solutions as it provided coverage for a primary component in an attack: endpoints. NTA, created to monitor network activity to identify potentially malicious behavior and improve visibility across the environment.

XDR offers visibility to potential vulnerabilities, reduced detection and response times to real-time threats, and integration of several security products into a unified securityoperations system that enables security teams and organizations to work more efficiently.

HOW DOES IT WORK?

Extended Detection and Response (XDR) solutions are designed to provide security teams with capabilities including:

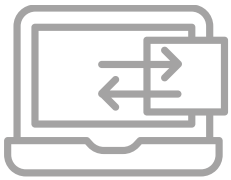


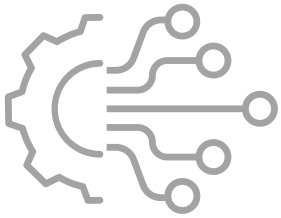
ANALYTICS & DETECTION

XDR solutions rely on a wide range of analytics for threat detection. Below are some of the analytical features you should expect to be included:

Analysis of Internal & External Traffic

Ensures that malicious insiders and compromised credentials are detected, as well as, identifying external attacks.





Integrated Threat Intelligence

Threat intelligence enables XDR to learn from attacks on other systems and use that information to detect similar events in your network.

Machine Learning Based Detection

Machine learning technologies enable XDR to detect zero-day threats and nontraditional threats that can omit standard methods.

INVESTIGATION & RESPONSE

Another important component of XDR is to provide SOCs the ability to investigate and respond to incidents from the same security platform. Instead of keeping logs in a separate silo, XDR logs can be used to initiate immediate response actions with higher confidence and greater depth of knowledge surrounding an escalation. For example, the typical SIEM approach is centered around monitoring network log data for threats and responding on the network through another security technology platform.

Once suspicious events are detected, XDR can provide tools that help security teams determine the severity of a threat and respond accordingly. Below are some of the features included in XDR that can assist with investigation and response:

Correlation of Related Alerts & Data

tools can automatically group related alerts, build attack timelines from activity logs, and prioritize events. This helps determine the root cause of an attack and can help them predict what an attacker might do next.

Centralized User Interface (UI)

enables analysts to investigate and respond to events from the same console. This helps speed up response time and makes management of responses simpler.

Response Orchestration Capabilities

enables response actions directly through XDR interfaces. For example, XDR can update endpoint policies across the enterprise, in response to an automatically blocked attack on a single endpoint.

FLEXIBLE DEPLOYMENTS & INTEGRATIONS

XDR solutions are designed to centralize threat tooling and gain greater control over security. Flexible deployments allows this to happen, meaning that more than one set of security tools can be deployed when necessary. Below are some of the features that improve control of security:

Security Orchestration

Is the ability to integrate with and leverage existing controls for unified and standard responses.

Flexible Deployments

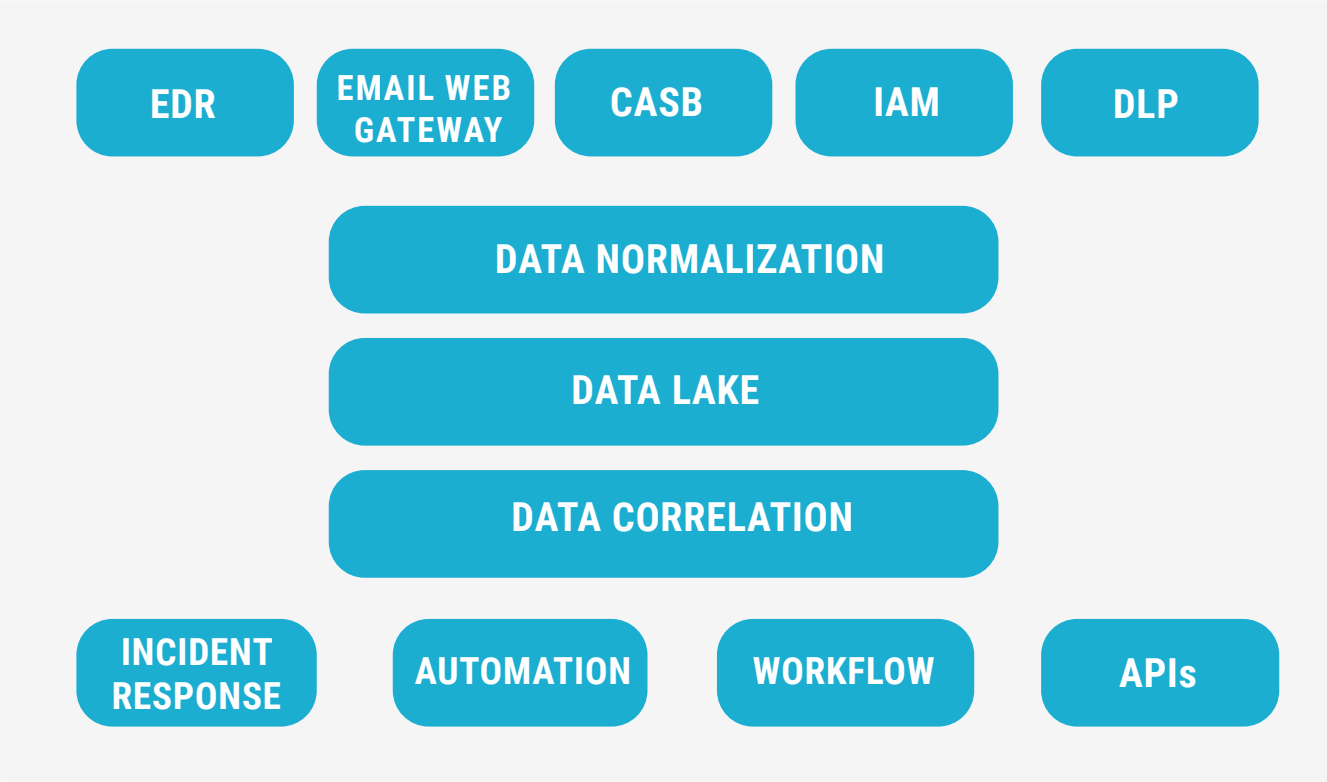
XDR solutions can also include automation features to help ensure that policies and tooling are deployed consistently.

Proactiveness

XDR uses machine learning capabilities to predict malicious behavior before it happens. Rather than EDR solutions that are designed to be reactive.

XDR evolved from standalone tools which offer limited visibility:
- EDR is strictly at the end-point.
- NTA is strictly at the network layer.
- Layer specific tools = more alerts, more effort.

XDR CONCEPTUAL ARCHITECTURE



Source: Gartner
ID: 466211_C

XDR solutions improve protection capability by:

1. Sharing local threat intelligence among security products, enhancing machine learning of threats across all components. Also, leveraging externally acquired threat intelligence in multiple different detection methods including the network and endpoint.

2. Combining weak signals from multiple components into stronger signals of malicious intent.

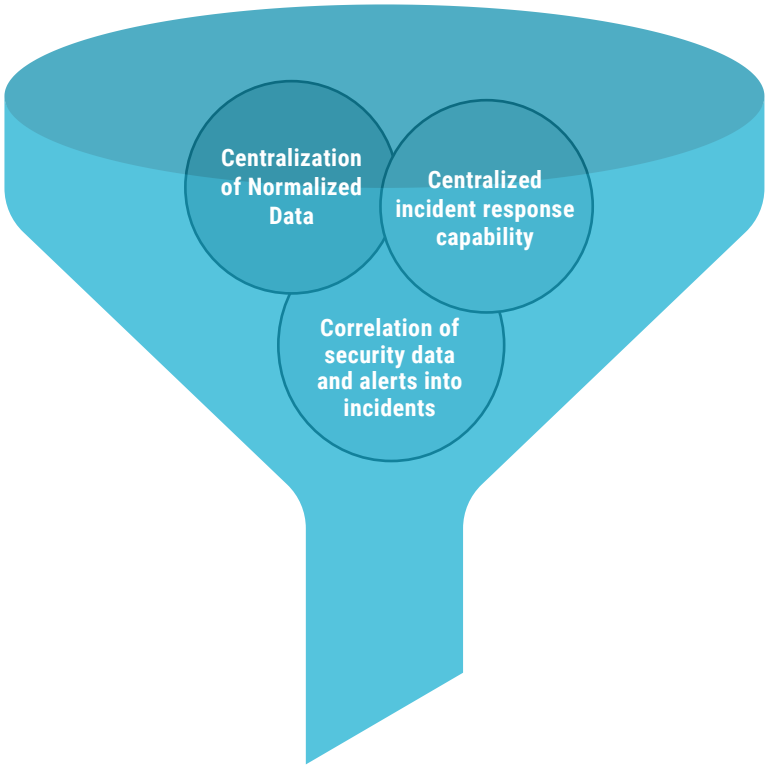
3. Reducing missed alerts by correlating and confirming alerts automatically.

4. Integrating relevant data for faster, more accurate alert triage.

5. Providing centralized configuration and hardening capability with weighted guidance to help prioritize activities.

XDR SYSTEM REQUIREMENTS

SIEM solutions aren't at the same level of threat detection and research analysis labs as XDR. While SIEM is delivered as SaaS, most XDR solutions are developed using new cloud-native architectures and services, making them an emerging alternative or complement to existing SIEM tools. However, XDRs are not a replacement for all SIEM use cases, such as generic log storage or compliance.



The three primary requirements of an XDR system are:

1. Centralization of normalized data – but primarily focusing on the XDR vendors' ecosystem only

2. Correlation of security data and alerts into incidents

3. A centralized incident response capability that can change the state of individual security products as part of incident response or security policy setting

USE CASES FOR XDR

In a report by Gartner, security professionals ranked three use cases, mirroring the tiers that security professionals are often classified with including:

Tier 1: Triage

XDR solutions can be adopted as the primary tool for aggregating data, monitoring systems, detecting events, and alerting security teams. These systems can form the base for further efforts or can enable a hand off to higher level teams.

Tier 2: Investigation

Teams can use solutions as repositories of analyses and information on events. This information, combined with with threat intelligence can be used to investigate events, evaluate response performance, and train security analysts.

Tier 3: Threat Hunting

Data collected by XDR solutions can be used as a baseline for performing threat hunting operations. These operations proactively seek evidence of threats have been overlooked by systems and analysts. Data used for, and collected during, threat hunting processes can also be used to create new threat intelligence which is then used to strengthen existing security policies and systems.

BENEFITS OF XDR

XDR solutions provide security leaders with many benefits including:

Improved protection

Inclusion of threat intelligence and adaptive machine learning ensures that solutions protect organizations against the most advanced adversaries. Plus, continuous monitoring and automated response blocks threats as soon as it's detected to prevent the attack from spreading.

Granular Visibility

Provides full user data at an endpoint combined with network and application communications, including information on access permissions, applications in use, and files accessed. Having full visibility across your environment from on-premises and in the cloud allows organizations to detect and prevent threats from escalating faster.

Effective Response

Robust data collection and analysis enables organizations to trace the path of attack and reconstruct the attacker's actions. This provides the information needed to locate the attacker wherever they are as well as valuable information that can be used to strengthen your defense strategy.

Greater Control

XDR's capabilities in both blacklisting and whitelisting traffic ensures that only approved actions and users can enter your environment.

Increased Productivity

Centralization reduces the number of alerts and time spent chasing false positives. In addition, since XDR solutions are deployed as platform, it's easier to maintain and manage, and reduce the number of interfaces that security teams need to access to remediate any escalating alerts.

AGILEBLUE

AgileBlue is a software company with innovative SOC|XDR-as-a-Service for 24/7 moinitoring, cloud security, data privacy and complicnace backed by our U.S. based SOC.

We detect cyber threats before you have been breached. Our SOC-as-a-Service platform is designed to monitor your cloud, network, and endpoints. Our modern SOC-as-a-Service is built on innovative machine learning and autonomous execution. For more information, visit our website: AgileBlue.com.

Ready to start protecting your company?

Request a Demo