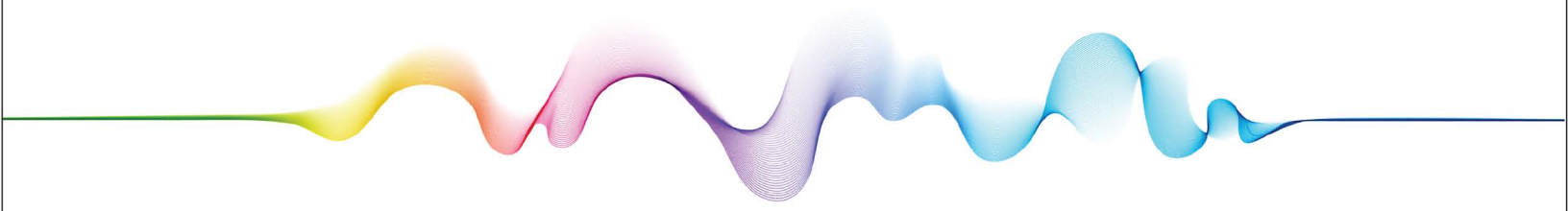
INSIGHT REPORT

OVERVIEW OF THE EMAIL SECURITY COMMERCIAL MARKET



TAG CYBERSECURITY

TAG Insights Report: Overview of the Email Security Commercial Market

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Infosphere
Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
March 17, 2024

Introduction

This TAG Insights Report on *Email Security* is intended to help companies, managers, practitioners, researchers, investors, and commercial vendors better understand current trends, issues, and market opportunities in this area. A list of representative commercial vendors working in various areas of email security is included. The five specific areas of covered in this report include:

1. Anti-Phishing Tools
2. DMARC
3. Email Encryption
4. Phish Testing and Training
5. Secure Email Gateway

This report is intended for general and unrestricted use, but interested readers are encouraged to connect with the TAG research and advisory team for more information on the private TAG Research as a Service (RaaS) community that covers, discusses, and shares information on these topics in more depth and includes a wider range of startups, vendors, and companies.

TAG Taxonomy

We organize this TAG Insights Report as per our updated TAG Taxonomy which includes twenty categories of modern solution areas where stakeholders and buyers can find suitable commercial products and services for purchase and use. Each category has five subcategories

that correspond to the main areas in which practitioners can focus. These subcategories are discussed below.

1 Application Security 1.1 API Security 1.2 Application Security Testing 1.3 Application Security Posture Mgmt. 1.4 Runtime Application Security 1.5 SBOM/SCA	**6 Email Security** 6.1 Anti-Phishing Tools 6.2 DMARC 6.3 Email Encryption 6.4 Phish Testing and Training 6.5 Secure Email Gateway	**11 Identity and Access Management** 11.1 Authorization 11.2 IAM Platforms 11.3 identity, Anti-Fraud, and KYC 11.4 Identity Governance and Admin. 11.5 Privileged Access Management	**16 Operational Technology Security** 16.1 ICS/OT Device Security 16.2 ICS/OT Visibility 16.3 Unidirectional Gateway 16.4 Vehicle Security 16.5 Zero Trust OT
2 Attack Surface Management 2.1 Bug Bounty Services 2.2 External Attack Surface Management 2.3 Automated Pen Testing/Red Teams 2.4 Breach and Attack Simulation 2.5 Security Ratings Platforms	**7 Encryption and PKI** 7.1 Certification Authority (CA) 7.2 Data Encryption 7.3 Key and Secret Management 7.4 Key and Certificate Protection 7.5 Post-Quantum Cryptography	**12 Security Operations and Response** 12.1 Data Forensics and eDiscovery 12.2 Incident Response 12.3 SIEM Platforms 12.4 SOC/SOAR Support 12.5 Threat Hunting	**17 Security Professional Services** 17.1 Penetration Testing 17.2 Security Assessments 17.3 Security Research and Advisory 17.4 Security Training 17.5 Value Added Resellers
3 Authentication 3.1 Biometrics 3.2 Multifactor Authentication 3.3 Passwordless Authentication 3.4 Password Management 3.5 Single Sign-On	**8 Endpoint Protection** 8.1 Antivirus Software 8.2 Browser Isolation 8.3 Content Disarm and Reconstruction 8.4 Endpoint Detection and Response 8.5 Security Enhanced Browser	**13 Managed Security Services** 13.1 DDOS Security 13.2 Managed Detection and Response 13.3 Managed Security Services Platform 13.4 Network Detection and Response 13.5 XDR Services	**18 Software Lifecycle Security** 18.1 AI/MLOps Security 18.2 Container/Kubernetes Security 18.3 Container Scanning 18.4 DevSecOps Platforms 18.5 Infrastructure-as-Code Security
4 Cloud Security 4.1 Cloud Data Fragmentation 4.2 Cloud Infrastructure Entitlement Mgmt. 4.3 Cloud Security Posture Management 4.4 Cloud Workload Protection Platform 4.5 Microsegmentation	**9 Enterprise IT Infrastructure** 9.1 Asset Inventory 9.2 Backup Platform 9.3 Infrastructure Resilience 9.4 Physical Security 9.5 Secure Sharing and Collaboration	**14 Mobility Security** 14.1 IOT Security 14.2 Mobile App Security 14.3 Mobile Device Management 14.4 Mobile Device Security 14.5 Mobility Infrastructure Security	**19 Threat and Vulnerability Management** 19.1 Digital Risk Protection 19.2 Security Scanning 19.3 Third Party Risk Management 19.4 Threat and Vulnerability Platform 19.5 Threat Intelligence
5 Data Security 5.1 Cloud Data Security Posture Mgmt. 5.2 Data Access Governance 5.3 Data Discovery and Classification 5.4 Data Leakage Protection 5.5 Data Privacy Platform	**10 Governance, Risk, and Compliance** 10.1 Continuous Compliance 10.2 Cyber Insurance 10.3 Incident Reporting 10.4 GRC Platform 10.5 Risk Management Platform	**15 Network Security** 15.1 Network Access Control 15.2 Next Generation Firewalls 15.3 Secure Access Service Edge (SSE) 15.4 Virtual Private Networks 15.5 Zero Trust Network Access	**20 Web Security** 20.1 Bot Management 20.2 Content Security 20.3 Secure Web Gateway 20.4 Web Application Firewall 20.5 Website Scanning

Figure 1. TAG Taxonomy for Cybersecurity

Overview of Email Security Solutions

The following emerging global commercial opportunities involving email security solutions are covered in this report, including the listing of several viable commercial entities providing solutions on the market today:

1. Anti-phishing tools help prevent cyber threats by identifying and blocking malicious emails, URLs, or attachments, reducing the risk of users falling victim to phishing attacks.
2. DMARC (Domain-based Message Authentication, Reporting, and Conformance) enhances email security by allowing domain owners to specify policies for email authentication, thwarting email spoofing and domain impersonation.
3. Email encryption safeguards sensitive information by encoding email content, attachments, and communication channels, ensuring confidentiality, and preventing unauthorized access.
4. Phish testing and training educates users on recognizing phishing attempts through simulated attacks, empowering them to identify and report suspicious emails, bolstering overall cybersecurity awareness and resilience.
5. Secure email gateways (SEGs) serve as a frontline defense mechanism, analyzing inbound and outbound emails for threats, enforcing security policies, and blocking malicious content, fortifying organizations' email infrastructure against cyber threats.

Focus Area: Anti-Phishing Tools

Anti-phishing tools play a critical role in cybersecurity by combatting one of the most prevalent and damaging cyber threats: phishing attacks. These tools utilize various techniques such as email filtering, URL analysis, and machine learning algorithms to detect and block phishing attempts. By analyzing email headers, content, and sender reputation, anti-phishing tools can identify suspicious emails that exhibit common phishing characteristics, such as deceptive subject lines, spoofed sender addresses, or malicious attachments.

Advanced anti-phishing tools employ real-time threat intelligence feeds to stay updated on emerging phishing tactics and trends, enabling organizations to proactively defend against evolving threats. Through continuous monitoring and analysis of email traffic, these tools can swiftly identify and neutralize phishing campaigns before they inflict harm.

Furthermore, anti-phishing tools often incorporate user education and awareness features, providing timely warnings and guidance to users when they receive suspicious emails. By educating users about phishing techniques and encouraging them to exercise caution, these tools empower individuals to make informed decisions and avoid falling victim to phishing scams.

Focus Area: DMARC

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is a key cybersecurity protocol that enhances email security by enabling domain owners to authenticate their emails and specify policies for handling unauthorized messages. By implementing DMARC, organizations can prevent email spoofing and domain impersonation, which are commonly exploited in phishing attacks.

DMARC works by allowing domain owners to publish policies instructing email recipients on how to handle emails that fail authentication checks. These policies can include options such as rejecting, quarantining, or monitoring suspicious emails. Additionally, DMARC provides valuable reporting mechanisms that give domain owners visibility into email authentication results, enabling them to identify unauthorized senders and take corrective actions.

Moreover, DMARC works in conjunction with other email authentication protocols such as SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to provide comprehensive email security. By aligning these authentication mechanisms, DMARC helps organizations establish a strong email security posture, mitigating the risk of email-based attacks and protecting their brand reputation.

Focus Area: Email Encryption

Email encryption is a vital cybersecurity measure that protects sensitive information by encoding email content, attachments, and communication channels, rendering them unreadable to unauthorized parties. By encrypting email communications, organizations can safeguard confidential data against interception, eavesdropping, and unauthorized access.

Encryption transforms plaintext email messages into ciphertext using cryptographic algorithms, making it virtually impossible for adversaries to decipher the content without the corresponding decryption key. Additionally, email encryption solutions often utilize public-key cryptography, where each user possesses a public key for encrypting messages and a private key for decrypting them, ensuring secure end-to-end communication.

Email encryption solutions may offer additional features such as digital signatures, which verify the authenticity and integrity of email messages, providing assurance that the communication has not been tampered with or altered in transit.

Focus Area: Phish Testing and Training

Phish testing and training initiatives are essential components of cybersecurity awareness programs aimed at educating users on recognizing and mitigating phishing threats. These programs simulate phishing attacks to assess users' susceptibility to social engineering tactics and provide targeted training to improve their awareness and response to phishing attempts.

Phish testing involves sending simulated phishing emails to employees to gauge their susceptibility to phishing scams. By analyzing user responses, organizations can identify areas for improvement and tailor training programs to address specific vulnerabilities. Additionally, phish testing helps raise awareness about phishing threats and fosters a culture of vigilance among employees.

Phish training delivers interactive educational materials, such as online courses, tutorials, and awareness campaigns, to equip users with the knowledge and skills needed to identify phishing indicators, verify email authenticity, and report suspicious emails effectively. By empowering users to become the first line of defense against phishing attacks, organizations can significantly reduce the risk of data breaches and security incidents.

Focus Area: Secure Email Gateway

A secure email gateway (SEG) serves as a frontline defense mechanism against email-borne threats, including phishing attacks, malware, spam, and other malicious content. SEGs analyze inbound and outbound email traffic using advanced threat detection techniques to identify and block potential threats before they reach end-users' mailboxes.

SEGs employ multiple layers of security controls, including email filtering, antivirus scanning, content analysis, and URL rewriting, to detect and neutralize various types of email-based threats. By inspecting email headers, attachments, and embedded URLs, SEGs can identify suspicious patterns, malicious payloads, and phishing attempts, protecting organizations from cyber threats.

SEGs incorporate threat intelligence feeds and machine learning algorithms to stay updated on emerging threats and adapt their defense mechanisms accordingly. By leveraging real-time

threat data and behavioral analytics, SEGs can accurately differentiate between legitimate and malicious email traffic, minimizing false positives and false negatives.

SEGs offer policy-based controls and customizable security settings, allowing organizations to enforce email security policies, comply with regulatory requirements, and mitigate risks associated with email communication.

Companies and Contributions

The companies listed below emerged as part of our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for email security as a means for driving toward a more secure global ecosystem.

Anti-Phishing Tool Vendors

1. Abnormal Security: Inbound Email Protection blocks email attacks including phishing, malware, ransomware, social engineering, executive impersonation, invoice fraud, spam and graymail using behavioral AI.
2. Agari: Agari provides email security solutions, including anti-phishing tools, to protect against email fraud, business email compromise, and advanced threats.
3. Area 1 Security:Area 1 Security provides anti-phishing solutions that preemptively block phishing attacks across email, web, and network channels.
4. Avanan: Avanan offers a cloud-native security platform that protects against phishing, malware, and data leakage in cloud-based email and collaboration platforms.
5. Barracuda Networks: Barracuda Email Protection offers AI-powered anti-phishing tools to detect and block spear-phishing attacks and email account compromise.
6. Cisco: Cisco Secure Email offers comprehensive email security solutions, including anti-phishing tools, to protect against advanced threats and phishing attacks.
7. Cofense: Cofense PhishMe provides phishing simulation and training solutions to educate users and improve awareness of phishing threats.
8. CTM360: CTM360 Brand Protection & Anti-Phishing allows users to detect and perform takedowns on all phishing sites, typo squatted domains, cyber evil twin sites and more.
9. Cyren: The Cyren Email Security Engine protects email servers and accounts by blocking any type of attack-spam, malware or phishing in real-time.
10. Egress: Egress Defend provides advanced detection capabilities that stop phishing attacks. Customers receive intelligent technologies that evaluate context, relationships and message content.
11. Eset: Customers receive a password manager, encryption, threat scanning, payment protection, network access protection, parental control, and anti-phishing capabilities.
12. Forcepoint: Forcepoint Email Security offers advanced threat protection, data loss prevention, and email encryption capabilities to defend against phishing attacks.
13. Fortinet: FortiPhish is a cloud-delivered phishing simulation service using deep knowledge of phishing techniques based on research by Fortinet FortiGuard Labs to help train and test awareness and vigilance of employees.

14. GreatHorn: GreatHorn offers cloud-native email security solutions to protect against phishing, malware, and account takeover attacks.
15. INKY: INKY uses machine learning and computer vision to identify and block zero-day phishing emails that get through legacy email systems.
16. IRONSCALES: IRONSCALES offers an AI-powered anti-phishing platform that combines human intelligence with machine learning to detect and remediate phishing attacks.
17. KnowBe4: KnowBe4 provides a security awareness training platform that includes phishing simulation and education to help organizations defend against social engineering attacks.
18. Material Security: Protect your organization from sophisticated email attacks with one solution for advanced inbound detection, threat hunting, abuse-mailbox automation, and real-world training
19. Microsoft: Microsoft Defender XDR includes anti-phishing capabilities to detect and block malicious emails.
20. Mimecast: Mimecast Email Security provides cloud-based protection against email-borne threats, including phishing, spam, and malware.
21. PhishLabs: PhishLabs offers a comprehensive anti-phishing platform that combines threat intelligence, monitoring, and takedown services to protect against phishing.
22. Proofpoint Proofpoint provides advanced threat protection solutions, including anti-phishing tools, to safeguard organizations from email and cyber threats.
23. Sophos: Sophos Email Security offers comprehensive protection against email threats, including phishing, ransomware, and data loss.
24. Spam Titan: SpamTitan blocks spam, viruses, malware, ransomware, phishing attempts, and other email threats.
25. Symantec- Symantec Enterprise Cloud provides email security solutions, including anti-phishing tools, to protect against targeted attacks and email fraud.
26. Trellix: Trellix Email Security offers threat prevention, detection, and response capabilities to protect against sophisticated email-based attacks, including phishing.
27. Trend Micro: Trend Micro Email Security provides protection against phishing and other email threats through threat intelligence and detection capabilities.
28. Vade Secure: Vade Secure provides AI-driven email security solutions to detect and block phishing, spear-phishing, and ransomware attacks.

DMARC Vendors

1. Agari: Agari (part of Fortra) Brand Protection leverages DMARC authentication to protect against email-based brand impersonation and phishing attacks.
2. Barracuda Networks: Barracuda Sentinel includes DMARC authentication capabilities to protect against domain spoofing and impersonation attacks.
3. Cisco: Cisco Secure Email includes DMARC authentication and reporting features to protect against email fraud and impersonation.
4. Mimecast: Mimecast DMARC Analyzer provides DMARC reporting and analysis tools to help organizations implement and monitor DMARC policies effectively.

5. CTM360: CTM360 DMARC360 offers DMARC deployment and management services to protect organizations from email impersonation and domain abuse.
6. Dmarcian: Dmarcian offers DMARC deployment and compliance solutions to help organizations protect their domains from email spoofing and abuse.
7. EasyDMARC: EasyDMARC provides DMARC implementation and monitoring solutions to enhance email security and domain reputation.
8. Google: Google Workspace includes DMARC authentication features to help organizations prevent email spoofing and phishing attacks.
9. Red Sift: Red Sift OnDMARC offers DMARC implementation and management solutions to help organizations secure their email domains and prevent spoofing attacks.
10. PowerDMARC: PowerDMARC offers automated DMARC deployment and monitoring solutions to improve email security and domain reputation.
11. Proofpoint: Proofpoint DMARC Analyzer offers visibility and control over email authentication with DMARC reporting and enforcement capabilities.
12. Valimail: Valimail offers DMARC implementation and management solutions to prevent email spoofing and domain impersonation.

Email Encryption Vendors

1. AppRiver: AppRiver provides a robust array of email security solutions aimed at protecting businesses from a wide spectrum of email-borne threats.
2. Barracuda: Barracuda offers email encryption solutions that protect against data leaks and unauthorized access to sensitive information.
3. Cisco: Cisco provides email encryption tools that enable organizations to secure their communications and prevent data breaches.
4. CyberRes: Offers a product called Voltage SecureMail, which provides email encryption software designed to protect sensitive data and ensure regulatory compliance.
5. DataMotion: DataMotion specializes in secure email encryption services that ensure compliance with industry regulations and protect sensitive data.
6. Echoworx: Echoworx delivers email encryption solutions that enable organizations to secure their communications and protect sensitive information.
7. Egress: Egress provides email encryption software that protects sensitive data and facilitates secure communication channels for organizations.
8. GlobalSign: Offers a product called S/MIME & Secure Email that provides S/MIME certificates and email encryption solutions for secure communication and data protection.
9. Intermedia: Intermedia provides email encryption services as part of its secure communication solutions, safeguarding against data breaches and unauthorized access.
10. Mimecast: Mimecast offers email encryption services that protect against data breaches by encrypting emails and attachments, preventing unauthorized access to sensitive information.
11. NeoCertified: Offers a product called SecureEmail which is an email encryption solution that ensures secure communication and compliance with data protection regulations.

12. Proofpoint: Proofpoint delivers email encryption services that safeguard sensitive data and prevent data loss through secure communication channels.
13. Symantec: Symantec is a Broadcom company that provides email encryption solutions that secure sensitive data in transit and at rest, ensuring confidentiality and regulatory compliance.
14. Trend Micro: Trend Micro offers email encryption solutions as part of its comprehensive cybersecurity suite, ensuring data privacy and protection.
15. Trustifi: Trustifi offers a comprehensive suite of email security solutions designed to protect organizations from a wide array of email-based threats.
16. Tutanota: Tutanota offers end-to-end encrypted email services that prioritize user privacy and security.
17. Virtru: Virtru specializes in end-to-end email encryption solutions that enable users to control access to their emails, ensuring privacy and security.
18. Zix: Zix offers email encryption solutions designed to secure sensitive information and comply with data protection regulations.

Phish Testing and Training Vendors

1. Cofense: Cofense specializes in phishing detection and incident response solutions, empowering organizations to detect, analyze, and mitigate phishing threats effectively.
2. Cyber Risk Aware: Cyber Risk Aware specializes in providing targeted security awareness training and simulated phishing campaigns to help organizations strengthen their human firewall against cyber threats.
3. CybeReady: Cybeready provides an automated security awareness platform that delivers personalized training and simulated phishing campaigns to effectively mitigate the risk of phishing attacks.
4. Global Learning Systems: Global Learning Systems delivers engaging security awareness training programs, including simulated phishing simulations and interactive content, to educate employees and foster a culture of security.
5. Huntress: Huntress offers engaging security awareness training programs and simulated phishing campaigns designed to transform employees into cybersecurity champions.
6. InfoSec Institute: InfoSec Institute offers a range of cybersecurity training solutions, including simulated phishing exercises, to empower employees with the knowledge and skills needed to recognize and respond to phishing attacks.
7. Infosec IQ: Infosec IQ offers a versatile security awareness and training platform that includes simulated phishing attacks, interactive modules, and personalized learning paths to address organizations' unique security needs.
8. KnowBe4: KnowBe4 offers a comprehensive platform for security awareness training and simulated phishing attacks, helping organizations educate employees and reduce the risk of falling victim to phishing scams.
9. Lucy Security: Lucy Security offers a comprehensive cybersecurity awareness and training platform, including simulated phishing simulations, security awareness courses, and customizable content.

10. Ninjio: Ninjio provides micro-learning cybersecurity awareness training videos that educate users on real-world cyber threats and empower them to make informed security decisions.
11. Phishing Tackle: Phishing Tackle offers a range of cybersecurity awareness solutions, including simulated phishing attacks and training modules, to help organizations reduce the human risk factor in cybersecurity.
12. PhishingBox: PhishingBox provides an intuitive platform for conducting simulated phishing campaigns and assessing user susceptibility to phishing attacks, enabling organizations to improve their security posture.
13. PhishLabs: PhishLabs delivers managed phishing awareness services, including simulated phishing exercises and training content, to help organizations strengthen their defenses against phishing attacks.
14. Proofpoint: Proofpoint provides interactive training modules and simulated phishing campaigns to educate users and strengthen defenses against social engineering attacks.
15. SANS Security Awareness: SANS Security Awareness provides a wide range of training resources, including simulated phishing exercises and awareness materials developed by cybersecurity experts.
16. Security Mentor: Security Mentor offers a library of interactive security awareness training modules covering various topics, including phishing, to educate employees and reduce security risks.
17. Terranova Security: Terranova Security delivers comprehensive phishing simulation and awareness training solutions to help organizations build a resilient human firewall against cyber threats.
18. Webroot: Webroot Security Awareness Training provides customizable security awareness programs, including simulated phishing campaigns and educational content, to reduce human error and enhance cybersecurity posture.

Secure Email Gateway Vendors

1. Barracuda: Offers a product called Barracuda Email Security Gateway which provides comprehensive email protection against spam, malware, phishing, and data leaks, ensuring secure and reliable email communication.
2. Cisco: Offers cloud-based email security solutions that provide advanced threat protection, data loss prevention, and encryption capabilities to safeguard organizations' email communications.
3. Forcepoint: Forcepoint offers cloud-based email security solutions that provide advanced threat protection, data loss prevention, and encryption capabilities to safeguard organizations' email communications.
4. Fortinet: Offers a product called FortiMail that provides email security appliances and cloud-based solutions that provide advanced threat protection, encryption, and compliance features to secure email communications.
5. Microsoft: Offers Microsoft Defender for Office 365 which provides integrated email security features, including anti-phishing, anti-malware, and URL scanning, to protect against advanced email threats within the Office 365 environment.

6. Mimecast: Mimecast Secure Email Gateway offers cloud-based email security solutions that protect against email-borne threats, provide data loss prevention, and ensure email continuity for organizations.
7. Proofpoint: Proofpoint Email Protection delivers multi-layered email security defenses, including threat intelligence, email authentication, and real-time threat detection, to defend against advanced email threats.
8. SonicWall: SonicWall Email Security delivers comprehensive email protection against spam, phishing, and advanced threats, leveraging multi-layered security defenses and real-time threat intelligence.
9. Sophos: Sophos Email Gateway offers comprehensive email security solutions that protect against phishing, malware, and data loss, leveraging advanced threat intelligence and machine learning algorithms.
10. Symantec: Symantec is a Broadcom company that offers cloud-based and on-premises email security solutions that protect against malware, phishing, and spam, ensuring secure communication for organizations of all sizes.
11. Trellix: Trellix Email Security offers advanced threat protection and real-time threat intelligence to detect and block email-based attacks, including spear-phishing and ransomware threats.
12. Trend Micro: Trend Micro Email Security delivers advanced threat protection, data loss prevention, and encryption capabilities to safeguard organizations against email-based attacks and data breaches.
13. Zix: Zix Email Encryption offers email encryption solutions that secure sensitive information and ensure compliance with regulatory requirements, protecting organizations' email communications from unauthorized access.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations in cybersecurity, artificial intelligence, and sustainability to enterprise teams, government agencies, and commercial vendors.