NetGuard® Plus Cyber Glossary

The following Cyber Glossary is provided to assist you in completing your application correctly and completely.

Endpoint Detection and Response (EDR), also known as endpoint *threat* detection and response, centrally collects and analyzes comprehensive endpoint data across your entire organization to provide a full picture of potential threats.

> **Common Providers:** Carbon Black Cloud; Crowdstrike Falcon Insight; SentinelOne; Windows Defender Endpoint

Immutable backups are backup files that are fixed, unchangeable, and can be deployed to production servers immediately in case of ransomware attacks or other data loss.

Multi-Factor Authentication (MFA) is an electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print). MFA for remote email access can be enabled through most email providers.

> **Common MFA providers for remote network access:** Okta; Duo; LastPass; OneLogin; and Auth0.

Next-Generation Anti-Virus (NGAV) is software that uses predictive analytics driven by machine learning and artificial intelligence and combines with threat intelligence to detect and prevent malware and fileless non-malware attacks, identify malicious behavior, and respond to new and emerging threats that previously went undetected. For purposes of completing this application, NGAV refers to anti-virus protection that focuses on detecting and preventing malware on each individual endpoint. If your organization has a NGAV solution and you are centrally monitoring and analyzing all endpoint activity, please indicate that you have NGAV & EDR on the application.

> **Common Providers:** BitDefender™; Carbon Black; CrowdStrike Falcon Prevent; SentinelOne; Sophos; Symantec

Offline/Air-gapped backup solution refers to a backup and recovery solution in which one copy of your organization's data is offline (i.e., disconnected) and cannot be accessed. If a file or system of files has no connection to the internet or a LAN, it can't be remotely hacked or corrupted.

Personally Identifiable Information (PII) is information that can be used to determine, distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, including, but not limited to, financial account numbers, security codes, personal identification numbers (PINs), credit and debit card numbers, medical or healthcare information, social security numbers, driver's license numbers, addresses, passwords, and any other non-public information as defined in Privacy Regulations.

Protected Health Information (PHI) is any health information that can identify an individual. PHI includes demographic identifiers, in medical records, like names, phone numbers, emails, and biometric information like fingerprints, voiceprints, genetic information, and facial images.

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server.

Remote Desktop Web (RDWeb), also known as Microsoft Remote Desktop Web Access, is a service that provides remote access to corporate resources through a web portal. Resources may include remote desktop access and other applications published on the portal.

Remote Monitoring and Management (RMM) tools allow IT providers to remotely manage and monitor network environments. RMM tools may include remote access, patch management, and reporting functionalities.

Common Providers: ConnectWise and ManageEngine

Virtual Private Network (VPN) encrypts connections between a remote device and an internal network. VPNs are utilized to allow systems from outside the network to connect to internal resources.

Common Providers: Fortnet, Cisco, and Palo Alto VPN Appliances