TOKIO MARINE HCC

Cyber Glossary

TO ASSIST YOU IN COMPLETING YOUR APPLICATION

Please refer to the terms that apply to your specific application.

Clientless SSL VPN (Web VPN) simplifies user authentication and network connection by allowing users to login over a webpage, from any device, managed or unmanaged, without installing a VPN client on the user's device. While extremely convenient, the login panels are easily discoverable by threat actors and prone to unauthorized logins due to the lack of a VPN client.

Cloud-Based Backup Solution is a service that stores copies of your data on remote third-party servers.

Endpoint Detection and Response (EDR) 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 and unchangeable, allowing immediate deployment in the event of ransomware attacks or other data loss.

Managed Detection and Response (MDR) is a holistic cybersecurity approach that protects against cyber threats. MDR service providers incorporate multiple security solutions, including EDR, NDR, DLP and other tools leveraged by a 24/7 SOC (Security Operation Center) to actively monitor, detect, and remediate threats by analyzing telemetry from multiple sources and leveraging threat intelligence data. Unlike standalone EDR or a self-managed XDR solution, an MDR provider fully manages all cybersecurity related issues.

Multi-Factor Authentication (MFA) is an electronic authentication requiring two or more forms of verification, such as knowledge (e.g., password), possession (e.g., phone or key), and inherence (e.g., FaceID or hand print).

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

Next-Generation Anti-Virus (NGAV) is endpoint antivirus software that leverages predictive analytics driven by machine learning and artificial intelligence 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.

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

Offline/Air-Gapped Backup Solution is a backup and recovery solution in which your data is stored 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, including, but is not limited to, financial account numbers, security codes, personal identification numbers (PINs), credit and debit card numbers, social security numbers, driver's license numbers, addresses, passwords, and any other non-public information as defined in the policy form.

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

Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol enabling users to connect remotely to another computer via a graphical interface. 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, including 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, including 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, securing external access to internal systems.

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