AGB
CYBER DIVISION

CYBER SECURITY SOLUTIONS

by

AGB CYBER DIVISION

ABOUT AGB CYBER DIVISION

At AGB Cyber, we provide comprehensive computer services along with premier customer service. We take the worry out of your technology by providing the knowledge and skills to keep your operations humming along; and we do it one-on-one, side-by-side with you, every step of the way. We don't just fix things, we evaluate your current and future needs and deliver the best solution for your business processes and objectives.

Advanced technology supported by our nationwide buying power gives you more cost-effective solutions than anywhere else. Let us become your IT Partner by helping you focus on your business, not your IT.

WHY AGB CYBER DIVISION

AGB Cyber brings more than 20 years combined experience in various industries (finance, healthcare, etc...). Whether you're concerned about workstation performance or upgrading your IT infrastructure, we can help. From managing high volume websites, email services, and migrations for mid sized companies, AGB Cyber can manage all your needs. Whether you need a server installed, a firewall updated, or your desktops cleared up from spyware and viruses, we provide expert technology services on these important issues.

We can partner with you as your IT staff, or provide additional support to your in-house team. We can install, maintain, monitor, and troubleshoot problems relating to your Microsoft , Fortinet, Cisco and SonicWALL, Windows and Mac desktops/Laptops, and general networking and computer hardware. We can plan and implement your backup solutions for disaster recovery.

AGB CYBER DIVISION'S APPROACH TO CYBER SECURITY

Numerous successful cyberattacks against even the best-funded, highly competent organizations demonstrate that current security strategies and solutions are not working. To address these shortcomings, AGB Cyber leverages its real-world cyber operations experience as well as evaluates the common patterns, strategies, and tactics that malicious cyber actors utilize to build cyber security solutions around the following principles:

.01

Breaches and compromises will occur. Regardless of the sophistication and layers of preventative and perimeter security, determined malicious cyber actors will continue to find ways to compromise organizations. Today, exploits, zero-days, poor IT hygiene, incorrect IT configuration, insecure hardware and software, human behavior, and insider threats lead to compromises. These causes, or variations of them, will remain effective for cyber attackers into the foreseeable future.

.02

Detection instead of prevention. Historically, cyber security solutions have focused on prevention. Preventing a compromise is more beneficial than detecting a compromise so intuitively it makes sense to focus efforts on prevention. Realistically, however, preventing all the possible methods of compromise is untenable, unaffordable, and arguably impossible. Such realization does not imply that organizations should abandon preventive cyber security solutions such as firewalls, intrusion prevention systems (IPS), and anti-virus (A/V), just that organizations should allocate equal resources, if not more, to detection-based cyber security solutions.

.03

Focus on detecting the common elements of malicious cyber activity, not malware. Examples of common elements include enumeration, lateral spread, and account compromise. Do not focus exclusively on malware detection - a reactionary strategy - as malware is constantly evolving and, as highlighted above, is not the only source for compromise.

.04

Malicious cyber actors have learned to leverage IT administration tools, tactics, and technologies to carry out their attacks. This “living-off-the-land” strategy is extremely effective as it’s easy to employ yet very challenging for many current cyber security solutions to detect. By leveraging benign in-place capabilities for malicious purposes, the effort, time, and technical skill needed to implement a successful attack is greatly reduced, allowing more malicious actors the ability to execute more frequent attacks with a willingness to throw away the initial malware or toolset.

.05

Understanding what happens at the endpoint is a necessity. Many cyber security solutions rely solely on network traffic analysis. With the majority of network traffic now encrypted, deep packet analysis is ineffective (unless SSL inspection is used which comes with its own implementation and management challenges). Regardless of whether network traffic is encrypted, aside from obvious threats such as traffic to/from known bad locations, trying to determine if network-based alerts are benign or malicious without evaluating the activity on the involved endpoints makes triaging such detections time-consuming and difficult. In addition, when malicious cyber actors use "living-off-the-land" techniques, the associated network traffic often is identical or very similar to the traffic of valid applications and users.

.06

Log analysis is time-consuming, technically demanding, and often expensive. Worse, unless suspicious events are immediately evaluated in detail, detecting a compromise in real-time becomes almost impossible. Even when a compromise is successfully detected, the investigation, correlation, and aggregation of related meta-data across log types is challenging and often requires highly skilled analysts. Furthermore, since storing and analyzing large amounts of log data is costly, log collection of endpoint activity (especially in large organizations) rarely occurs. This contradicts the previous principle of understanding endpoint activity. While organizations frequently implement log collection to support compliance or monitoring requirements, log collection itself is not security.

.07

Asset visibility and awareness is important to cyber security. In order to best protect an organization's infrastructure, the organization must first know what is connected to it. With the growth in smartphones, IP-enabled devices, and the Internet-of-Things (IoT), organizations need to know every device that is connected to their infrastructure, where they're located, and what they're doing in real-time.

.08

Network-based monitoring and detection is the near-term solution to IoT security. With the proliferation of IP-enabled devices across all industries and consumer segments, the numberof IoT devices is exponentially surpassing the number of traditional IT devices (desktops, laptops, server, routers, switches, smartphones, etc.).

The purpose and variety of IoT devices as well as the lack of standards, regulations, and security-hardening by current IoT vendors means that an endpoint-focused approach to IoT security is currently not feasible and may always be a challenge. Therefore, monitoring and detecting access to/from IoT devices aswell as monitoring and **detecting the activity of the devices themselves via network traffic is the most** cost-effective and widely applicable strategy.

.09

IoT (and its industrial counterparts such as building automation systems [BAS], operational technology [OT], and industrial control systems [ICS]) **and traditional IT security must be integrated.** In today's organizations, IoT/BAS/OT/ICS and traditional IT infrastructure coexist. Failing to detect threats or suspicious activity on either type of equipment or network can result in catastrophic outcomes. For example, in the infamous Target breach the compromise started on the IoT/BAS/OT/ICS side via a breached HVAC system and laterally spread to the IT infrastructure to steal payment information. In the case of the Ukraine PowerGrid attack the IT infrastructure was compromised to steal the necessary credentials to remotely access the air-gapped OT network.

.10

Response is required. Cyber security solutions excel at monitoring and detection. However, many have limited or no response capability. Organizations need to adopt more solutions that can effectively respond to emerging threats.

.11

Detection and response must be faster. Statistics vary on the duration between the initial compromise of an organization and its detection. For example, the 2018 Ponemon Cost of a Data Breach report has the average duration at 197 days while Fireeye's 2018 MTrend report has the median duration at 101 days. If organizations are going to win the cyber fight, these durations must be reduced to hours, minutes, and seconds.

.12

Security must be affordable. The cost to conduct a cyberattack has decreased. Conversely, most organizations' cyber security budgets continue to increase.

This trend must be reversed. One strategy is to disincentive malicious actors by **making cyberattacks more expensive by increasing the difficulty to carry out a** successful attack and reducing economic payouts for successful compromises. To accomplish this goal, organizations must be better secured. Unfortunately, if cyber security is cost-prohibitive, especially for small and medium-sized organizations, then organizations cannot afford better security and cyber-crime remains profitable. Without better securing organizations everywhere of all sizes, organizations will lose the cyber war.

WHEN WOULD I UTILIZE AGB CYBER'S SOLUTIONS?

Organizations choose AGB Cyber's solutions to solve numerous cyber security challenges and problems. The following list contains common reasons organizations choose ECT PROTECT to secure their network:

- Looking for advanced security since firewalls and anti-virus are no longer enough to stop modern cyberattacks
- Limited or no capability to monitor and detect lateral spread and compromised privileged accounts (both used in the majority of successful cyberattacks)
- Adequate perimeter protection and prevention solutions in place, but no real-time, live breach detection and response solution
- **Significant log data is consumed but there is a struggle to efficiently analyze the** information and detect threats in real-time
- Concerned about insider threats
- Manage environments with Internet-of-Things (IoT) devices, Operational Technology (OT), or Industrial Control Systems (ICS)
- Limited in-house resources to support an effective security program
- Incident response, ongoing threat remediation, and forensics
- Need to understand current cyber security posture, vulnerabilities, and risk (i.e., cyber security assessment)
- For service providers, want to better protect clients while increasing annual recurring revenue with an engaged, customer-focused partnership
- Compliance requirements

WHAT DIFFERENTIATES AGB CYBER

AGB Cyber differentiates itself from competitors through its proprietary technology, experienced personnel, and approach to cyber security. Moreover, ECT PROTECT's solutions provide multiple features and capabilities often found in more expensive point solutions at an affordable cost. The following items highlight key features and capabilities AGB Cyber's offers:

- Patented lateral movement/spread detection
- Detailed, real-time monitoring of privileged user accounts and activity
- Asset discovery and visibility; includes Bring-Your-Own-Devices (BYODs) and non-traditional IT equipment
- Live Network Map
- Built-in orchestration between SNAP-Defense platform and 3rd party integrations
- Integrated IoT/OT/BAS/ICS and traditional IT cyber security
- Integrated network and endpoint threat detection and response
- Point-and-click threat neutralization; isolate compromised devices to stop emerging threats
- Former US Government Cyber Security Operators and Technical Engineers
- Decades of experience conducting cyber assessments and incident response

WHAT DOES AGB CYBER OFFER?

AGB Cyber offers cyber security solutions primarily focused on threat detection and response. Aside from the cyber assessment and incident response services, AGB Cyber's products and services focus on:

- Real-time lateral movement detection
- Real-time network and infrastructure enumeration detection
- Real-time tradecraft detection
- Real-time monitoring of privileged accounts and activity
- Real-time monitoring and auditing of remote access
- Real-time effective response

Products:

AGB Cyber offers several cyber security products for direct sale. All add-on products extend or enhance the core capabilities of the primary product, SNAP-Defense, but are not required for comprehensive security coverage though highly recommended especially if no similar solution is currently in place. An organization would run these products directly utilizing their own in-house resources.

SNAPDEFENSE

Security Operations and Incident Response Platform

AGB Cyber's primary product is SNAP-Defense. Built as a security operations and incident response platform, SNAP-Defense includes patented real-time detection of malicious cyber techniques and tradecraft. SNAP-Defense consists of a Windows-based endpoint agent as well as a virtual appliance that collects core infrastructure data from Cisco and Juniper switches or Cisco Meraki devices. The endpoint is required while the virtual appliance is optional since not all environments contain Cisco and Juniper devices. SNAP-Defense provides a web-based user interface and supports flexible deployment options including on-premise and cloud-hosted.

SNAP-Defense capabilities include:

- Asset Discovery
- Network Visualization
- Real-time Monitoring
- Real-time Threat Detection
- Real-time Response
- Compliance
- Reporting
- Notifications
- Multi-Tenancy
- Flexible deployment options

SNAP-Defense currently supports the following 3rd-party integrations:

- Cisco Meraki
- Cisco AMP for Endpoint
- Sophos A/V and Intercept-X
- Tenable.io
- Webroot

NOTE: Additional 3rd-party integrations are continuously being added to the SNAP-Defense platform. Please contact AGB Cyber for a complete, updated list of integration partners.

Additional Product Add-ons:

In addition to offering its propriety SNAP-Defense platform, AGB Cyber also offers Sophos Anti-Virus, a traditional A/V endpoint protection product, as well as Sophos Intercept-X, an advanced endpoint protection product. These products are not required but are offered at cost for organizations that are looking for recommended endpoint protection solutions that integrate into the SNAP-Defense platform.

SOPHOS

Sophos Anti-Virus: Integrated anti-virus (A/V)

SNAP-Defense integrates with Sophos A/V via the Sophos Central Cloud API to provide a single platform for reviewing and monitoring traditional anti-virus activity. When SNAP-Defense receives a Sophos alert, it automatically surveys any endpoints involved in the alert with the SNAP-Defense endpoint agent. The additional meta-data collected by the SNAP agent helps triage whether the Sophos alert is a false positive or, if a real threat, was fully contained by the Sophos agent. Sophos A/V capabilities include:

- Anti-malware
- Pre-execution Behavior Analysis
- Web Security
- Download reputation

SOPHOS

Sophos Intercept-X: Integrated advanced endpoint protection

Like Sophos A/V, SNAP-Defense integrates with Sophos Intercept-X via the Sophos Central Cloud API to provide a single platform for reviewing and monitoring advanced endpoint threat activity. When SNAP-Defense receives an Intercept-X alert, it automatically surveys any endpoints involved in the alert with the SNAP-Defense endpoint agent. The additional metadata collected by the SNAP agent helps triage the Intercept-X alert, assisting in root cause analysis and ensuring Intercept-X completely contained any legitimate threat. Sophos Intercept-X capabilities include:

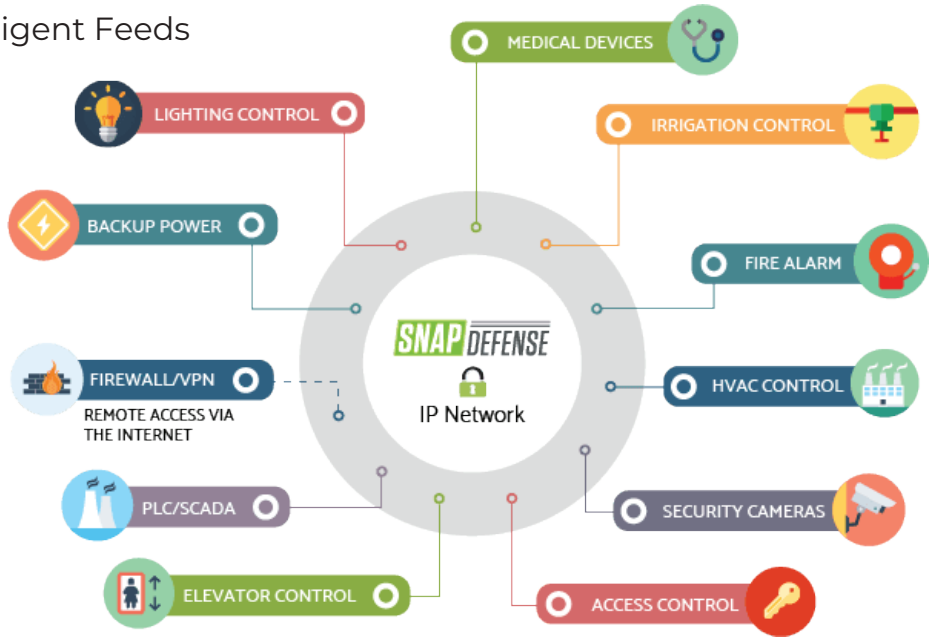
- Deep Learning Anti-malware
- Ransomware File Protection
- Man-in-the-browser Protection
- Disk & Boot Record Protection
- Credential Theft Protection
- Process Privilege Escalation
- Malicious Process Migration
- Asynchronous Procedure Calls Protection

NICOS

SNAP-Defense Hardware Appliance: Network monitoring and threat detection

The NICOS add-on is a hardware-based network appliance that resides internally on an organization's network. It is recommended for all environments, especially those that contain IoT/BAS/OT/ICS assets, such as smart buildings, manufacturing, shipping, transportation, power generation, energy, etc. The appliance monitors north/south and **east/west network traffic via a mirror or SPAN port. Newly detected devices and threats** are sent to the central SNAP-Defense platform. NICOS capabilities include:

- Asset Discovery and Visibility
- Port Scanning Detection
- **Obfuscated (TOR) Traffic Detection**
- Malicious Domain Detection
- Remote Access Monitoring (SSH, RDP, VNC, etc.)
- Custom rulesets
- Threat Intelligent Feeds



Services:

AGB Cyber's services cover the full spectrum of cyber security: assessment, monitoring, detection, and response. To provide these services, AGB Cyber leverages its experienced staff and partners as well as its SNAP-Defense platform.

MDR

24x7 Managed Detection and Response (MDR)

ECT PROTECT's signature service is its managed detection and response (MDR) which provides its SNAP-Defense platform and any purchased add-ons as a service offering. Clients that utilize this service receive 24-hour monitoring, threat detection, active threat hunting, and response. With our MDR service, organizations can focus their resources on their core business while maintaining an advanced cyber security posture.

MDR is the next evolution in managed security services. Most traditional managed security services rely on monitoring logs, especially of perimeter (e.g., firewall), network-based (e.g.,netflow), or malware-focused cyber security solutions. When a threat is detected, these services notify the organization and may provide remediation steps or response course of action. Very few, if any, can take an active response against an emerging threat.

Conversely, MDR focuses on detecting an emerging threat as soon as possible, ideally in realtime. Once a threat is detected, MDR includes an active response that can mitigate the attack regardless of the time or day thereby reducing overall impact to an organization's operations. Most MDR services, including AGB Cyber's, also focus heavily on endpoint detection as that is where most initial compromises occur. Finally, some MDR services may provide proactive threathunting and IT hygiene assessment to help organizations stay secure and reduce risk and vulnerabilities. AGB Cyber does provide these activities in its MDR service.

Cyber Security Assessments

AGB Cyber's cyber security assessments are custom-designed for each orgnizati based on the client's areas of interest and assessment requirements. Assessments typically include a comprehensive examination of an organization's cyber security posture from external vulnerabilities to its hiring and screening practices. Each assessment may also be adjusted during the process to specifically target or address any shortcomings or critical issues addressed as the assessment unfolds. Assessment activities include:

- Acquire information: Determine organization's information assets and prioritize them based on criticality.
- Identify vulnerabilities: Identify and document relevant vulnerabilities that put the organization at risk.
- Plan and prioritize: Effectively plan and prioritize remediation steps in the event of a breach based on the organization's goals, budgets, and timelines.
- Review security practices: Review and adjust security practices, policies, and solutions to insure organization is secure.

Incident Response

AGB Cyber's incident response services help an organization recover, reconstruct, and review data and information that was possibly compromised during a breach. The incident response team has decades of experience in computer forensics, e-discovery, cyber security, and expert testimony. Response and investigation activities are available for numerous incidents, including insider threats, external attacks, ransomware, and spear-phishing. The investigative process will provide answers to the following questions:

- How did it happen?
- What was stolen, encrypted, or destroyed?
- What steps should be taken to prevent further damage or compromise?
- Has the threat been eliminated, remediated, or resolved?Additional Product

CLIENT REQUIREMENTS

SNAP-Defense Platform & MDR Service

The following checklist will help determine if AGB Cyber's SNAP-Defense or MDR service are suitable for an organization as well as scope the implementation effort.

Note: For the # of devices below, include physical and virtual machines.

Microsoft Windows-based devices? _____
of Windows domain controllers _____

Linux based devices? _____

Apple Mac devices? _____

Does the organization have core network infrastructure (routers, switches, etc.)? _____
Cisco routers/switches? _____
Juniper routers/switches? _____
Cisco Meraki devices? _____
Independent Network Sites? _____

Does the organization have virtualization technology capable of running an OVA? _____

Does the organization have network infrastructure that supports mirror/SPAN ports? _____

IoT/OT/ICS devices? _____

of locations with IoT/OT/ICS devices? _____
If greater than 0, does the traffic of these devices flow through a central data center or network core? _____

Existing Anti-Virus product? (provide name) _____
If so, when does current contract expire? _____
Is the organization interested in updating A/V? _____
Is the organization interested in advanced endpoint protection (Sophos-X)? _____

Does the client currently use AWS? _____
What AWS services? _____

Does the client currently use Microsoft Azure? _____
What Azure Services? _____

Does the client use Office365? _____
Is AzureAD utilized? _____

Does the organization have a Remote Monitoring & Management (RMM) tool that can deploy Software? (product name) _____

Is the organization interested in buying the SNAP-Defense platform and managing it in-house or using AGB Cyber's MDR service? _____
If using the platform, does the organization plan to host the solution on-premise? _____

The minimum requirements for the SNAP-Defense platform or MDR service are:

SNAP-Defense Server (for on-premise SNAP-Defense installations only):

- Capability to run virtual machine OVA (may be cloud hosted as long as endpoints have network access to virtual machine) with following specifications:

Devices	>1,000	5,000	15,000	30,000
Processor Cores	2	4	8	10
Memory	8 GB	16 GB	24 GB	48 GB
Hard Drive*	SSD	SSD	SSD	SSD

*Size (GB) depends on the amount of historical data needed

SNAP-Defense Windows Endpoint Agent, Sophos A/V, and Sophos Intercept-X:

- Windows 7 SP1 or Windows Server 2008 R2 or newer
- Endpoint agent requires 10 MB RAM, 0% CPU, and no restart on install
- For large-scale deployments: RMM tool, PDQ Deploy, Windows Group Policy, or Windows SCCM

Core Router and Switch Collection:

- Cisco routers and switches and/or Juniper routers and switches and/or Cisco Meraki devices
- SNMP Read-only (RO) account

- For non-Meraki device collection, capability to run virtual machine OVA (may be cloud hosted as long as machine has access to core infrastructure devices) with following specifications:

Devices	>5,000	10,000+
Processor Cores	2	4
Memory	4 GB	16 GB
Hard Drive*	SSD	SSD

*Size (GB) depends on the amount of historical data needed

NICOS

- Router or switch infrastructure capable of supporting a mirror or SPAN port. **Ideally, placed at a location that can monitor north/south as well as east/west traffic.** Multiple NICOS may be required for independent geographic locations and/or heavily segmented networks (depending on the monitoring and visibility desired).

Cyber Assessment and Incident Response Services

Due to organization-specific requirements for cyber assessments and circumstances of incident response, organizations should contact AGB Cyber directly to determine the applicability and scope of the desired service.

SOLUTIONS IMPLEMENTATION

Implementation of AGB Cyber's solutions varies on whether an organization purchases product to manage in-house or utilizes one of ECT PROTECT's services. ECT PROTECT has spent considerable effort to streamline implementation and reduce an organization's resources and time-toimplement. For cloud-hosted or MDR service implementations, ***onboarding and setup often takes less than a day and many times under an hour.***

SNAP-Defense Platform

Organizations that purchase the SNAP-Defense platform and plan to manage it in-house can choose from two deployment options:

- On-premise (hosted in organization's own datacenter or public/private cloud infrastructure)
  - o AGB Cyber:
    - Provide the organization with the SNAP Server OVA and NIS OVA (only if multisite installation). Include installation and setup instructions.
    - If needed, ECT PROTECT will provide remote or on-site (depending on organization's location to a AGB Cyber office) installation assistance should problems arise.
    - Pre-configure any NICOS appliances and deliver to organization's locations.
    - **Provision on-premise license (either offline installation or online to SNAP** Hub) and provide to organization.
  - o Organization:
    - Load SNAP Server OVA into virtual infrastructure and configure as instructed. Add on-premise license from AGB Cyber..
    - If multiple-site installation, and additional Network Interaction Server (NIS) are necessary, load SNAP NIS OVA into virtual infrastructure and configure as instructed at each remote site.
    - Plug in pre-configured NICOS appliances at identified mirror or tap points in the network.
    - Deploy the SNAP-Defense Windows agent and Sophos A/V / Intercept-X (if add-ons purchased) using RMM tool or Windows Group Policy or SCCM.
- AGB Cyber-hosted Cloud Infrastructure
  - o AGB Cyber:
    - Provide the organization with cloud accounts and quick start guide.

- Provide the organization with SNAP NIS OVA (only if organization is utilizing core network collection).
- Pre-configure any NICOS appliances and deliver to organization's locationS.

o Organization:

- If performing core network collection, load SNAP NIS OVA into virtual infrastructure and configure as instructed at each site.
- Plug in pre-configured NICOS appliances at identified mirror or tap points in the network.
- Deploy the SNAP-Defense Windows agent and Sophos A/V / Intercept-X (if add-ons purchased) using RMM tool or Windows Group Policy or SCCM.

MDR Service

For the managed detection and response service, the only supported implementation model uses AGB Cyber's hosted cloud infrastructure. This model allows AGB Cyber to remotely monitor an organization's infrastructure without needing direct network access (e.g. RDP, VPN, SSH, etc.). The implementation plan consists of:

o AGB Cyber:

- Provide the organization with SNAP NIS OVA (only if organization is utilizing core network collection).
- Pre-configure any NICOS appliances and deliver to organization's locations.
- Establish response matrix (e.g., playbook) with organization to identify response actions during threat events

o Organization:

- If performing core network collection, load SNAP NIS OVA into virtual infrastructure and configure as instructed at each site.
- Plug in pre-configured NICOS appliances at identified mirror or tap points in the network.
- Deploy the SNAP-Defense Windows agent and Sophos A/V / Intercept-X (if add-ons purchased) using RMM tool or Windows Group Policy or SCCM.
- Establish response matrix (e.g., playbook) with AGB Cyber to identify response actions during potential threat events

Cyber Assessments and Incident Response

Implementations for the cyber assessments and incident response services are heavily dependent on the organization's location, services requested, desired service scope, and completion timeline. Contact AGB Cyber for organization-specific implementation details.