5.Ten types of cybersecurity Many types of cybersecurity are employed to protect digital systems from malicious and accidental threats.At its core, zero trust is based on several practices, including: Continuously verifying users' identity Establishing and enforcing the principle of least privilege for access, granting only the access that is explicitly required for a user to perform a job and only for as long as that access is required Micro segmenting networks Trusting no users (i.e., internal or external) 6.Many of the solutions within each of these types of cybersecurity are used across subcategories, such as: Anti-malware software Antivirus systems Backup Data loss prevention (DLP) Enterprise mobility management Encryption Endpoint detection and response (EDR) Enterprise mobility management (EMM) Firewalls Identity and access management (IAM) Intrusion detection and prevention system (IDPS) Mobile application management (MAM) Multi-factor authentication Network access control (NAC) Next-generation firewall (NGFW) Secure access service edge (SASE) Secure email gateways (SEG) Security information and event management (SIEM) 17 Security orchestration, automation, and response (SOAR) User and entity behavior analytics (UEBA) Virtual private networks (VPNs) Web application firewalls (WAFs) 7.Critical infrastructure security Special security processes and types of cybersecurity solutions are used to protect the networks, applications, systems, and digital assets depended on by critical infrastructure organizations (e.g., communications, dams, energy, public sector, and transportation).1.2.3.4.5.6.7.8.9.10.

Summarized by © lakhasly.com