Evolve MGA
Security Controls Glossary

Application whitelisting
A security solution that allows organizations to specify what software is allowed to run on their systems, in order to prevent any nonwhitelisted processes or applications from running.

Antivirus
A product that can detect and prevent malicious software on computers, laptops and other tech devices.

Asset inventory
A list of all IT hardware and devices an entity owns, operates or manages. Such lists are typically used to assess the data being held and security measures in place on all devices.

Brute force attack
A method whereby threat actors submit multiple password attempts in rapid succession until they successfully gain entry into business networks.

Cloud
A virtual space on the internet used for storing digital resources instead of on local computer networks. Clouds can be public, private or hybrid, each with pros and cons. Examples include Google Drive, Apple iCloud, Netflix, Amazon Web Services (AWS), Dropbox and Microsoft OneDrive.

Custom threat intelligence
The collection and analysis of data from open source intelligence (OSINT) and dark web sources to provide organizations with intelligence on cyber threats and cyber threat actors pertinent to them.

Cyber
Relates to or characteristic of the culture of computers, information technology, and virtual reality

Cyber attack
An unauthorized attempt by hackers to damage, destroy, alter or exploit a computer network, system, or employees.

Cybercrime
Extortion by phishing, ransom attacks, social engineering or losses caused by malware or DDOS.

Cyber event
Actual or suspected unauthorized system access, electronic attack or privacy breach.

Cyber insurance
Cyber insurance exists to help protect businesses against the threat of cybercrime.

Cyber security
The technologies, processes and controls used to protect and support information technology (IT).

Cyber threat analysis
The dedicated team typically provided by a cyber insurer to help detect, prevent and stop cyber attacks from affecting businesses before they fall victim.

Database encryption
Where sensitive data is encrypted while it is stored in databases. If implemented correctly, this can stop malicious actors from being able to read sensitive data if they gain access to a database.

Data loss prevention
Software that can identify if sensitive data is being exfiltrated from a network or computer system.

DDoS mitigation
Hardware or cloud based solutions used to filter out malicious traffic associated with a Distributed Denial of Service (DDoS) attack, while allowing legitimate users to continue to access an entity's website or web-based services.

DMARC
An internet protocol used to combat email spoofing – a technique used by hackers in phishing campaigns.

DNS filtering
A specific technique to block access to known bad IP addresses by users on your network.

Email filtering
Software used to scan an organization's inbound and outbound email messages and place them into different categories, with the aim of filtering out spam and other malicious content.

Employee awareness
Training programmes designed to increase employees' security awareness. For example, programmes can focus on how to identify potential phishing emails.

End user device
Any computer or mobile device used by the end customer.

Endpoint protection
Software installed on individual computers (endpoints) that uses behavioral and signature based analysis to identify and stop malware infections.

Extortion
A crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack.

Firewall
Hardware solutions used to control and monitor network traffic between two points using predefined parameters.

Incident response
An organized approach involving technical, legal and claims expertise to address and remediate a cyber incident. These are typically offered by a cyber insurer as the full suite claims service.

Incident response plan
Action plans for dealing with cyber incidents to help guide an organization's decision-making process and return it to a normal operating state as quickly as possible.

Intrusion detection system
A security solution that monitors activity on computer systems or networks and generates alerts when signs of compromise by malicious actors are detected.

Malware
Includes viruses, trojans, worms or any code or content that could have an adverse impact on organizations or individuals.

Managed service provider
A third party organization that provides a range of IT services, including networking, infrastructure and IT security, as well as technical support and IT administration.

Mobile device encryption
Encryption involves scrambling data using cryptographic techniques so that it can only be read by someone with a special key. When encryption is enabled, a device's hard drive will be encrypted while the device is locked, with the user's passcode or password acting as the special key.

Multi-factor authentication (MFA/2FA)
Where a user authenticates themselves through two different means when remotely logging into a computer system or web based service. Typically a password and a passcode generated by a physical token device or software are used as the two factors.

Network
Two or more computers linked to share electronic communications, resources and file exchanges.

Network monitoring
A system, utilising software, hardware or a combination of the two, that constantly monitors an organization's network for performance and security issues.

Next-generation firewalls
Software or hardware solutions that combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems and anti-virus.

Patching
Applying updates to software to improve security and/or enhance functionality.

Penetration test (pen test)
Authorized simulated attacks against an organization to test its cyber security defenses. May also be referred to as ethical hacking or red team exercises.

Perimeter firewalls
Hardware solutions used to control and monitor network traffic between two points according to predefined parameters.

Phishing
Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransom attacks
The act of using malicious software to freeze or encrypt a victims data until they pay the requested demand.

Ransomware
Malicious software that freezes data so the attacker can threaten to publish it on a public domain. Or render systems and data unusable until the victim makes a payment.

Response app
A proprietary app offered by cyber insurers (Evolve) to allow for threat intelligence alerts notifying policyholders of a potential vulnerability or compromise.

Remote desktop protocol (RDP)
RDP is a proprietary Microsoft protocol that allows a user to access their desktop and computing resources remotely from another computer. It is also sometimes referred to as Terminal Services.

Security info and event management (SIEM)
System used to aggregate, correlate and analyze network security information – including messages, logs and alerts – generated by different security solutions across a network.

Security operations centre (SOC)
A facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. SOC's can be internal and run by the organization themselves or outsourced to a third party.

Social engineering
Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Supply chain partner
A third party who businesses depend on to operate, with services including but not limited to hosting, platforms, software or file storage.

System failure
Sudden, unexpected and continuous downtime of computer systems which renders them incapable of supporting normal business functions.

Threat actor
An individual, or group of individuals, intending to maliciously cause harm to a company's intangible assets and digital operations.

Threat intelligence
The collection and analyzis of data from open source intelligence and dark web sources to provide organizations with intelligence on cyber threats pertinent to them.

Trojan
A type of malware or virus disguised as legitimate software that is used to hack into the victim's computer.

Virtual private network (VPN)
A VPN is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. Most commonly used to provide a secure remote connection to an organization's network.

Vulnerability
A weakness or flaw in software, systems or processes. A threat actor may seek to exploit a vulnerability to gain unauthorized access to a system.

Vulnerability scans
Automated tests designed to probe computer systems or networks for the presence of known vulnerabilities that would allow malicious actors to gain access to a system.

Web application firewall
Protects web facing servers and the applications they run from intrusion or malicious use by inspecting and blocking harmful requests and malicious internet traffic.

Web content filtering
The filtering of certain web pages or web services that are deemed to pose a potential security threat to an organization. For example, known malicious websites are typically blocked through some form of web content filtering.

Zero-day
Vulnerabilities that are discovered by threat actors before vendors become aware of it. These can then be exploited before patch updates are made available to businesses.