MVECA Managed Security Services

mveca
miami valley educational computer association

The Miami Valley Educational Computer Association provides a comprehensive suite of security services in the form of a managed service that all of our MVECANet Internet services customers can consume at the current price of $2.50 per student per our approved FY25 Fee Schedule. These services are fully eligible for funding under the new Erate Cybersecurity Pilot Program.

Managed Service Included Components

Palo Alto Next Generation Firewall Services - MVECA employs fully redundant, state of the art, next-generation Palo Alto firewall appliances. These firewalls take advantage of Palo Alto's numerous security features and are constantly updated to prepare for the newest threats. Heuristic-based analysis detects anomalous packet and traffic patterns such as port scans, host sweeps, and denial-of-service (DoS) attacks.

Palo Alto's Malware Protection strategy utilizes WildFire to leverage a global threat intelligence community that covers the network, endpoint, and cloud. Wildfire ensures files are safe by automatically preventing unknown malware variants. WildFire receives protection updates 60X faster with the industry's largest threat intelligence and malware prevention engine. Wildfire analyzes two times more unique malware samples per month than competing sandboxing engines, while inline machine learning immediately stops rapidly changing malware, such as ransomware and fast-moving threats on the firewall — all with no required cloud analysis, no damage to content and no loss of user productivity.

MVECA’s Palo Alto implementation is protected by platinum level support services to ensure 24/7 access to technical experts to provide advanced assistance at best-in-class response times. Security assurance for assisted first responses, expedited 15-minute response time for high severity issues, and access to Palo Alto's Senior Engineers ensures that Platinum Support meets the highest standards of customer service.

Palo Alto Panorama provides a centralized security rule base for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. App-ID technology-based rules, dynamic security updates, and rule usage analysis all help to reduce administrative workload and improve overall security posture.

Palo Alto GlobalProtect VPN provides Identity-Based access control to simplify remote access for employees. GlobalProtect assesses devices’ health and security posture before connecting, preventing compromised hosts from connecting to the network while allowing the workforce to stay mobile. It extends Palo Alto's next-generation security platform and applies its capabilities to understand application use, associate traffic with users and devices, and enforce existing security policies.

AgileBlue Advanced Cyber Security Platform for SOC/SIEM – 24/7 expert analysts, comprehensive security protection and an AI-powered SecOps platform for Security Information and Event Management (SIEM). AgileBlue is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. AgileBlue's SIEM surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response.

Apptega for Compliance Assessment – MVECA utilizes the Apptega Cybersecurity Compliance platform, which provides a comprehensive way to manage compliance with security frameworks including NIST 800-53, SOC 1, CMMC, and many more. From risk identification to control validation, Apptega's tools simplify the process of building, maintaining, and reporting on our security posture.

Trustwave MailMarshal – Email continues to be the number one vector for threat actors to attack organizations. Trustwave's MailMarshal utilizes machine learning phishing engines to detect a wide variety of threats including phishing, malware, BEC, and spam. MailMarshal handles the containment, blocking, and notification of threatening mail for on-prem mail servers. MailMarshal gives visibility and contextual insight on the always-evolving landscape of email-based threats.

Securly Content Filtering – Securly Filter is a cloud-based web filtering solution developed specifically to address the needs of K-12. Filter supports any device and operating system to manage student devices both on and off network. Filter goes beyond basic web-filtering by leveraging user-level reporting, custom policies, seamless integration with other Securly services, and real-time insight into your school's usage.

MS-ISAC and CIS Services – MVECA coordinates directly with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Center for Internet Security (CIS) to improve the overall cybersecurity posture of our organization and our members. MS-ISAC provides a number of services including the Cyber Incident Response Team (CIRT), Cybersecurity Advisory Services Program (CASP), Cyber Threat Intelligence (CTI), and Cybersecurity Advisory mailing lists, and access to CIS SecureSuite integrated cybersecurity resources. Additionally, MS-ISAC offers a host of information sharing, cybersecurity awareness, and education resources. CIS provides vulnerability management solutions for networks and web applications, as well as penetration testing and phishing engagements. These services include network discovery and mapping, vulnerability assessment reporting, testing vulnerabilities for false-positives, identifying high-value assets, prioritizing vulnerabilities based on risk, and conducting custom phishing simulations.

OARNET – The Ohio Academic Resources Network (OARNet) provides large-scale DDoS Mitigation services. OARnet offers two levels of DDoS mitigation protection. First, on-premise custom filters are developed by OARnet engineers to protect again common DDoS attack vectors, serving as a first line of defense. Second, cloud-based DDoS mitigation utilizes a carrier service to block large-scale attacks and includes a scrubbing service to remove bad traffic and forward clean traffic to the client. OARnet's unique DDoS mitigation service combines both on-premise and cloud-based to protect the network and minimize service disruptions.

Cisco DUO for Hosted Applications and Network Security - Duo is a two-factor authentication solution that helps organizations boost security by verifying user identity, establishing device trust, and providing a secure connection to company networks and applications. MVECA utilizes DUO in conjunction with GlobalProtect, network and Active Directory authentication, and for various locally hosted applications.

Around the Clock Support – MVECA is available when you need us, offering both daytime (937-767-1468, helpnetwork@mveca.org) and after hours (937-767-8325) contact information to our clients.

Additional Cybersecurity Products Available Through MVECA – Call or email for quote

Sophos Intercept X with MDR – Sophos Intercept X with Managed Detection and Response (MDR) is a fully managed 24/7 service that detects and responds to cyberattacks targeting computers, servers, networks, and more. Sophos delivers unparalleled protection against advanced attacks, responding to threats and utilizing hundreds of experts backed by seven SOCs to accelerate human-led responses. Sophos MDR analysts perform proactive threat hunts to identify attacker behaviors that only a human can detect and rapidly eliminate threats that tools alone can't stop.

Techguard InfoSec Cybersecurity Awareness Training – With the widespread prevalence of phishing, social engineering, and fraud, Techguard works to bolster the "human firewall" with award-winning security awareness training & phishing simulations that reduce cybersecurity events with simulations and phishing templates, reinforce cyber security behaviors with industry and role-based training, and strengthen cybersecurity culture while meeting compliance requirements.

Abnormal Security – Abnormal Security is a cloud-based solution offering comprehensive email protection against attacks that exploit human behavior, including phishing, social engineering, and account takeovers. Abnormal Security offers a fundamentally different approach to email security by using behavioral AI and ML models to stop the full spectrum of email attacks. Automation reduces manual work by up to 95%, allowing organizations to eliminate costly and redundant secure email gateways. The API architecture makes deployment a painless process.

Cisco DUO for school district deployments – Duo multi-factor authentication protects your organization's data at every access attempt, from any device, and from any location. It verifies user trust, establishes device trust, and provides secure access to company apps and networks—from wherever users are logging in.

Cyber Security Framework Deployment Program – Comprehensive program providing:

- Personalized Gap and Risk Assessment to understand your current data security strengths and areas for improvement through a tailored assessment.
- Deep Dive into Controls: Gain a thorough understanding of essential data security controls to protect your organization's information.
- Incident Response and Business Continuity Planning: Participate in workshops designed to prepare you for potential data breaches and ensure continuity of operations.

If you have any questions or need pricing on products listed above, please contact Thor Sage, MVECA Executive Director (sage@mveca.org, 937-767-1468 x3101).