



Effective November 01, 2025. These Service Descriptions supersede and replace all prior versions.

Schedule of Managed Services

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Any services outlined in the Order are offered and billed at the monthly rate, based on the following counts ascertained by Provider at contract inception:

- Workstations (Desktops & Laptops)
- Users (e.g., employees, contractors, or any Client staff)
- Servers (On-premises)
- Servers (Cloud-based)
- Physical Locations (e.g., Corporate Offices)

MANAGED SECURITY SERVICES (GENERAL OVERVIEW)

Provider, through its Third-Party Service Providers, will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms of use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Client acknowledges that it can take up to six (6) months for Provider to fully implement any security services and that Client's environment may remain vulnerable during the implementation period.

Remote Access - Provider will install remote access and remote monitoring and management (RMM) software on Client's Devices and possibly other equipment at Client's office, to be utilized by Provider. Client grants explicit permission to Provider to install any RMM software or tools deemed necessary by Provider.

BASIC CYBERSECURITY PROGRAM

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Next-Generation Antivirus (NGAV) - leverages signature-less anti-malware solution that relies on machine learning (ML) and other technologies to streamline malware discovery and improve threat detection at the endpoint. As such, Provider will provide and install anti-malware software of Provider's choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs, or links ("Harmful Content"), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

Password Credential Management Services - Provider will administer Password Credential Management Services to enhance security and efficiency in managing access credentials across the organization. This will leverage systems to enforce password complexity requirements, and password audits to minimize the risk of unauthorized access and data breaches. Training materials (documentation & tutorials) are made available to educate on this product and encourage broad-scale adoption by Client's staff.

End-user Security Training - Provider will implement a managed cybersecurity awareness training (CSAT) platform ordered through a third party on Client's behalf. The program features:

- Initial enrollment of all technology-facing workforce members in the program; future additions and/or deletions to be performed by Client representative(s).
- Access to a curriculum of industry-leading cybersecurity awareness education.
- Management reporting and visibility into workforce participation and progress in the training curriculum.
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks that target individuals or groups.
- Automated enrollment into remedial training for individual workforce members who need more support, when more training is needed.
- Management reporting and visibility into workforce performance on testing campaigns.
- Management reporting and visibility into the improvement in workforce awareness and performance over time. Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals.

Phishing Simulation & Testing - Provider will acquire and assign an appropriate number of licenses to support the client environment. The Service will schedule email social engineering (commonly known as "phishing") campaigns to send at random times during a specified period. The campaigns are trackable, fully customizable and designed to keep track of every user's participation, creating both accountability and making cybersecurity education measurable.

Firewall Management - Provider will manage, monitor, and maintain Client's firewalls to ensure optimal performance and security. This includes configuration updates, rule adjustments, firmware upgrades, and real-time monitoring to protect the network from unauthorized access and evolving threats. This service does not include the initial procurement, installation, or provisioning of firewall equipment; Client is responsible for procurement, installation, and physical maintenance of the necessary hardware. Client also agrees to follow Provider's recommendations regarding the acquisition or replacement of equipment if deemed necessary to fulfill Client's objectives for network security.

Dark Web Monitoring - Provider will deliver Dark Web Monitoring services to identify instances where Client's sensitive data, such as credentials and other proprietary information, may appear on dark web forums, marketplaces, or other unauthorized platforms. This service enhances visibility into potential data breaches, providing actionable insights to help mitigate security risks and protect organizational assets.

Technology Business Reviews - Provider will conduct scheduled Technology Business Reviews (TBRs) to assess the alignment of your technology, security infrastructure and systems, with your organization's business objectives. These reviews will analyze key performance indicators, identify areas for improvement, and recommend strategic initiatives to enhance efficiency and competitiveness. TBRs will be conducted at a cadence and frequency determined by Provider.

ADVANCED CYBERSECURITY PROGRAM

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

This program is to include everything in the *BASIC CYBERSECURITY PROGRAM*, outlined above, as well as the following:

Security Incident Event Management (SIEM) Monitoring – Where compatible, Provider will deploy SIEM monitoring services to monitor all supported network devices including: client-requested compatible web services that have been reviewed and approved by Provider, onsite servers, workstations, firewalls, network switches and routers.

Managed Threat Detection & Response - Security data collected from the SIEM is correlated by enterprise-grade threat intelligence to detect, prioritize, and enable action against malware attack.

Security Operations Center (SOC) - The Services include:

- Advanced Malware Protection supported by SOC.
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
- Risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, as well as the root causes of these malicious activities, by quickly identifying and diagnosing corrupt source processes and system settings.
- Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify, and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action.

Managed Advanced Email Security - Provider will implement and manage advanced email security solutions designed to protect Client's email systems from threats such as phishing, malware, spam, and unauthorized access. These services include real-time threat detection, email encryption, and advanced filtering to safeguard sensitive communications and reduce the risk of email-based attacks. Client acknowledges that additional licensing or hardware may be

required and agrees to follow Provider's recommendations to achieve desired security outcomes.

Zero-Trust Endpoint Protection - Provider will deploy Zero-Trust Endpoint Protection solutions to secure devices and endpoints by implementing strict access controls, continuous monitoring, and behavior-based threat detection.

Application Whitelisting – Provider, with assistance and direction of Client, will deploy application whitelisting technology creating a baseline of permitted software applications & programs on endpoint systems. This means that only explicitly approved applications should be allowed to run, reducing the likelihood of disallowed programs from running, and which may attempt to inject unintended, non-allowed or malicious code into the environment.

ELITE CYBERSECURITY PROGRAM

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

To include the services outline in both the *BASIC CYBERSECURITY and ADVANCED CYBERSECURITY PROGRAMS* outlined above, as well as the following:

Vulnerability Assessment and Management (VA/VM) - Provider will perform regular VA/VM scans to identify and prioritize security vulnerabilities within your network infrastructure. These scans will be followed by comprehensive reports detailing discovered vulnerabilities and recommended remediation strategies to strengthen your organization's security posture. While Provider will notify Client of any vulnerabilities discovered that require Client's attention and cannot be easily resolved by Provider, please note that it will be the sole responsibility of the Client to make available resources, including financial, when needed, allowing Provider those resources needed to remediate the discovered vulnerabilities. This may include new products or services, which will be outlined in a separate Order.

Secure Access Service Edge (SASE) - Provider will implement Secure Access Service Edge (SASE) solutions to enable secure and seamless access to cloud-based applications and resources from any previously allowed location. This includes the integration of comprehensive security features such as zero-trust network access, secure web gateway, and cloud access security broker (CASB) to protect your organization's data and users against evolving cyber threats. Implementation of SASE may require implementation of optional conditional access policies in Microsoft 365 and/or location whitelisting and Site VPN tunnels depending on network topology, which could incur additional charges to be fully operational.

DMARC Email Security Services - Provider will implement and manage Domain-based Message Authentication, Reporting, and Conformance ("DMARC") services to assist in protecting Client's primary email domain from spoofing, phishing, and other unauthorized use. DMARC is an advanced email authentication protocol that validates the origin of email messages by verifying that they are sent from authorized servers and conform to the organization's domain policies. Through ongoing monitoring, policy enforcement, and reporting, Provider will help ensure that legitimate messages are delivered while fraudulent or deceptive emails are rejected or quarantined. This service strengthens Client's overall email security posture, safeguards organizational reputation, and provides actionable reporting to identify and mitigate unauthorized email activity.

Secure DNS - Provider will deploy Secure DNS solutions to enhance your organization's cybersecurity defenses by filtering malicious domain requests and preventing access to known malicious websites. This proactive approach helps mitigate the risk of malware infections, phishing attacks, and data exfiltration attempts by blocking malicious DNS queries at the network level.

Deep Packet Inspection (DPI) - Provider will employ DPI technology to analyze network traffic at the packet level, allowing for granular examination of data for security threats, performance issues, and potential compliance violations (compliance-related services available via separate Order).

Web Content Filtering - Provider will implement Web Content Filtering solutions to control and monitor internet access, allowing organizations to enforce their own acceptable use policies, block access to malicious or inappropriate websites, and mitigate the risk of malware infections and data breaches.

Software as a Service (SaaS) Monitoring and Alerting - Provider will establish monitoring and alerting systems tailored to Software as a Service (SaaS) applications, ensuring continuous oversight of performance metrics, availability, and security posture. SaaS applications, which Client may request Provider to monitor on their behalf, which can include for example: Microsoft 365, Google Workspace, Salesforce, Slack & Dropbox)

Written Information Security Plan (WISP) - Provider will assist with the development of a comprehensive Written Information Security Plan (WISP) outlining organizational policies, procedures, and controls for safeguarding sensitive information and mitigating cybersecurity risks. This plan will address areas such as data classification, access controls, and incident response, providing a framework for maintaining confidentiality, integrity, and availability of critical assets. The WISP documents will be designed to support the implementation of the Services and do not include specific regulatory or compliance obligations unique to the Client. Additionally, any policies or procedures that the Provider uses internally to govern the solutions and systems for the Client will be incorporated into the Client's WISP and inherited as part of their security program.

HELPDESK & IT SUPPORT (BOLT-ON)

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Overview: This Bolt-On Helpdesk & IT Support program is to be regarded as an optional addition to ONE of the security service programs offered above (*BASIC CYBERSECURITY*, *ADVANCED CYBERSECURITY* or *ELITE CYBERSECURITY*). Choosing ONE of the security programs is a pre-requisite for the Bolt-On Helpdesk & IT Support service offering to be made available to Client.

Unlimited Remote I.T. Support and Assistance - Provider will provide help desk support via desktop support application, e-mail, and phone. Provider can remotely access & control desktops to support Client staff. Unless otherwise included in an Order, all help desk services will include unlimited remote support to assist in resolving end-user communicated problems only to restore previous functionality, as required. New software may be installed after management requests approval for, and change management processes are followed, after the

request is received, in writing. Onsite support services are not included and will be billed separately (see "Onsite Support Services" below).

Aside from the exception of end-user computer replacements; all requests for moves, additions, changes or deletions to any Client-owned or Client-specific information system(s) are not included and will be considered a project, and will be quoted under another order and, once approved by Client, will be invoiced and billed separately.

Network and Device Maintenance – The Services include:

- **Server Monitoring and Management:** Provider will perform server monitoring and management including, alert monitoring and management of servers, periodic reporting and performance tuning, and prioritization of alerts to identify high-priority incidents. Provider will also perform remote remediation services as needed, and backup software monitoring and management. The Service Fee does not include major hardware / software upgrades or replacements or system/data migrations or new server installations.
- **Desktop Monitoring and Management:** Provider will perform desktop monitoring and management including alert monitoring & management of desktops, prioritization of alerts to identify high-priority incidents, remote remediation services as needed, quarterly configuration backups, occasional firmware updates (as required by manufacturer), and regular reporting and performance tuning. The Service Fee does not include hardware replacement or new hardware installations.
- **Core Security Services:** Provider will include in its services monthly Microsoft patch management, antivirus software and management, and remote software installations. Core Security Services also includes new / terminated employee setup and configuration.
- **Problem Management Services:** Provider will undertake problem management as soon as the Provider's monitoring staff becomes aware of an issue. All issues, with status or resolution, will be documented by posting updates to the Ticket Tracking System assigned to Client ("Problem Tickets").

Identity Access and Device Management - Provider will implement and manage solutions to ensure secure access to Client's systems and devices. This includes enforcing role-based access controls, managing user credentials, monitoring device compliance, and supporting multi-factor authentication (MFA) to mitigate risks associated with unauthorized access. Client acknowledges that additional software or hardware may be required and agrees to follow Provider's recommendations to achieve optimal security outcomes.

Microsoft 365 Backup Services - Provider will acquire and provide a solution that safeguards critical data in Microsoft 365, offering automated third-party backups of Client's Microsoft 365 user accounts, including granular recovery options to allow for comprehensive data protection and restoration.

ON-SITE SUPPORT SERVICES

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

Upon request and subject to the limitations identified in the Order, for Services that are within the scope of this Service Attachment, Provider will also deliver support Services on-site, at

Client's previously documented office locations only, during normal business hours (residences and/or home offices cannot be supported with on-site services). For on-site support that is not explicitly included in the Order, Client will pay Provider's then-prevailing hourly rate.

DATA BACKUP AND BUSINESS CONTINUITY PROGRAM

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order that includes those requested Services.

Option 1: Remote Backups for Endpoints - Provider, through its Third-Party Service Providers, will make its best effort to ensure the protection and recovery of Client's information. Data files of targeted workstations or servers requested to be backed up by Client, in writing, are backed up via a Third-Party Service Provider's on-premises software application (the "Application"), encrypted, and then sent to a storage server at Third-Party Service Provider's data center facility. There is no local (on-site) copy of the Client's backed-up data. Data files of targeted workstations or servers can be restored from the cloud back to the Client server at a file or image level. Targeted workstations or servers CANNOT be recovered (or "booted") in the cloud. This service will be considered a disaster recovery solution ONLY, and NOT a business continuity solution. Client understands and accepts that additional equipment (e.g., workstations, servers, network equipment), and configuration services may be required during any disaster recovery scenarios to restore Client's workstation and/or server data files. Provider will monitor the status of all scheduled backup jobs, notify Client of storage failures, as well as any corrective actions, as necessary.

Option 2: Remote & On-Site Backups for Endpoints (Cloud-only virtualization) - Provider, through its Third-Party Service Providers, will make its best effort to ensure the protection and recovery of Client's information. Data files of targeted workstations or servers are backed up via a Third-Party Service Provider's on-premises software application (the "Application"), encrypted, sent to an on-premises storage device at Client facility, and then further replicated to a cloud storage server at Third-Party Service Provider's data center facility. Targeted workstations or servers are intended to be recovered (or "booted") in the cloud using Third-Party Service Provider's data center facilities. Client understands and accepts that additional equipment (e.g., workstations, servers, network equipment), and configuration services may be required during any business continuity or disaster recovery scenarios to restore Client's workstation and/or server data files. Provider will monitor the status of all scheduled backup jobs, notify Client of storage failures, as well as any corrective actions necessary.

Option 3: Remote & On-Site Backups for Endpoints (Cloud & on-premises virtualization) - Provider, through its Third-Party Service Providers, will make its best effort to ensure the protection and recovery of Client's information. Data files of targeted workstations or servers are backed up via a Third-Party Service Provider's on-premises software application (the "Application"), encrypted, and then sent to an on-premises storage server at Client facility, and then sent to a storage server at Third-Party Service Providers data center facility. Targeted workstations or servers can be recovered (or "booted") in the cloud using Third-Party Service Provider's data center facilities OR using on-premises storage server at Client facility, whichever option is technically most feasible at the time of failure, and when manual failover to this backup system is requested by Client. Client understands and accepts that additional equipment (e.g., workstations, servers, network equipment), and configuration may be required during any

business continuity or disaster recovery scenarios to, temporarily or permanently, restore Client's workstation and/or server data files. Provider will monitor the status of all scheduled backup jobs, as well as notify Client of storage failures and corrective actions, as necessary.

Option 4: Remote Backup for Cloud Services - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files of compatible cloud services (e.g., Microsoft 365, QuickBooks Online) are backed up via a Third-Party Service Provider's proprietary web services and connections, and then sent to a storage server at Third-Party Service Provider's data center facility. Targeted cloud services cannot be recovered or "booted" in the cloud if Client's cloud provider's services are unavailable. Therefore, this service is considered a disaster recovery solution ONLY, and NOT a business continuity solution. Client understands and accepts that additional services (e.g., additional cloud storage, services with cloud service providers) and configuration may be required during any disaster recovery scenarios to Client's data files of cloud services. Provider will monitor the status of all scheduled backup jobs, notify Client of storage failures and corrective actions.

If Client experiences an event precipitating a major loss of data, Client will notify Provider that such a data loss event has occurred within no more than 1 business day.

Termination of Data Backup and Business Continuity Program - Upon termination of these Data Backup Services, Provider will request, and Client shall return, any and all Provider-owned backup equipment and remove the Application from Client systems. Provider will work with Third-Party Service Providers to ensure that Client data is removed from Third-Party Service Provider's data center facilities.

VIRTUAL CHIEF SECURITY OFFICER (vCSO) PROGRAM

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

This program is to include everything in the *VIRTUAL CHIEF SECURITY OFFICER (vCSO) PROGRAM*, outlined above, as well as the following:

Provider will deliver Virtual Chief Security Officer services to support the Client's strategic and operational cybersecurity needs.

Recurring Third-Party Assessments - Provider will coordinate and support assessments conducted by an independent third party, providing unbiased evaluations of the Client's cybersecurity posture and the Provider's performance to ensure transparency and continuous improvement.

Internal & External Third-Party Vulnerability Analysis - Provider will conduct regular vulnerability analyses for both internal systems and third-party integrations to identify and remediate security weaknesses.

Stakeholder Tabletop Security Exercises - Provider will organize and lead simulated security incidents ("Tabletop Exercise") annually to train and prepare stakeholders on incident response strategies and protocols.

Governance, Policies, and Procedures Consulting - Provider will assist in the creation, review, and refinement of governance frameworks, policies, and procedures to align with industry best practices and regulatory requirements.

Board & Executive Stakeholder Evidence Reviews - Provider will present and review cybersecurity evidence and key performance indicators with the Client's Board and executive stakeholders annually to support informed decision-making and strategic planning.

NOTE: This section is intended as an informational overview of the vCSO program, and this Service will be fully outlined and defined in a separate statement of work (SOW). In the event of a disparity between this section's service description and the separate vCSO program SOW, the content and terms outlined in the vCSO program SOW shall prevail.

COMPLIANCE AS A SERVICE (CaaS) PROGRAM

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

This program is to include everything in the *COMPLIANCE AS A SERVICE (CaaS) PROGRAM*, outlined above, as well as the following:

Provider will deliver Compliance as a Service solutions to assist the Client in achieving and maintaining compliance with relevant frameworks and regulatory requirements. CaaS Program cost and term's structure dependent on customer selected frameworks and control sets, as well as implementation complexity.

Access to Next-Generation Governance, Risk, and Compliance (GRC) Engine - Provider will grant access to a GRC platform designed to streamline the management of governance, risk, and compliance activities with advanced capabilities for tracking, reporting, and automation.

Automated Monitoring and Evidence Collection - Provider will implement tools to automate the monitoring of compliance activities and collection of evidence to support audits and assessments.

Program for Compliance Against Required Control Frameworks - Provider will assist in building and managing a compliance program tailored to meet the requirements of relevant control frameworks selected by Client (such as CMMC, ISO, and NIST).

Access to Vendor Risk Management Engine - Provider will provide tools to enable the Client to assess, monitor, and manage risks associated with third-party vendors.

Access to Risk Register and Management Engine - Provider will deliver access to a centralized risk register to document, track, and mitigate risks effectively across the organization.

Inherited Security Policies and Program Governance - As part of the Services provided under this Agreement, Client acknowledges and agrees that certain operational and security policies are integrated into the Services and will be inherited by Client based on the tier of services selected (Basic, Advanced, or Elite) as specified in the applicable Order. These

policies reflect Provider's internal standards for configuration, management, and oversight, and are essential for delivering services in a secure and compliant manner, and are reflected in the Policy Inheritance Matrix attached to this Schedule.

NOTE: This section is intended as an informational overview of the CaaS program, and this Service will be fully outlined and defined in a separate statement of work (SOW). In the event of a disparity between this section's service description and the separate CaaS program SOW, the content and terms outlined in the CaaS program SOW shall prevail.

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY
TIME WITHOUT NOTICE.**

Policy Inheritance Matrix Based On Plan Selection

Policy ID	Policy Name	BCS	ACS	ECS	ITM	VCSO	CAAS
POL-2	ACCESS MANAGEMENT POLICY		X	X	X		
POL-3	ANTIVIRUS POLICY	X	X	X	X		
POL-4	APPLICATION SECURITY POLICY		X	X	X		
POL-5	ASSET MANAGEMENT POLICY	X	X	X	X		
POL-6	AVAILABILITY POLICY				X		
POL-7	BACKUP POLICY				X		
POL-8	CONFIDENTIALITY POLICY	X	X	X	X	X	
POL-12	ENCRYPTION POLICY	X	X	X	X		
POL-13	INCIDENT MANAGEMENT POLICY	X	X	X	X	X	
POL-14	LOGGING AND MONITORING POLICY	X	X	X			
POL-15	NETWORK MANAGEMENT POLICY	X	X	X	X		
POL-16	PASSWORD POLICY	X	X	X	X		
POL-17	PATCH MANAGEMENT POLICY				X		
POL-18	PERSONNEL SECURITY POLICY	X	X	X	X	X	
POL-19	REMOTE ACCESS POLICY	X	X	X	X		
POL-21	VENDOR MANAGEMENT POLICY					X	
POL-22	VULNERABILITY MANAGEMENT POLICY			X		X	
POL-26	BUSINESS CONTINUITY POLICY				X		
POL-29	DISASTER RECOVERY POLICY				X		
POL-31	MOBILE & BYOD DEVICE POLICY				X		
POL-33	RISK MANAGEMENT POLICY						X
POL-35	SOFTWARE DEVELOPMENT LIFECYCLE POLICY (IT OPS ONLY)				X		

Procedure ID	Procedure Name	BCS	ACS	ECS	ITM	VCSO	CAAS
PRO-2	EMPLOYEE AND ASSET ONBOARDING PROCEDURES				X		
PRO-4	BUSINESS CONTINUITY AND DISASTER RECOVERY PROCEDURES				X		
PRO-4	PATCH MANAGEMENT PROCEDURE				X		
PRO-6	RANSOMWARE PROCEDURE	X	X	X	X	X	

PRO-7	PROCEDURE FOR CONTROL OF DOCUMENTED INFORMATION	X	X	X	X		
PRO-1	CONTACT PROCEDURE WITH LOCAL AUTHORITIES	X	X	X	X	X	
PRO-11	INTERNAL AUDIT PROCEDURE						X
PRO-12	POLICY ALIGNMENT FOR GOVERNANCE PROCEDURE						X

<i>Legend of Exceed's Service Plans</i>	
BCS = Basic Cybersecurity	ITM = IT Management (Helpdesk & IT Support – Bolt-on)
ACS = Advanced Cybersecurity	VCISO = Virtual Chief Security Officer
ECS = Elite Cybersecurity	CAAS = Compliance as a Service