Edge secure

CYBERSECURITY HEALTH CHECK PROGRAM

A proactive, standards based program to protect your organization from risks before cyber attacks and security breaches occur.

WHAT ARE THE GOALS OF A CYBERSECURITY PROGRAM?

The goal of a cybersecurity program is to identify the risk exposure of cyber assets in an enterprise. Periodic assessments are the basis of a responsible approach to cybersecurity, to determine security readiness and measure progress over time.

A PROACTIVE SOLUTION LED BY CYBERSECURITY EXPERTS

The Edge Cybersecurity Health Check Program generates actionable and concise cybersecurity reports, presented on a monthly basis. Each month, a cybersecurity assessment report will provide a snapshot of network security at the current point in time, giving you actionable intelligence on an ongoing basis to remediate new vulnerabilities and exploits as they arise.

Our subscription-based cybersecurity approach provides:

Regular monthly assessments to identify timely vulnerabilities and improve cybersecurity posture over time.

An assessment protocol based on NIST Cybersecurity Framework* best practices.

A comprehensive, ongoing network infrastructure audit, including hardware, software, and related components.

Access to our assessment team's in-depth knowledge of cybersecurity frameworks and strategies.

Risk mitigation reporting, analysis, and prioritization.

With Edge's nonprofit approach, we offer the subscription-based service for an affordable $6000/year which includes 12 monthly assessments.

Periodically assessing network security is a crucial part of a business's cyber security plan. Our team's in-depth knowledge of technology and security techniques help to proactively identify and prevent potential risks that may adversely impact your organization's ability to operate safely and security.

READY TO TAKE PROACTIVE CONTROL OF YOUR CYBERSECURITY NEEDS? CONTACT INFO@NJEDGE.NET.

* All facets of the Cybersecurity Health Check Program comply with the NIST Cybersecurity Framework (CSF) which categorically creates five concurrent and continuous reference functions - Identify, Protect, Detect, Respond and Recover. Each category maintains a strategic view of the life cycle within an organization's cybersecurity program. The operation, prioritization, measuring and monitoring are implemented using the Center for Internet Security - Critical Security Controls (CSC) to map directly to the CSF core requirements. Collectively these methods formulate the strategy to meet many standards such as: NIST SP 800-53, ISO/IEC 27001:2013, CIS CSC, HIPPA, PCI DSS 3.0, COBIT 5, ITIL.

STRATEGIC PARTNERS

CISCO Cisco Umbrella

COMODO
Creating Trust Online®

CYBERHAT

KnowBe4
Human error. Conquered.

splunk>

EDGESECURE ALSO BENEFITS FROM ALLIANCES WITH THE FOLLOWING INDUSTRY PARTNERS:

f5®

FORESCOUT

Qualys.

Secureworks®

KnowBe4
Human error. Conquered.

paloalto NETWORKS

Edge also offers access to a Virtual Chief Information Security Office, advanced security consulting, and access to affordable procurement for industry-leading security vendors. We can assist with any necessary security remediation, including:

- Cybersecurity Policy and Procedure Consultation
- Cybersecurity Policy Writing
- Privacy and Compliance
- Ransomware and Malware Protection Strategy
- Remote Work Security Consultation
- Endpoint (Laptop, Desktop, and Mobile) Security
- Disaster Recovery and Business Continuity Planning
- Ethical Hacking
- Wireless Penetration Testing
- Managed Security Operations Center
- Phishing and Social Engineering (User Awareness) Training
- Firewall Auditing
- Overall Management of Network Mapping
- Network Port and Service Scanning
- Vulnerability Assessment on Hosts
- Risk Modeling