AGILEBLUE

We Detect Cyber Threats
Before You're Breached

Our SOC platform is designed to monitor your cloud, network, and endpoints, so you can rest easy

We custom fit AgileBlue to you so you not only get the best technology, but the right technology for your company. Adaptive, evolutionary and alert, we learn the ins and outs of your on-premise network, cloud services, SaaS applications and data, so you get the capabilities of our next generation technology, customized to keep up with your team. When considering a SOC-as-a-Service partner, it's important to understand what each company offers and how they differ.

AGILEBLUE DIFFERENTIATORS:

Customized Cyber Risk Score and Dashboard that makes your security easy to understand

Silencer Technology with a 95% True Positive confidence score

Fixed Monthly Cost with no expensive surprises

One-on-One Support and quick access to real people when you need them

STRENGTHS AND ADVANTAGES:

Customization

We don't just watch for 'normal' industry threats. Our machine learning adapts to the behaviors of your specific cloud, network and users to create one-of-a-kind security operations center.

Relentless Monitoring

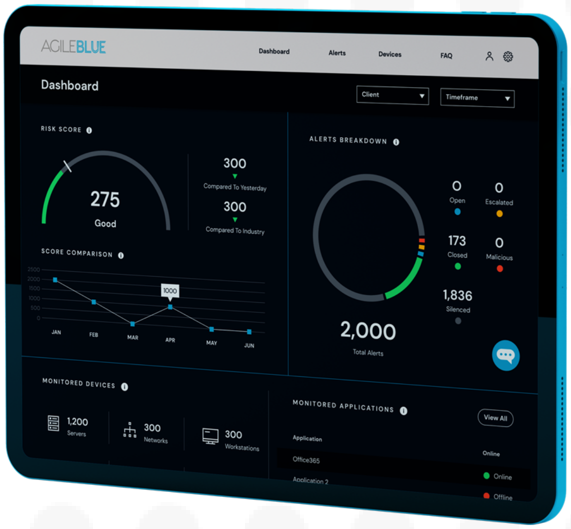
Our algorithms look for malicious threats, malware, ransomware, and software vulnerabilities. Our 24 x 7 x 365 promise to you includes human-based responses, asset discovery, vulnerability assessment, intrusion detection, behavior monitoring, log management, and cloud-based SIEM.

Customer Service

We'll break down the info when you're in a crisis, and in between you'll get consistent update meetings, one-on-one support, and quick access to real people when you need them.

EASY INTEGRATIONS:

- 2 week deployment time using a single agent across all endpoints
- Integrates with core threat vectors; Devices, Network, Cloud, Apps



AGILEBLUE

We Detect Cyber Threats
Before You're Breached

AgileBlue

Managed Service
MDR MEDR

Build Your Own
EDR SIEM

	AGILEBLUE	EDR	MEDR	SIEM	MDR
Monitor Your Entire Digital Infrastructure Identify and detect risks across your network, cloud platforms, endpoints, and applications.	✓	X	X	X	X
Machine Learning & User Behavior Analytics Real-Time Alerts driven by anomalous patterns in your data.	✓	X	X	✓	X
SIEM Access and Visibility See all security log data in the SIEM, on-demand access to retained logs.	✓	X	X	X	X
Instant Access to Security Experts Communicate around the clock with a US-based SOC Team.	✓	X	X	X	X
Issue Triage and Guided Remediation Critical events and actionable insights are delivered in ~ 8 minutes.	✓	X	✓	X	✓
Silencer Technology Detect the indicators of attack faster and with a 95% confidence score.	✓	X	X	X	X
Threat Hunting Daily hunting for suspicious activity across all of your environments.	✓	X	✓	✓	✓
Per Client Cyber-Risk Scoring Based on 13 critical security factors and Indicators of Attack (IoA) from MITRE framework.	✓	X	X	X	X
Pooled & Tiered Partner Pricing Flexible and predictive pricing based off client profile.	✓	X	X	X	X
Per Client On-Boarding Concierge White-glove setup and integration to monitor and enhance existing security layers.	✓	✓	✓	X	✓

Managed Endpoint Detection & Response (MEDR)
- Only covers endpoints, leaving vulnerabilities within the environment.

Extended Detection & Response (EDR)
- Requires the people and processes of a SOC to operate.

Managed Detection & Response (MDR)
- Limited by vendor and by levels of detection and response for the entire environment.

Security Information and Event Management (SIEM)
- Collects security data, requires a SOC team to operate.