Tailored Solutions Aligned with the FCC's Cybersecurity Pilot Program

MGT

As a selected participant in the Cybersecurity Pilot Program, you are evaluating your cybersecurity needs and determining the best use of funding. Partner with MGT for end-to-end cybersecurity solutions—including assessments, technology infrastructure, and managed services—most of which qualify as eligible services under the Cybersecurity Pilot Program. With a team of 350+ certified engineers and decades of E-rate expertise, we identify vulnerabilities, recommend and then implement solutions that strengthen your cybersecurity posture, ensuring better protection for your schools and libraries.

MGT Highlights

- Portfolio of eligible cybersecurity solutions

- Network and security assessments to identify security weaknesses

- Pre-sales design support to recommend solutions

- Decades of E-Rate expertise

- 350+ engineers with network & security expertise

- Comprehensive technology & services solution

Cybersecurity Pilot Program

- The Federal Communications Commission (FCC) has launched the Schools and Libraries Cybersecurity Pilot program to provide $200 million to selected schools and libraries to defray the costs of cybersecurity equipment and services.

- The FCC selected 707 participants on 1-16-25. Congratulations to the selected participants!

- Form 470's are available effective 1-17-25

- Form 471 Filing window is 3-18-25 to 9-15-25

- Eligible services include a variety of network and security infrastructue as well as managed services that can enhance the cybersecurity posture of K-12 schools, libraries, and consortia. See the back page for a list of eligible MGT solutions and managed services.

Selected Participant Next Steps

1. **Start with an Assessment**
   Start with a cybersecurity assessment to identify breach points and weaknesess with current infrastructure.

2. **Review Recommendations**
   After evaluating your network and security infrastructure, our engineers will recommend a technology and managed services solution. We can help identify which technology solutions are eligible within the Cybersecurity Pilot Program.

3. **Follow FCC Process**
   Follow the FCC steps for soliciting bids and procuring desired cybersecurity services and equipment.

SOURCES: fcc.gov/cybersecurity-pilot-program

Cybersecurity Pilot Program - MGT Eligible Services

FCC Category	Equipment or Service	MGT Solution	Eligible
Advanced/ Next-Generation Firewalls	Advanced Threat Detection and Prevention	Element Management (Firewall / ATP)	Yes
	AI/ML Threat Detection and Response	Managed SOC, SIEM or MDR Services	Yes
	Application Awareness & Control	Element Management (Firewall)	Yes
	Cloud-Delivered Threat Intelligence	Managed SOC, MDR	Yes
	Comprehensive Network Visibility Software-defined Firewalls	Element Management (Firewall)	Yes
	Deep Packet Inspection (DPI)	Element Management (Firewall)	Yes
	Distributed-Denial-of-Service (DDoS) Protection	DDOS Monitoring as a Service	Yes
	Firewall as a Service (FWaaS)	Firewall as a Service	Yes
	Integrated Intrusion Prevention Systems (IPS)	Element Management (Firewall / IDS)	Yes
	Internet of Things (IoT) Security	Element Management (Firewall)	Yes
	Intrusion Prevention/Detection	Element Management (Firewall / IPS)	Yes
	Malware Detection	Endpoint Monitoring / Management (EDR)	Yes
	Network Segmentation	Element Management (Firewall)	Yes
	Patch Management Systems	Patch Management as a Service	Yes
	VPN	Element Management (Firewall / VPN Concentrator)	Yes
Endpoint Protection	Anti-Malware	Endpoint Monitoring / Management (EDR)	Yes
	Anti-Ransomware	Endpoint Monitoring / Management (EDR)	Yes
	Anti-Spam	Endpoint Monitoring / Management (EDR)	Yes
	Anti-Virus	Endpoint Monitoring / Management (EDR)	Yes
	Endpoint Detection & Response (EDR)	Endpoint Monitoring / Management (EDR)	Yes
	Extended Detection & Response (XDR)	Endpoint Monitoring / Management (EDR)	Yes
	Insider and Privilege Misuse	Endpoint Monitoring / Management (EDR)	Yes
	Privileged Access Management	Element Management (PAM)	Yes
	Secure Sockets Layer (SSL) Inspections	Element Management (Firewall)	Yes
	Target Intrusions	Endpoint Monitoring / Management (EDR)	Yes
	Web Application Hacking	Element Management (Firewall / WAF)	Yes
Identity Protection and Authentication	Active Countermeasure Tools	Element Management (Firewall)	Yes
	Cloud Application Protection	Element Management (Firewall)	Yes
	Cloud Services	Element Management (Firewalls / Internet Gateways)	Yes
	Credential Stuffing	Element Management (EDR / MFR / WAF)	Yes
	Content Blocking and Filtering/URL Filtering	Element Management (Firewall)	Yes
	Customer Portal Services	Element Management Services	Yes
	Digital Identity Tools	Element Management (MFA / SSO / PAM)	Yes
	Distributed-Denial-of-Service (DDoS) Protection	DDOS Monitoring as a Service	Yes
	DNS/DNS-Layer Security, Blocking, and Filtering	Element Management (Firewall)	Yes
	Email and Web Security	Element Management (Email Security)	Yes
	Identity Governance & Technologies	Not Available	Yes
	Intrusion Detection Systems (IDS)	Element Management (Firewall / IDS)	Yes
	Logging Practices / Event Logging	SIEM or MDR Services	Yes
	Network Access Control	Element Management (NAC) or NAC as a Service	Yes
	Offsite/Immutable back-ups	Business Continuity / Disaster Recovery as a Service	Yes
	MFA/Phishing-Resistant MFA	Element Management (MFA / SSO)	Yes
	Patching	Patch Management as a Service	Yes
	Password Spraying	SIEM or MDR Services	Yes
	Privileged Identity Management	Element Management (PIM / SSO)	Yes
	Products with TPM Chips	Element Management Services	Yes
	Secure Access Service Edge (SASE)	Element Management (SASE)	Yes
	Secure-By-Design Equipment and Services	Element Management Services	Yes
	Security Information and Event Management (SIEM)	SIEM or MDR Services	Yes
	Security Updates	Element Management Services	Yes
	Single Sign-On (SSO)	Element Management (SAML)	Yes
	Trusted Platform Module (TPM)	Element Management Services	Yes
	Web Content Controls	Element Management (Firewall / WAF)	Yes
	Wireless Access Controllers	Element Management (WLAN) or WLAN as a Service	Yes
	Zero Trust Architecture	Element Management (Firewall) or Firewall as a Service	Yes
Monitoring, Detection, and Response	Advanced Attack Surface Management & Asset Management	Managed SOC, SIEM or MDR Services	Yes
	Bug Bounty Solutions & Services	Penetration Testing Services	Yes
	Compliance Assessment	Professional and Consulting Services	Yes
	Dark Web Scanning	Network and Security Assessment Services	Yes
	Data Loss Prevention	Element Management (Firewall) or Firewall as a Service	Yes
	Internal/External Vulnerability Scanning	Vulnerability Management as a Service	Yes
	Network/Device Monitoring & Response	Monitoring and Network Performance Management	Yes
	Network Security Audit	Network and Security Assessment Services	Yes
	Network Traffic Analysis	Element Management Services	Yes
	Managed Detection & Response (MDR)	Managed SOC, SIEM or MDR Services	Yes
	Maturity Models	Network and Security Assessment Services	Yes
	Network Detection Response (NDR)	Managed SOC, SIEM or MDR Services	Yes
	Penetration Testing	Penetration Testing Services	Yes
	Security Operations Center (SOC) for Around the Clock (24/7/365) Monitoring, Detection, and Response	SOC as a Service	Yes
	Threat Hunting/Updates and Threat Intelligence	SOC as a Service	Yes
	Vulnerability Management	Vulnerability Management as a Service	Yes