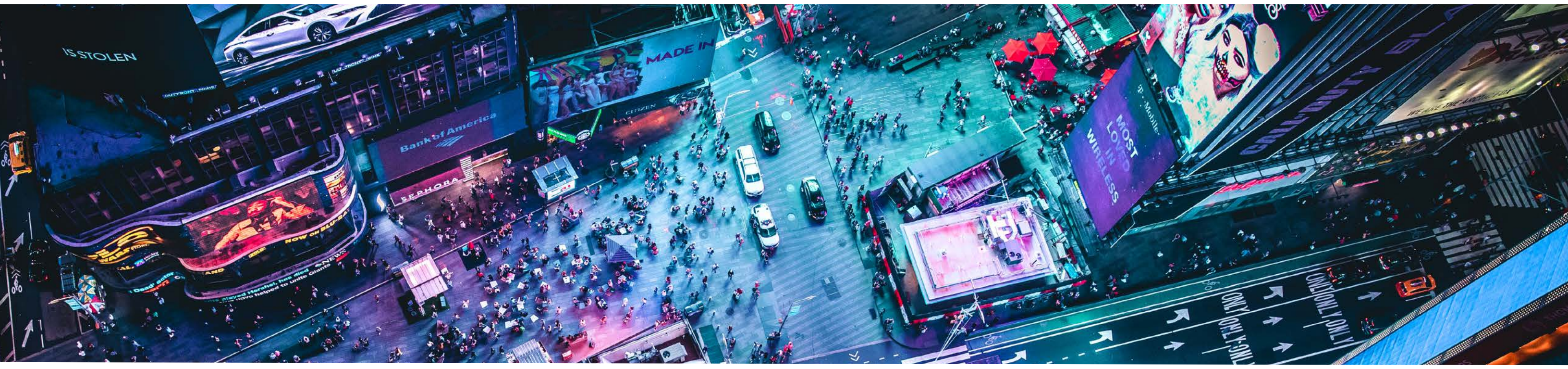
AGIO

AGIO MANAGED DETECTION & RESPONSE



The world of cybersecurity has evolved to the point where creating and maintaining a robust security posture is only the first step. The second step is about detection, and the third deals with response. Traditionally, cybersecurity investments have been directed at prevention, but as we become more sophisticated, and the market understands there is no bulletproof prevention method, we're seeing a shift towards the second and third phases – detection and response. Specifically, 68% of companies plan to enhance incident response capabilities in the next 12 months, and Gartner estimates by 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches – an increase from less than 30% in 2016.

We're here to help. Agio Managed Detection & Response (MDR) takes a real-time 360° approach to proactively monitoring your environment 24x7x365 so you're never caught on your heels. Leveraging our portfolio of services to fortify your cyber-defenses means the difference between a security threat and a security breach.

Specifically, when you sign up for our MDR solution, you get the full suite:

- **Agio Unified Security Management**
  powered by AlienVault
- **Agio Incident Response Management**
- **Agio Endpoint Detection & Response**
  powered by Cylance
- **Agio Email Threat Protection**
  powered by ProofPoint
- **Agio Phishing Protection**
  powered by Inky
- **Agio Mobile Web Security**
  powered by Cisco Umbrella
- **Agio Executive Privacy Monitoring**
  powered by AlienVault

AGIO UNIFIED SECURITY MANAGEMENT

powered by AlienVault

Our Unified Security Management service lies at the heart of our Managed Detection & Response portfolio, and it includes a number of elements:

ASSET DISCOVERY

We begin our Managed Detection & Response service with an asset discovery process within your environment, which provides a referenceable inventory of all your protected endpoints. This is critical, given most firms struggle to ever map their endpoints thoroughly and accurately. Our assessment also ensures that changes to your environment, like adding or removing servers, security appliances, network devices, etc., are always captured so no endpoints ever fall through the cracks.

SECURITY INCIDENT & EVENT MANAGEMENT (SIEM)

We use a discovery-driven approach designed to prevent future security blind spots, adding user, application, and business service context to events. Whether your information lives in your own data center, a hosted environment or the cloud, our engineers collect, aggregate and normalize logs, providing unparalleled threat monitoring, prioritization and mitigation responses. We look at data across the full spectrum – from security devices, to network devices, Active Directory, Windows and Linux servers, database servers, storage, and applications – to cross-correlate all of your security event data in real-time. What's more, we offer industry-specific custom alerts and correlation rules so our service works smarter and faster for your unique business.

ACTIVE THREAT DETECTION

We defend against ever-evolving, sophisticated evasion techniques, even when they are applied on multiple protocol levels. Through deep packet analysis at the internet perimeter and business critical network segments, signature-based attack recognition, content analysis of your data stream, and best-in-class subscription-based threat intelligence, as well as Open Threat Exchange (OTX), our security engineers are armed with everything they need to see the forest through the trees, detecting movement and threats of malicious execution.

VULNERABILITY SCANNING

Our automated scans assess network assets for vulnerabilities on a weekly (or monthly) basis to clearly identify potential areas of exploitation and increased security risk. We track these ongoing vulnerabilities and provide continual remediation recommendations. Finally, we also do the dirty work of eliminating the false positives, so your internal teams don't have to – reporting to you on the operating system, patch levels, and running services on all monitored systems.

SECURITY OPERATIONS CENTER (SOC)

Our 24x7x365 SOC offers event and problem management along with unlimited support; troubleshooting and diagnosis of system alerts and outages; root-cause analysis including workarounds for immediate resolution as well as longer-term permanent remediation; threat hunting; and finally, real-time access to your security dashboard, events and alerts so you can always see what we see. Our CISSP and SANS GSEC-certified security team then create weekly reports on your environment and meet with you monthly to summarize the traffic trends, attacks, and anomalies we're seeing. We conclude each of our monthly sessions by walking you through your specific and actionable recommendations, including how to quickly and efficiently implement those improvements.

It’s this level of service, delivered by our level of security engineers, on top of the best-in-breed platforms we leverage that set Agio’s Unified Security Management apart from the market. Our solution is the definition of a true 360° cybersecurity service to keep you protected and at the ready at all times.

AGIO INCIDENT RESPONSE MANAGEMENT

Agio Incident Response Management is a planned solution designed for the unplanned. We onboard, organize, prep and continually test your ability to respond when a breach happens.

Specifically, the program includes:

- Onboarding
    - Environment Discovery
    - Data Mapping
    - Incident Response Plan Development & Review
        - › Incident Response Policy
        - › Data Classification Policy
        - › Incident Response Procedure
        - › Incident Response Communication-Chain of Command Procedure
    - Tactical/Operational Incident Response Tabletop Exercise
- Monthly Incident Response Readiness Review
- Quarterly Status Review (monthly for first three months after going live)
    - Intelligence Briefings
    - Cybersecurity Events & Incidents Statistics Review
- Annual Executive IR Tabletop Exercise
- Incident Response Annual Review & Report
- Red Team Security Assessment* (annually, if applicable)

And when a breach does happen, we mobilize immediately and effectively to neutralize the threat and contain your exposure. Here is our cadence for you:

- We respond within 15 minutes of discovery.
- We send updates every 2 hours and hold conference calls every 4 hours, for critical incidents.
- We work the incident until it’s contained, and eradication and remediation plans have been defined.
- We send a full incident report, including recommendations, within 2 weeks of an incident being resolved.

AGIO ENDPOINT DETECTION & RESPONSE

powered by Cylance

We combine the most sophisticated endpoint detection technology with our 24x7x365 SOC to hunt, investigate and eradicate attacks before they damage your business. We go beyond no missed alerts, and proactively recommend changes to keep your environment more secure, always.

Specifically, our service includes:

- Zero-Day Prevention
- 24x7x365 Detection & Response
- Threat Hunting
- Industry-Specific Configuration Baseline
- Script Management
- USB Mass Storage Management

AGIO EMAIL THREAT PROTECTION

powered by ProofPoint

We provide multiple layers of cybersecurity to stop malware and non-malware threats, such as email fraud and imposter email. We control all aspects of inbound and outbound email to detect and block threats, preventing confidential information from getting into the wrong hands.

AGIO PHISHING PROTECTION

powered by Inky

Phishing is the #1 cyber-threat to your organization, which means you need a specific service designed to combat this specific beast. Our solution is a holistic, AI-driven solution to ensure your email stays protected as the threat landscape continues to evolve. We partner with Inky's best-in-breed Phish Fence technology, leveraging machine learning, behavior profiling and advanced heuristics forgery detection to uncover even the most sophisticated deep-sea phishing attacks that both trained users and conventional email filters miss. Once implemented, here's a run-down of what you can expect:

- State-of-the-art spam and anti-malware protection for both spear phishing and brand forgery attacks, while HTML sanitization blocks XSS, JavaScript, CSS attacks
- Incoming mail automatically checked against over two dozen computer vision and text analysis models that "see" the message much like a person would — so even very convincing forgeries get blocked
- Malicious mail automatically quarantined, while questionable mail is delivered with a clear, prominent warning your users will understand
- Users can click on the "Report Phish" link in an email to send the message to Agio's client support team for further analysis.

Bottom line, we've got you covered when it comes to the #1 threat to your users – phishing.

AGIO MOBILE WEB SECURITY

powered by Cisco Umbrella

Agio Mobile Web Security protects your mobile workforce from advanced threats wherever they are - in the office or on the road - offering you visibility while securing traffic both on and off your networks. Our service specifically leverages DNS and IP layer enforcement to stop threats over all ports and protocols, preventing malware from reaching your endpoints. Content enforcement also utilizes 80+ content categories to ensure your workforce is adhering to firm policies in and out of the office. Finally, command and control callback blocking prevents infected machines from reaching the attackers' servers to thwart exfiltration of data and execution of ransomware.

AGIO EXECUTIVE PRIVACY MONITORING

powered by AlienVault

Our Executive Privacy Monitoring service proactively monitors your executives' data, such as email and sensitive files, 24x7x365 for unauthorized access, retaining logs for 12-months. We collect email and pre-defined files' access/editing logs across the corporate environment and escalate if unauthorized access and/or editing of emails and files is discovered. We then provide you with a monthly, customizable report that identifies trends, anomalies, etc. with actionable recommendations.

WHY AGIO?

#OneAgio

When you select Agio, you're investing in a relationship with everyone who's a part of this firm. Our teams operate in a symbiotic relationship, based on deposits and withdrawals, that creates a vehicle for delivering more than just service. We deliver an experience that reaffirms to our clients we've got them covered. From clean, concise implementations; to consistent support backed by automation and tools that work the way they're supposed to; to value-add reporting; to accurate, timely invoicing; and content on the latest IT and cybersecurity trends, we bring the full breadth and depth of our talent to bear. We deliver #OneAgio.

For more information, please contact:

877.780.2446 | sales@agio.com