Disclosures

The views of John Blank, PhD are not necessarily the views of Zacks Investment Research. Past performance is no guarantee of future results. Inherent in any investment is the potential for loss. This material is being provided for informational purposes only and nothing herein constitutes investment, legal, accounting or tax advice, or a recommendation to buy, sell or hold a security. No recommendation or advice is being given as to whether any investment is suitable for a particular investor. It should not be assumed that any investments in securities, companies, sectors or markets identified and described were or will be profitable. All information is current as of the date herein and is subject to change without notice. Any views or opinions expressed may not reflect those of the firm as a whole. Zacks Investment Research is not a licensed securities dealer, broker or US investment adviser or investment bank.

Cybersecurity Stocks 2025
A Critical Info Tech Group

Part One: Tables and Charts, Laying Out the Cybersecurity Industry Narrative
Part Two: Top Cybersecurity Stocks, for Four Style Classes

Presented by:

John Blank, PhD
Zacks Chief Equity Strategist and Economist

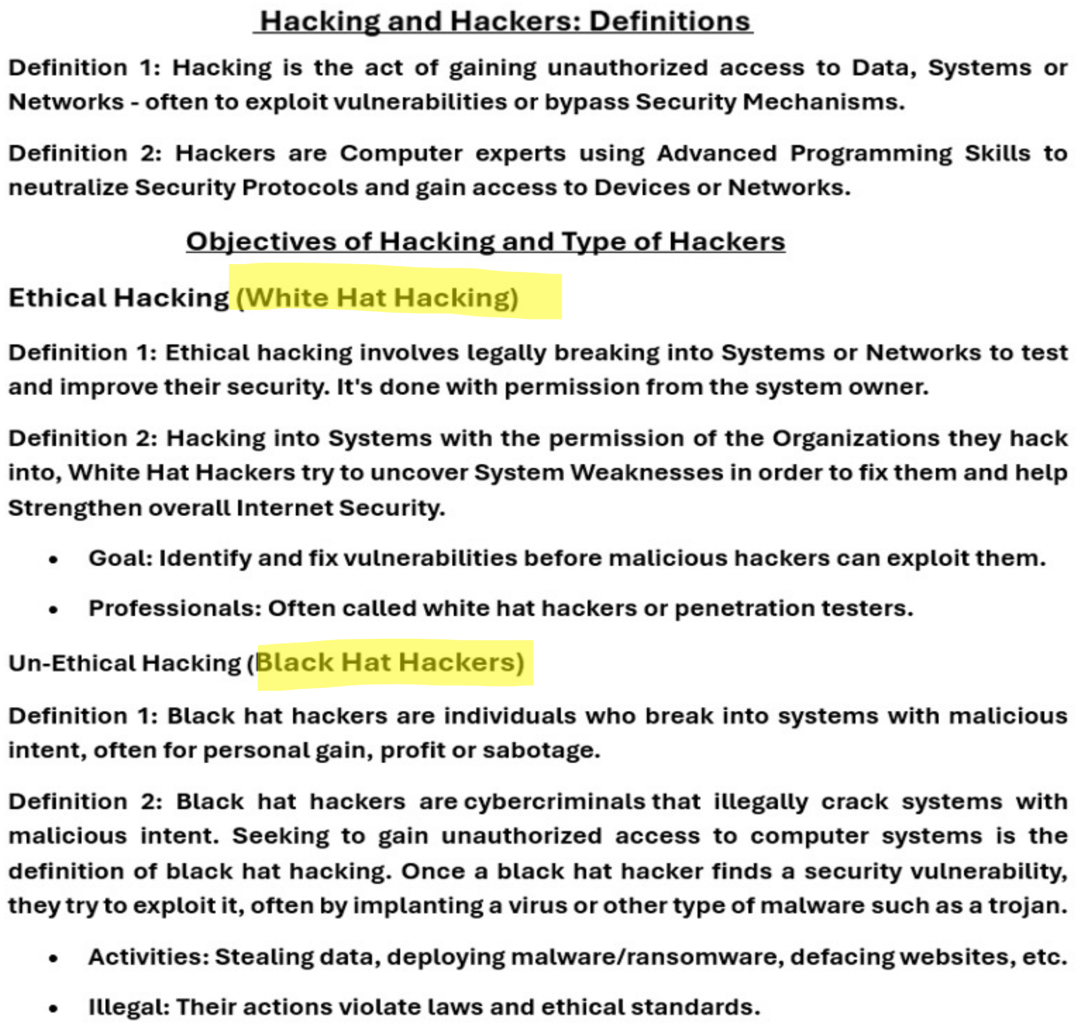
07/28/2025

This is useful information for traders and investors in these stocks

1. Tables and Charts, Laying Out the Cybersecurity Industry Narrative

Hacking and Hackers: Definitions

Objectives and Different Types of Hackers



Hacking and Hackers: Definitions

Definition 1: Hacking is the act of gaining unauthorized access to Data, Systems or Networks - often to exploit vulnerabilities or bypass Security Mechanisms.

Definition 2: Hackers are Computer experts using Advanced Programming Skills to neutralize Security Protocols and gain access to Devices or Networks.

Objectives of Hacking and Type of Hackers

Ethical Hacking (White Hat Hacking)

Definition 1: Ethical hacking involves legally breaking into Systems or Networks to test and improve their security. It's done with permission from the system owner.

Definition 2: Hacking into Systems with the permission of the Organizations they hack into, White Hat Hackers try to uncover System Weaknesses in order to fix them and help Strengthen overall Internet Security.

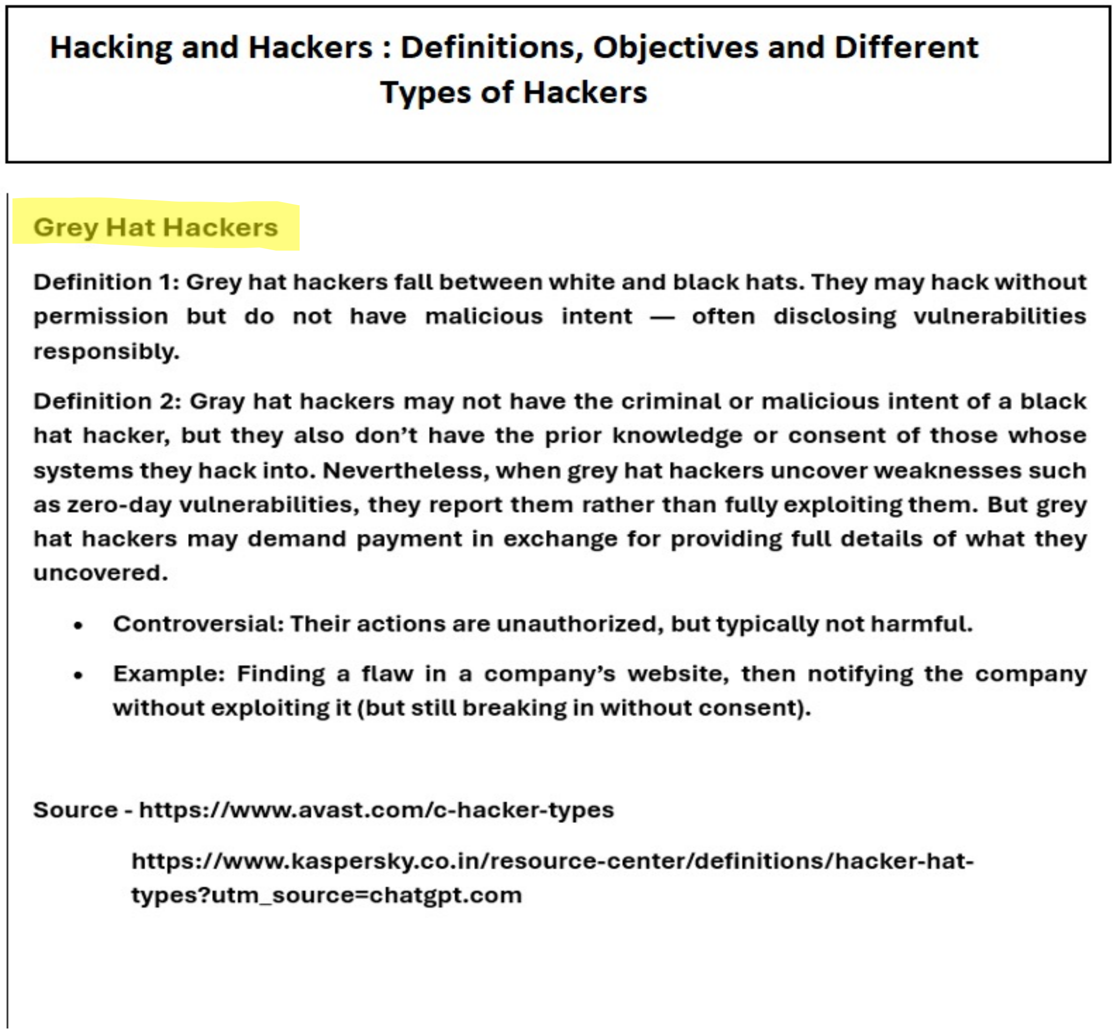
- **Goal: Identify and fix vulnerabilities before malicious hackers can exploit them.**
- **Professionals: Often called white hat hackers or penetration testers.**

Un-Ethical Hacking (Black Hat Hackers)

Definition 1: Black hat hackers are individuals who break into systems with malicious intent, often for personal gain, profit or sabotage.

Definition 2: Black hat hackers are cybercriminals that illegally crack systems with malicious intent. Seeking to gain unauthorized access to computer systems is the definition of black hat hacking. Once a black hat hacker finds a security vulnerability, they try to exploit it, often by implanting a virus or other type of malware such as a trojan.

- **Activities: Stealing data, deploying malware/ransomware, defacing websites, etc.**
- **Illegal: Their actions violate laws and ethical standards.**



Hacking and Hackers : Definitions, Objectives and Different Types of Hackers

Grey Hat Hackers

Definition 1: Grey hat hackers fall between white and black hats. They may hack without permission but do not have malicious intent — often disclosing vulnerabilities responsibly.

Definition 2: Gray hat hackers may not have the criminal or malicious intent of a black hat hacker, but they also don't have the prior knowledge or consent of those whose systems they hack into. Nevertheless, when grey hat hackers uncover weaknesses such as zero-day vulnerabilities, they report them rather than fully exploiting them. But grey hat hackers may demand payment in exchange for providing full details of what they uncovered.

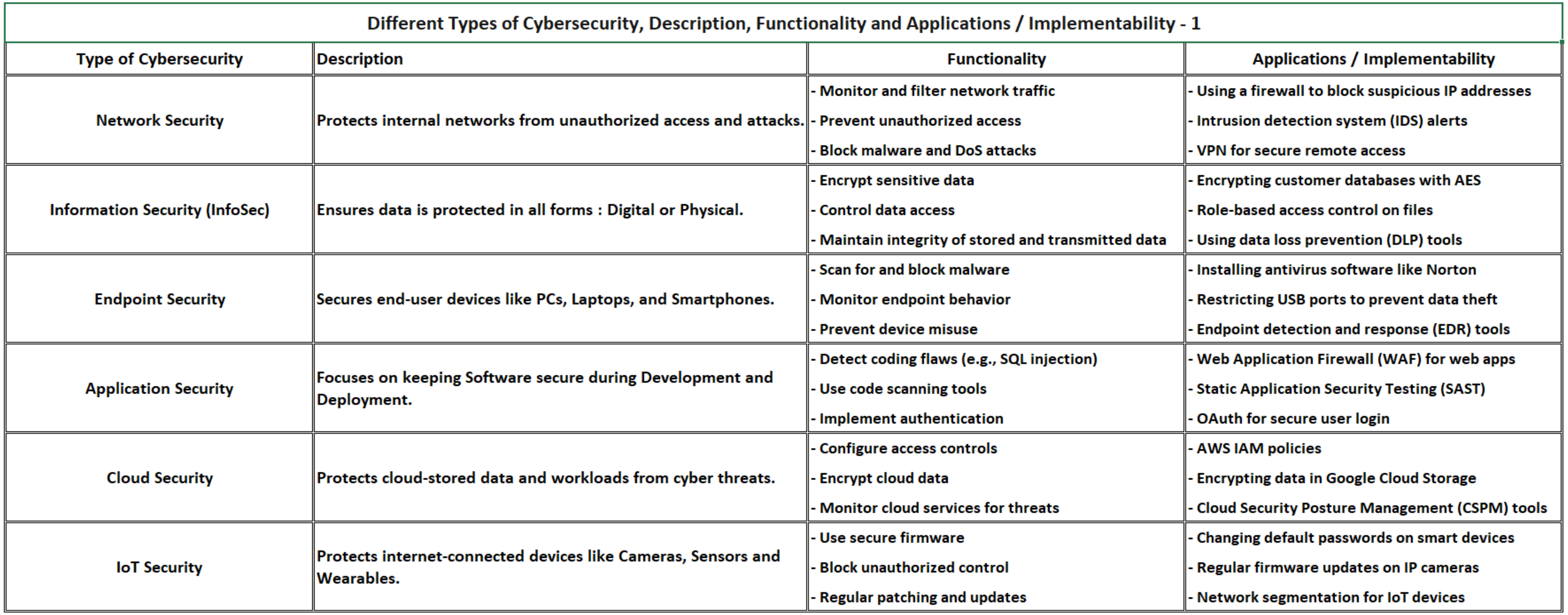
- **Controversial: Their actions are unauthorized, but typically not harmful.**
- **Example: Finding a flaw in a company's website, then notifying the company without exploiting it (but still breaking in without consent).**

Source - https://www.avast.com/c-hacker-types

https://www.kaspersky.co.in/resource-center/definitions/hacker-hat-types?utm_source=chatgpt.com

Different Types of Cybersecurity, Descriptions, Functionality, and Applications/Implement-ability - 1

What is Cybersecurity?



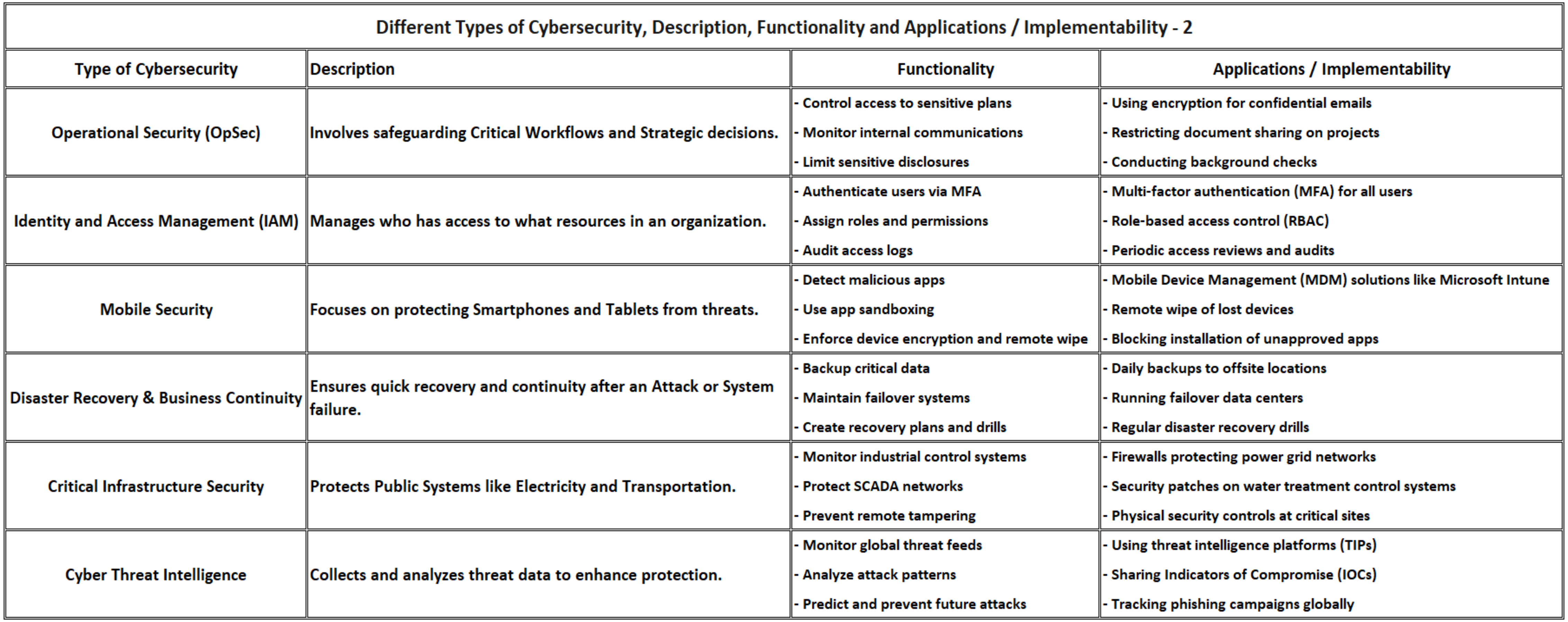
Different Types of Cybersecurity, Description, Functionality and Applications / Implementability - 1

Type of Cybersecurity	Description	Functionality	Applications / Implementability
Network Security	Protects internal networks from unauthorized access and attacks.	- Monitor and filter network traffic - Prevent unauthorized access - Block malware and DoS attacks	- Using a firewall to block suspicious IP addresses - Intrusion detection system (IDS) alerts - VPN for secure remote access
Information Security (InfoSec)	Ensures data is protected in all forms : Digital or Physical.	- Encrypt sensitive data - Control data access - Maintain integrity of stored and transmitted data	- Encrypting customer databases with AES - Role-based access control on files - Using data loss prevention (DLP) tools
Endpoint Security	Secures end-user devices like PCs, Laptops, and Smartphones.	- Scan for and block malware - Monitor endpoint behavior - Prevent device misuse	- Installing antivirus software like Norton - Restricting USB ports to prevent data theft - Endpoint detection and response (EDR) tools
Application Security	Focuses on keeping Software secure during Development and Deployment.	- Detect coding flaws (e.g., SQL injection) - Use code scanning tools - Implement authentication	- Web Application Firewall (WAF) for web apps - Static Application Security Testing (SAST) - OAuth for secure user login
Cloud Security	Protects cloud-stored data and workloads from cyber threats.	- Configure access controls - Encrypt cloud data - Monitor cloud services for threats	- AWS IAM policies - Encrypting data in Google Cloud Storage - Cloud Security Posture Management (CSPM) tools
IoT Security	Protects internet-connected devices like Cameras, Sensors and Wearables.	- Use secure firmware - Block unauthorized control - Regular patching and updates	- Changing default passwords on smart devices - Regular firmware updates on IP cameras - Network segmentation for IoT devices

Source : https://www.cisco.com/site/in/en/learn/topics/security/what-is-cybersecurity.html

Different Types of Cybersecurity, Descriptions, Functionality, and Applications/Implement-ability - 2

What is Cybersecurity?

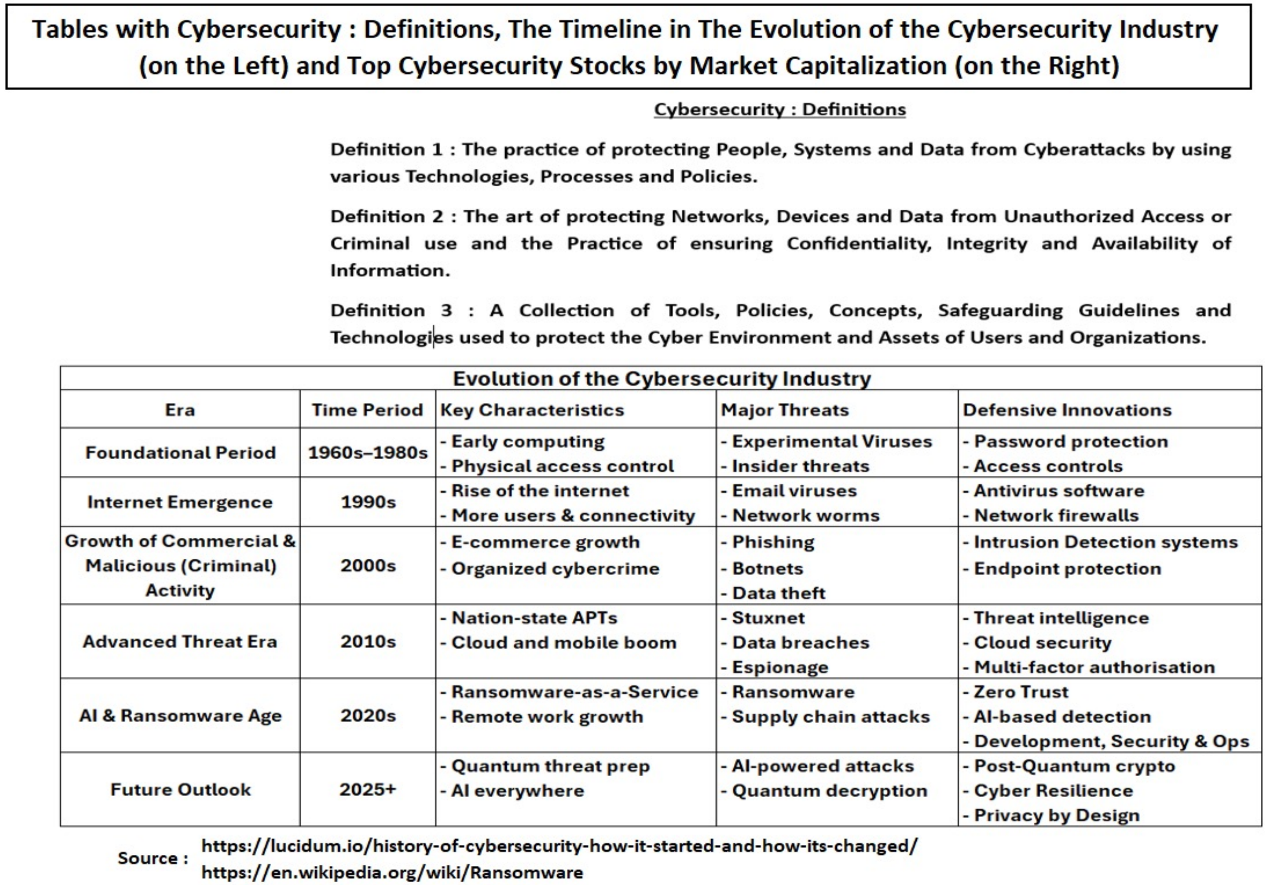


Different Types of Cybersecurity, Description, Functionality and Applications / Implementability - 2			
Type of Cybersecurity	**Description**	**Functionality**	**Applications / Implementability**
Operational Security (OpSec)	Involves safeguarding Critical Workflows and Strategic decisions.	- Control access to sensitive plans - Monitor internal communications - Limit sensitive disclosures	- Using encryption for confidential emails - Restricting document sharing on projects - Conducting background checks
Identity and Access Management (IAM)	Manages who has access to what resources in an organization.	- Authenticate users via MFA - Assign roles and permissions - Audit access logs	- Multi-factor authentication (MFA) for all users - Role-based access control (RBAC) - Periodic access reviews and audits
Mobile Security	Focuses on protecting Smartphones and Tablets from threats.	- Detect malicious apps - Use app sandboxing - Enforce device encryption and remote wipe	- Mobile Device Management (MDM) solutions like Microsoft Intune - Remote wipe of lost devices - Blocking installation of unapproved apps
Disaster Recovery & Business Continuity	Ensures quick recovery and continuity after an Attack or System failure.	- Backup critical data - Maintain failover systems - Create recovery plans and drills	- Daily backups to offsite locations - Running failover data centers - Regular disaster recovery drills
Critical Infrastructure Security	Protects Public Systems like Electricity and Transportation.	- Monitor industrial control systems - Protect SCADA networks - Prevent remote tampering	- Firewalls protecting power grid networks - Security patches on water treatment control systems - Physical security controls at critical sites
Cyber Threat Intelligence	Collects and analyzes threat data to enhance protection.	- Monitor global threat feeds - Analyze attack patterns - Predict and prevent future attacks	- Using threat intelligence platforms (TIPs) - Sharing Indicators of Compromise (IOCs) - Tracking phishing campaigns globally

Source : https://www.cisco.com/site/in/en/learn/topics/security/what-is-cybersecurity.html

On the Left, a Timeline on the Evolution of the Cybersecurity Industry
On the Right, a List of Cybersecurity Stocks by Market Cap in 4 Categories

Also, Expanded Forms & Description of Important Technical Terms/Semiconductor Jargon



Tables with Cybersecurity : Definitions, The Timeline in The Evolution of the Cybersecurity Industry (on the Left) and Top Cybersecurity Stocks by Market Capitalization (on the Right)

Cybersecurity : Definitions

Definition 1 : The practice of protecting People, Systems and Data from Cyberattacks by using various Technologies, Processes and Policies.

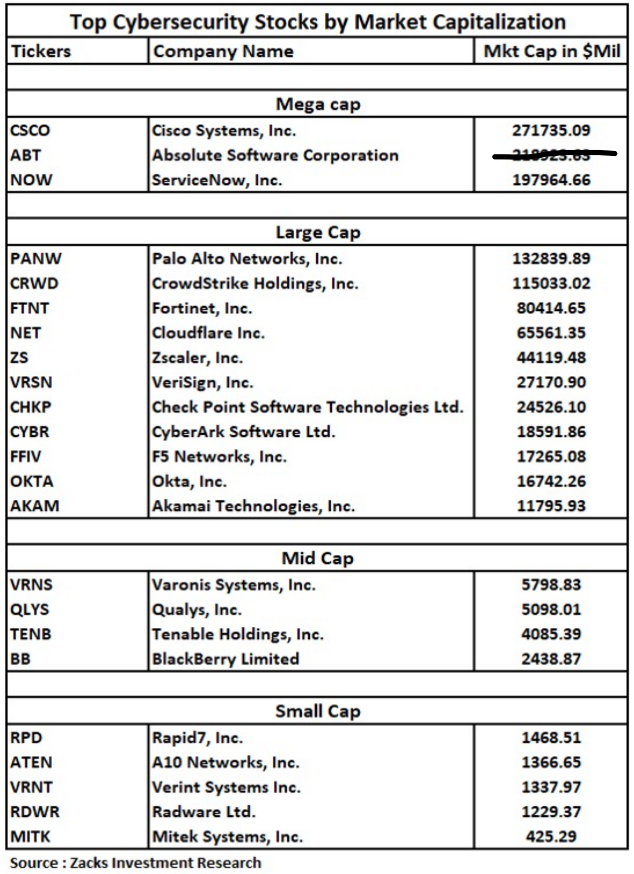
Definition 2 : The art of protecting Networks, Devices and Data from Unauthorized Access or Criminal use and the Practice of ensuring Confidentiality, Integrity and Availability of Information.

Definition 3 : A Collection of Tools, Policies, Concepts, Safeguarding Guidelines and Technologies used to protect the Cyber Environment and Assets of Users and Organizations.

Evolution of the Cybersecurity Industry

Era	Time Period	Key Characteristics	Major Threats	Defensive Innovations
Foundational Period	1960s–1980s	- Early computing - Physical access control	- Experimental Viruses - Insider threats	- Password protection - Access controls
Internet Emergence	1990s	- Rise of the internet - More users & connectivity	- Email viruses - Network worms	- Antivirus software - Network firewalls
Growth of Commercial & Malicious (Criminal) Activity	2000s	- E-commerce growth - Organized cybercrime	- Phishing - Botnets - Data theft	- Intrusion Detection systems - Endpoint protection
Advanced Threat Era	2010s	- Nation-state APTs - Cloud and mobile boom	- Stuxnet - Data breaches - Espionage	- Threat intelligence - Cloud security - Multi-factor authorisation
AI & Ransomware Age	2020s	- Ransomware-as-a-Service - Remote work growth	- Ransomware - Supply chain attacks	- Zero Trust - AI-based detection - Development, Security & Ops
Future Outlook	2025+	- Quantum threat prep - AI everywhere	- AI-powered attacks - Quantum decryption	- Post-Quantum crypto - Cyber Resilience - Privacy by Design

Source : https://lucidum.io/history-of-cybersecurity-how-it-started-and-how-its-changed/
https://en.wikipedia.org/wiki/Ransomware



Top Cybersecurity Stocks by Market Capitalization

Tickers	Company Name	Mkt Cap in $Mil
	Mega cap	
CSCO	Cisco Systems, Inc.	271735.09
ABT	Absolute Software Corporation	~~218923.63~~
NOW	ServiceNow, Inc.	197964.66
	Large Cap	
PANW	Palo Alto Networks, Inc.	132839.89
CRWD	CrowdStrike Holdings, Inc.	115033.02
FTNT	Fortinet, Inc.	80414.65
NET	Cloudflare Inc.	65561.35
ZS	Zscaler, Inc.	44119.48
VRSN	VeriSign, Inc.	27170.90
CHKP	Check Point Software Technologies Ltd.	24526.10
CYBR	CyberArk Software Ltd.	18591.86
FFIV	F5 Networks, Inc.	17265.08
OKTA	Okta, Inc.	16742.26
AKAM	Akamai Technologies, Inc.	11795.93
	Mid Cap	
VRNS	Varonis Systems, Inc.	5798.83
QLYS	Qualys, Inc.	5098.01
TENB	Tenable Holdings, Inc.	4085.39
BB	BlackBerry Limited	2438.87
	Small Cap	
RPD	Rapid7, Inc.	1468.51
ATEN	A10 Networks, Inc.	1366.65
VRNT	Verint Systems Inc.	1337.97
RDWR	Radware Ltd.	1229.37
MITK	Mitek Systems, Inc.	425.29

Source : Zacks Investment Research

ABT? The ticker symbol for Absolute Software Corporation is ABST.

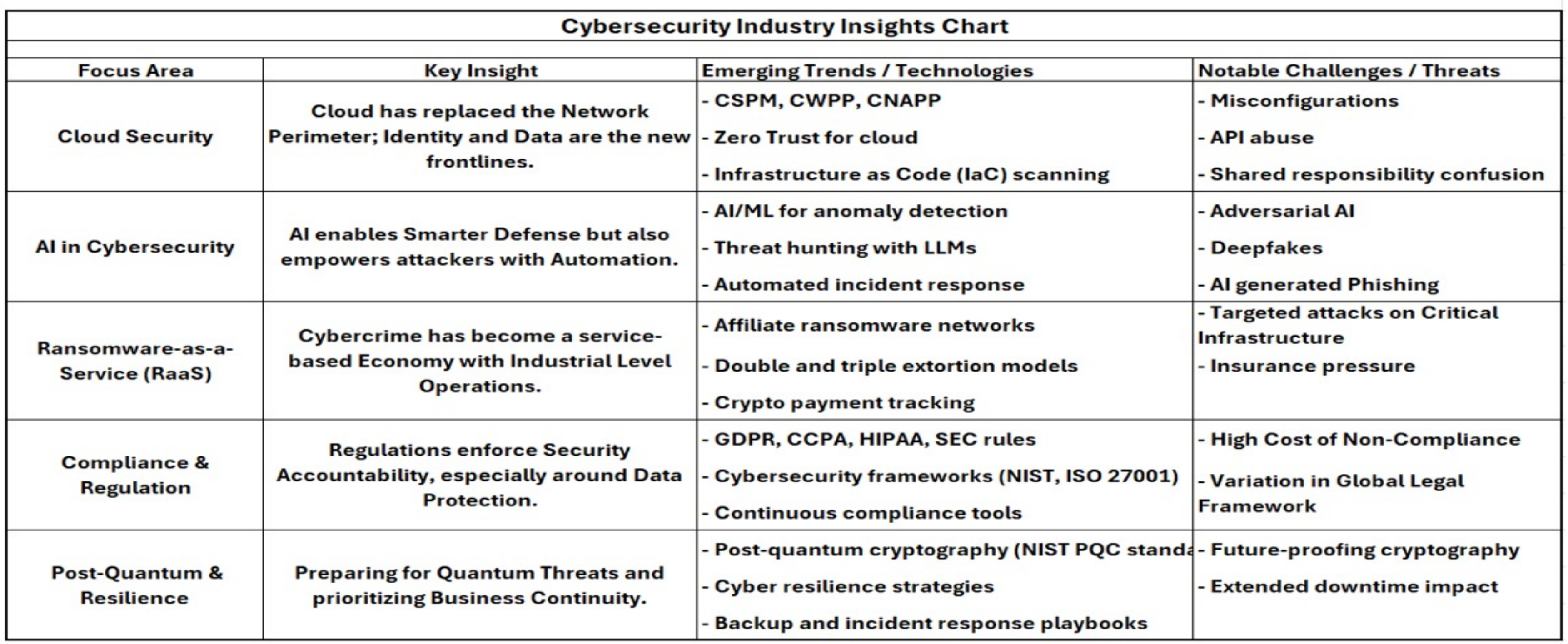
It previously traded on both the Toronto Stock Exchange (TSX) and NASDAQ, but delisted from both in July 2023 following an acquisition by Crosspoint Capital Partners.

However, some financial sources may still list the ticker ABST.

Cybersecurity Industry Insights Chart

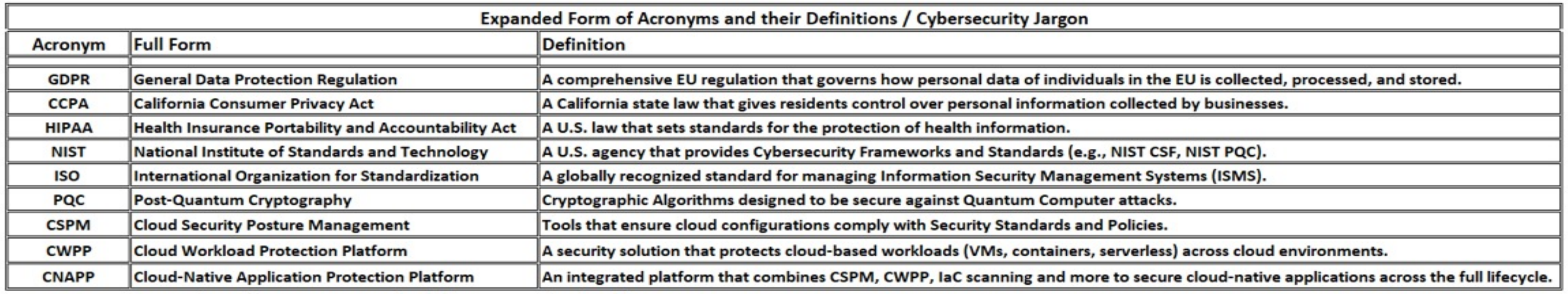
NOTE: Zacks Analysts Show You a Table at the Bottom. These are Needed Cybersecurity Industry Acronym Explanations.

Tables for Cybersecurity Industry Critical Insights (at Top) and Cybersecurity Industry Acronyms and Definitions (at Bottom)



Cybersecurity Industry Insights Chart

Focus Area	Key Insight	Emerging Trends / Technologies	Notable Challenges / Threats
Cloud Security	Cloud has replaced the Network Perimeter; Identity and Data are the new frontlines.	- CSPM, CWPP, CNAPP - Zero Trust for cloud - Infrastructure as Code (IaC) scanning	- Misconfigurations - API abuse - Shared responsibility confusion
AI in Cybersecurity	AI enables Smarter Defense but also empowers attackers with Automation.	- AI/ML for anomaly detection - Threat hunting with LLMs - Automated incident response	- Adversarial AI - Deepfakes - AI generated Phishing
Ransomware-as-a-Service (RaaS)	Cybercrime has become a service-based Economy with Industrial Level Operations.	- Affiliate ransomware networks - Double and triple extortion models - Crypto payment tracking	- Targeted attacks on Critical Infrastructure - Insurance pressure
Compliance & Regulation	Regulations enforce Security Accountability, especially around Data Protection.	- GDPR, CCPA, HIPAA, SEC rules - Cybersecurity frameworks (NIST, ISO 27001) - Continuous compliance tools	- High Cost of Non-Compliance - Variation in Global Legal Framework
Post-Quantum & Resilience	Preparing for Quantum Threats and prioritizing Business Continuity.	- Post-quantum cryptography (NIST PQC standa - Cyber resilience strategies - Backup and incident response playbooks	- Future-proofing cryptography - Extended downtime impact



Expanded Form of Acronyms and their Definitions / Cybersecurity Jargon

Acronym	Full Form	Definition
GDPR	General Data Protection Regulation	A comprehensive EU regulation that governs how personal data of individuals in the EU is collected, processed, and stored.
CCPA	California Consumer Privacy Act	A California state law that gives residents control over personal information collected by businesses.
HIPAA	Health Insurance Portability and Accountability Act	A U.S. law that sets standards for the protection of health information.
NIST	National Institute of Standards and Technology	A U.S. agency that provides Cybersecurity Frameworks and Standards (e.g., NIST CSF, NIST PQC).
ISO	International Organization for Standardization	A globally recognized standard for managing Information Security Management Systems (ISMS).
PQC	Post-Quantum Cryptography	Cryptographic Algorithms designed to be secure against Quantum Computer attacks.
CSPM	Cloud Security Posture Management	Tools that ensure cloud configurations comply with Security Standards and Policies.
CWPP	Cloud Workload Protection Platform	A security solution that protects cloud-based workloads (VMs, containers, serverless) across cloud environments.
CNAPP	Cloud-Native Application Protection Platform	An integrated platform that combines CSPM, CWPP, IaC scanning and more to secure cloud-native applications across the full lifecycle.

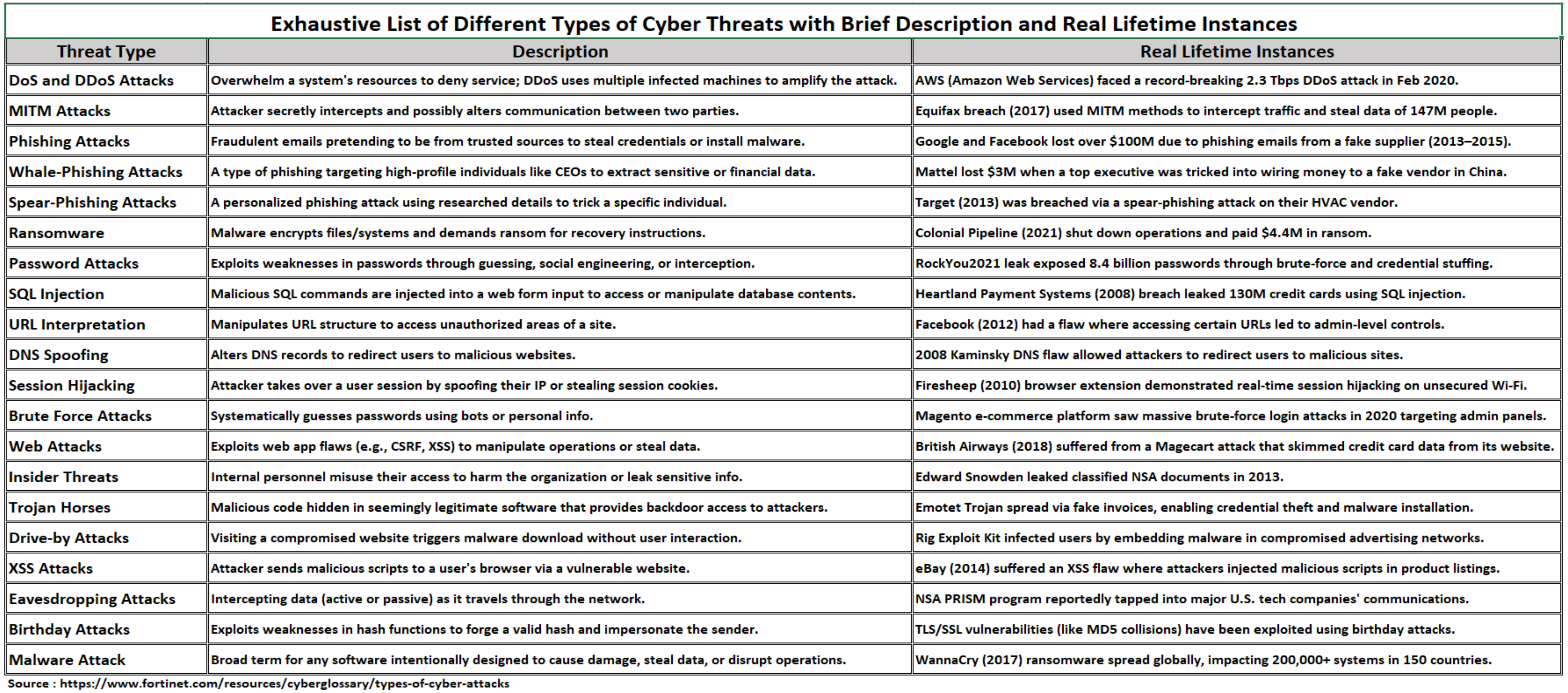
Source : https://www.gartner.com/en/information-technology/glossary

Sources - https://cloudsecurityalliance.org/
https://www.digitalguardian.com/

An Exhaustive List of Different Types of Cyber Threats

With a Brief Description and Real Lifetime Instances

Distributed Denial of Service(DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.



Exhaustive List of Different Types of Cyber Threats with Brief Description and Real Lifetime Instances

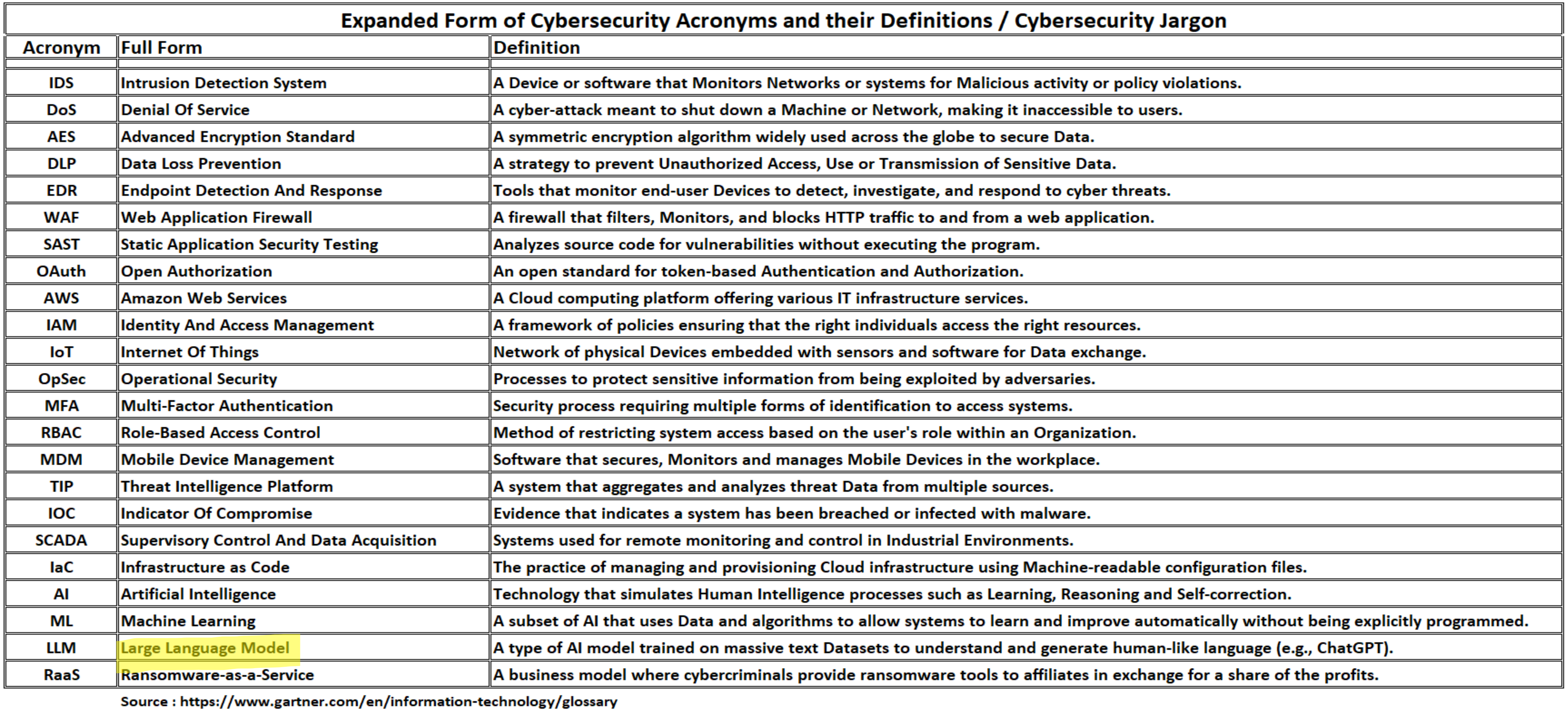
Threat Type	Description	Real Lifetime Instances
DoS and DDoS Attacks	Overwhelm a system's resources to deny service; DDoS uses multiple infected machines to amplify the attack.	AWS (Amazon Web Services) faced a record-breaking 2.3 Tbps DDoS attack in Feb 2020.
MITM Attacks	Attacker secretly intercepts and possibly alters communication between two parties.	Equifax breach (2017) used MITM methods to intercept traffic and steal data of 147M people.
Phishing Attacks	Fraudulent emails pretending to be from trusted sources to steal credentials or install malware.	Google and Facebook lost over $100M due to phishing emails from a fake supplier (2013–2015).
Whale-Phishing Attacks	A type of phishing targeting high-profile individuals like CEOs to extract sensitive or financial data.	Mattel lost $3M when a top executive was tricked into wiring money to a fake vendor in China.
Spear-Phishing Attacks	A personalized phishing attack using researched details to trick a specific individual.	Target (2013) was breached via a spear-phishing attack on their HVAC vendor.
Ransomware	Malware encrypts files/systems and demands ransom for recovery instructions.	Colonial Pipeline (2021) shut down operations and paid $4.4M in ransom.
Password Attacks	Exploits weaknesses in passwords through guessing, social engineering, or interception.	RockYou2021 leak exposed 8.4 billion passwords through brute-force and credential stuffing.
SQL Injection	Malicious SQL commands are injected into a web form input to access or manipulate database contents.	Heartland Payment Systems (2008) breach leaked 130M credit cards using SQL injection.
URL Interpretation	Manipulates URL structure to access unauthorized areas of a site.	Facebook (2012) had a flaw where accessing certain URLs led to admin-level controls.
DNS Spoofing	Alters DNS records to redirect users to malicious websites.	2008 Kaminsky DNS flaw allowed attackers to redirect users to malicious sites.
Session Hijacking	Attacker takes over a user session by spoofing their IP or stealing session cookies.	Firesheep (2010) browser extension demonstrated real-time session hijacking on unsecured Wi-Fi.
Brute Force Attacks	Systematically guesses passwords using bots or personal info.	Magento e-commerce platform saw massive brute-force login attacks in 2020 targeting admin panels.
Web Attacks	Exploits web app flaws (e.g., CSRF, XSS) to manipulate operations or steal data.	British Airways (2018) suffered from a Magecart attack that skimmed credit card data from its website.
Insider Threats	Internal personnel misuse their access to harm the organization or leak sensitive info.	Edward Snowden leaked classified NSA documents in 2013.
Trojan Horses	Malicious code hidden in seemingly legitimate software that provides backdoor access to attackers.	Emotet Trojan spread via fake invoices, enabling credential theft and malware installation.
Drive-by Attacks	Visiting a compromised website triggers malware download without user interaction.	Rig Exploit Kit infected users by embedding malware in compromised advertising networks.
XSS Attacks	Attacker sends malicious scripts to a user's browser via a vulnerable website.	eBay (2014) suffered an XSS flaw where attackers injected malicious scripts in product listings.
Eavesdropping Attacks	Intercepting data (active or passive) as it travels through the network.	NSA PRISM program reportedly tapped into major U.S. tech companies' communications.
Birthday Attacks	Exploits weaknesses in hash functions to forge a valid hash and impersonate the sender.	TLS/SSL vulnerabilities (like MD5 collisions) have been exploited using birthday attacks.
Malware Attack	Broad term for any software intentionally designed to cause damage, steal data, or disrupt operations.	WannaCry (2017) ransomware spread globally, impacting 200,000+ systems in 150 countries.

Source : https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

Man-in-the-Middle (MitM) attack is a type of cyberattack where a malicious actor intercepts and potentially alters communication between two parties who believe they are communicating directly with each other.

A More Expansive List of Cybersecurity Acronyms and Their Definitions

Still More Cybersecurity Jargon to Learn!



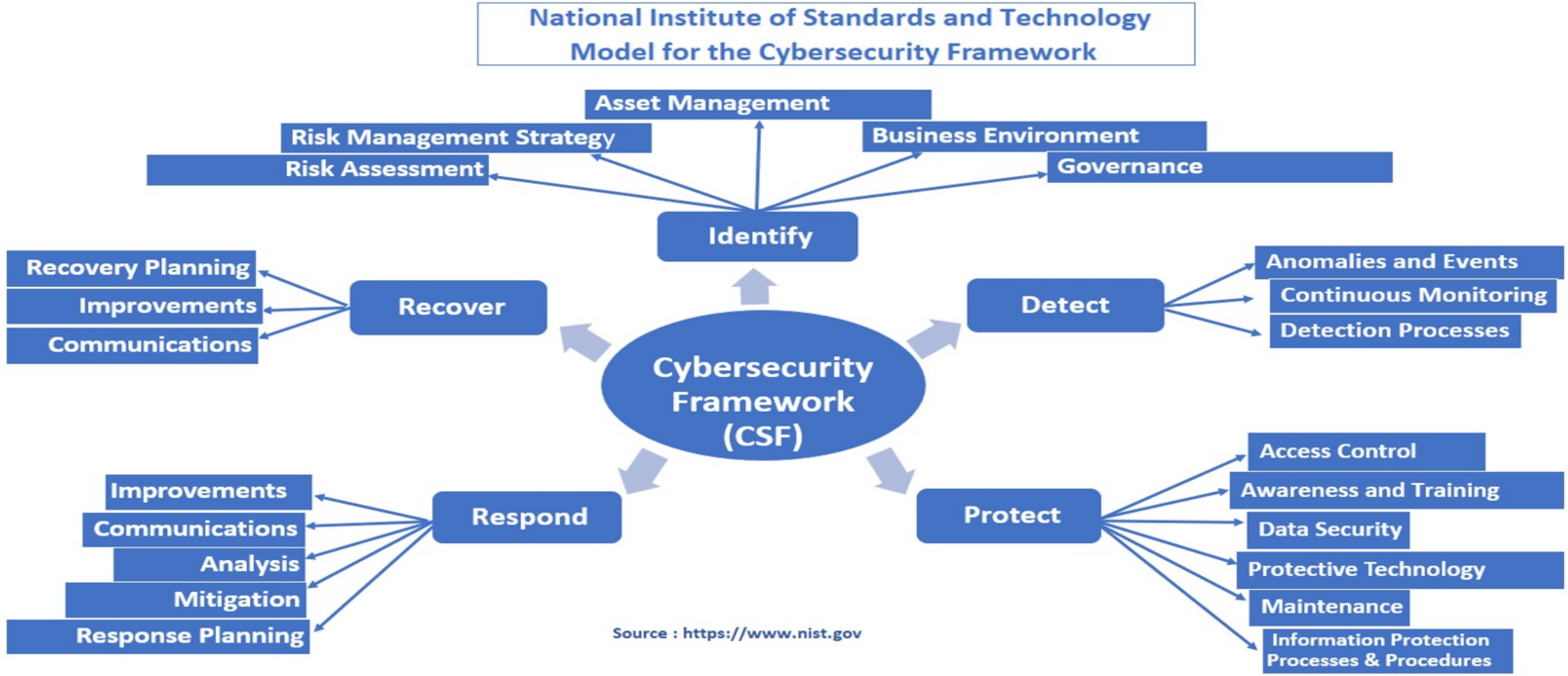
Expanded Form of Cybersecurity Acronyms and their Definitions / Cybersecurity Jargon

Acronym	Full Form	Definition
IDS	Intrusion Detection System	A Device or software that Monitors Networks or systems for Malicious activity or policy violations.
DoS	Denial Of Service	A cyber-attack meant to shut down a Machine or Network, making it inaccessible to users.
AES	Advanced Encryption Standard	A symmetric encryption algorithm widely used across the globe to secure Data.
DLP	Data Loss Prevention	A strategy to prevent Unauthorized Access, Use or Transmission of Sensitive Data.
EDR	Endpoint Detection And Response	Tools that monitor end-user Devices to detect, investigate, and respond to cyber threats.
WAF	Web Application Firewall	A firewall that filters, Monitors, and blocks HTTP traffic to and from a web application.
SAST	Static Application Security Testing	Analyzes source code for vulnerabilities without executing the program.
OAuth	Open Authorization	An open standard for token-based Authentication and Authorization.
AWS	Amazon Web Services	A Cloud computing platform offering various IT infrastructure services.
IAM	Identity And Access Management	A framework of policies ensuring that the right individuals access the right resources.
IoT	Internet Of Things	Network of physical Devices embedded with sensors and software for Data exchange.
OpSec	Operational Security	Processes to protect sensitive information from being exploited by adversaries.
MFA	Multi-Factor Authentication	Security process requiring multiple forms of identification to access systems.
RBAC	Role-Based Access Control	Method of restricting system access based on the user's role within an Organization.
MDM	Mobile Device Management	Software that secures, Monitors and manages Mobile Devices in the workplace.
TIP	Threat Intelligence Platform	A system that aggregates and analyzes threat Data from multiple sources.
IOC	Indicator Of Compromise	Evidence that indicates a system has been breached or infected with malware.
SCADA	Supervisory Control And Data Acquisition	Systems used for remote monitoring and control in Industrial Environments.
IaC	Infrastructure as Code	The practice of managing and provisioning Cloud infrastructure using Machine-readable configuration files.
AI	Artificial Intelligence	Technology that simulates Human Intelligence processes such as Learning, Reasoning and Self-correction.
ML	Machine Learning	A subset of AI that uses Data and algorithms to allow systems to learn and improve automatically without being explicitly programmed.
LLM	Large Language Model	A type of AI model trained on massive text Datasets to understand and generate human-like language (e.g., ChatGPT).
RaaS	Ransomware-as-a-Service	A business model where cybercriminals provide ransomware tools to affiliates in exchange for a share of the profits.

Source : https://www.gartner.com/en/information-technology/glossary

The National Institute of Standards and Technology (NIST) Model for the Cybersecurity Framework

From nist.gov

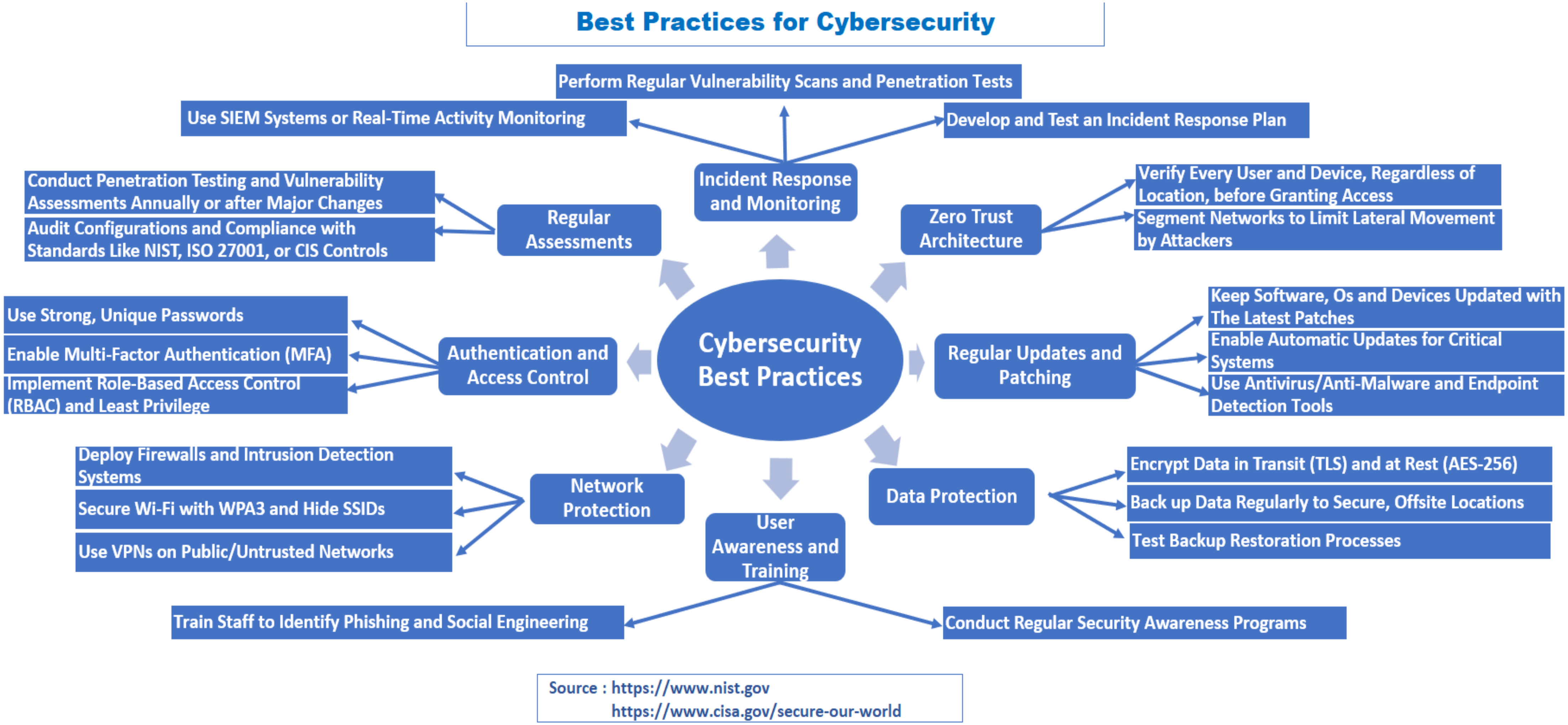


National Institute of Standards and Technology
Model for the Cybersecurity Framework

Source : https://www.nist.gov

Best Practices for Cybersecurity

From nist.gov and cisa.gov



Best Practices for Cybersecurity

Cybersecurity Best Practices

Incident Response and Monitoring
- Use SIEM Systems or Real-Time Activity Monitoring
- Perform Regular Vulnerability Scans and Penetration Tests
- Develop and Test an Incident Response Plan

Regular Assessments
- Conduct Penetration Testing and Vulnerability Assessments Annually or after Major Changes
- Audit Configurations and Compliance with Standards Like NIST, ISO 27001, or CIS Controls

Zero Trust Architecture
- Verify Every User and Device, Regardless of Location, before Granting Access
- Segment Networks to Limit Lateral Movement by Attackers

Authentication and Access Control
- Use Strong, Unique Passwords
- Enable Multi-Factor Authentication (MFA)
- Implement Role-Based Access Control (RBAC) and Least Privilege

Regular Updates and Patching
- Keep Software, Os and Devices Updated with The Latest Patches
- Enable Automatic Updates for Critical Systems
- Use Antivirus/Anti-Malware and Endpoint Detection Tools

Network Protection
- Deploy Firewalls and Intrusion Detection Systems
- Secure Wi-Fi with WPA3 and Hide SSIDs
- Use VPNs on Public/Untrusted Networks

Data Protection
- Encrypt Data in Transit (TLS) and at Rest (AES-256)
- Back up Data Regularly to Secure, Offsite Locations
- Test Backup Restoration Processes

User Awareness and Training
- Train Staff to Identify Phishing and Social Engineering
- Conduct Regular Security Awareness Programs

Source : https://www.nist.gov
https://www.cisa.gov/secure-our-world

What Tickers Look Good?

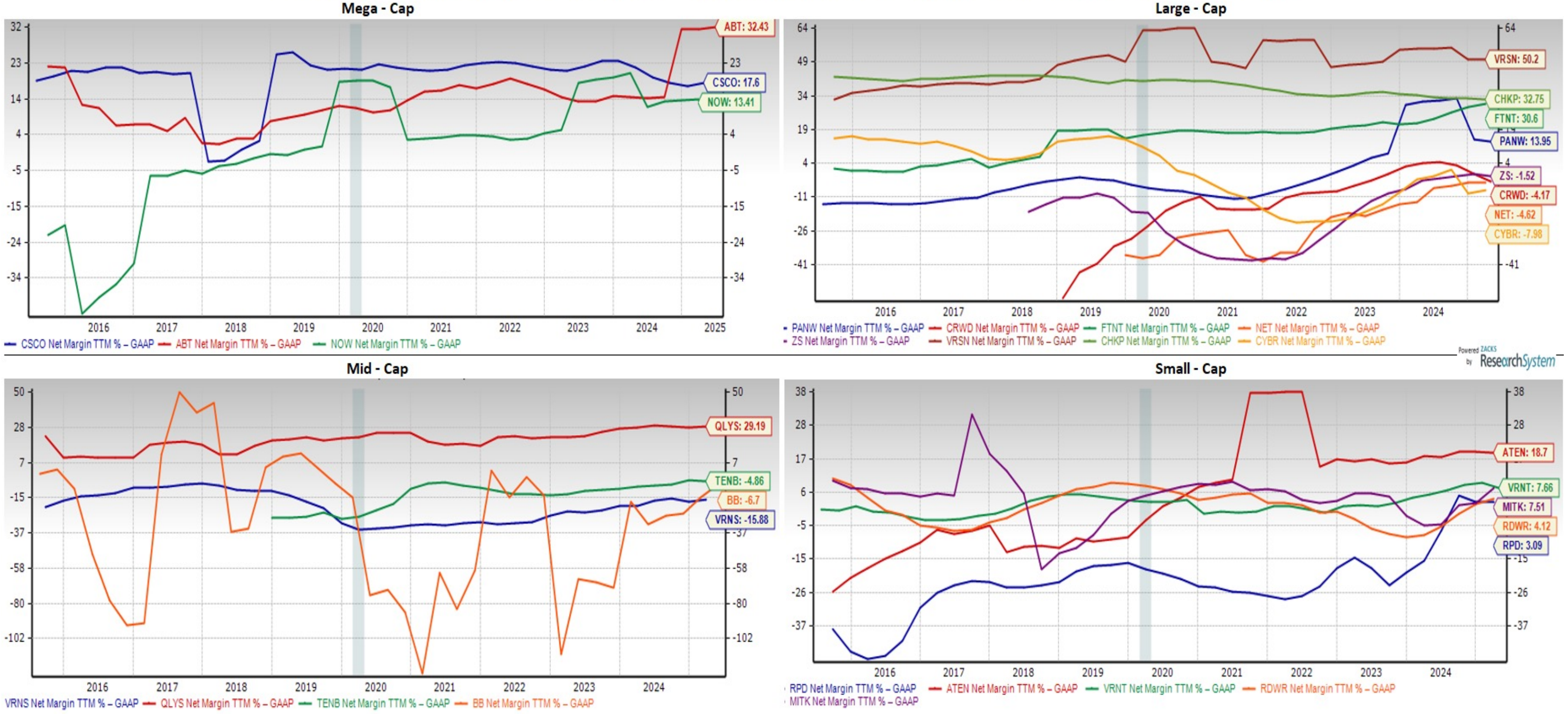
2. Top Cybersecurity Stocks

Done for Four Style Classes

Net Margin TTM% Charts for Top Cybersecurity Stocks

By Market Capitalization, Classified into Four Groups

Net Margin TTM% Charts for Top Cybersecurity Stocks by Market Capitalization Classified into Four Groups

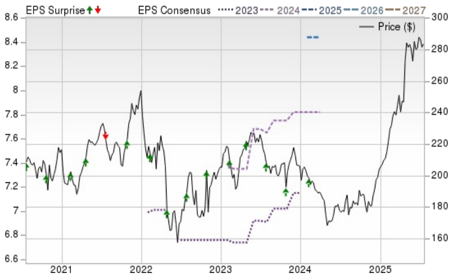

Mega - Cap

Large - Cap

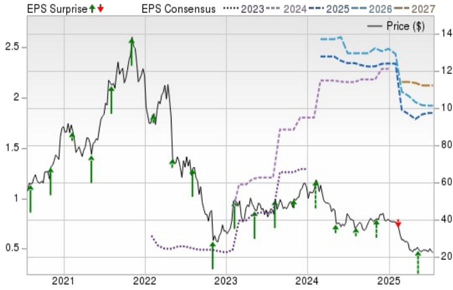
Mid - Cap

Small - Cap

Verisign (VSRN)

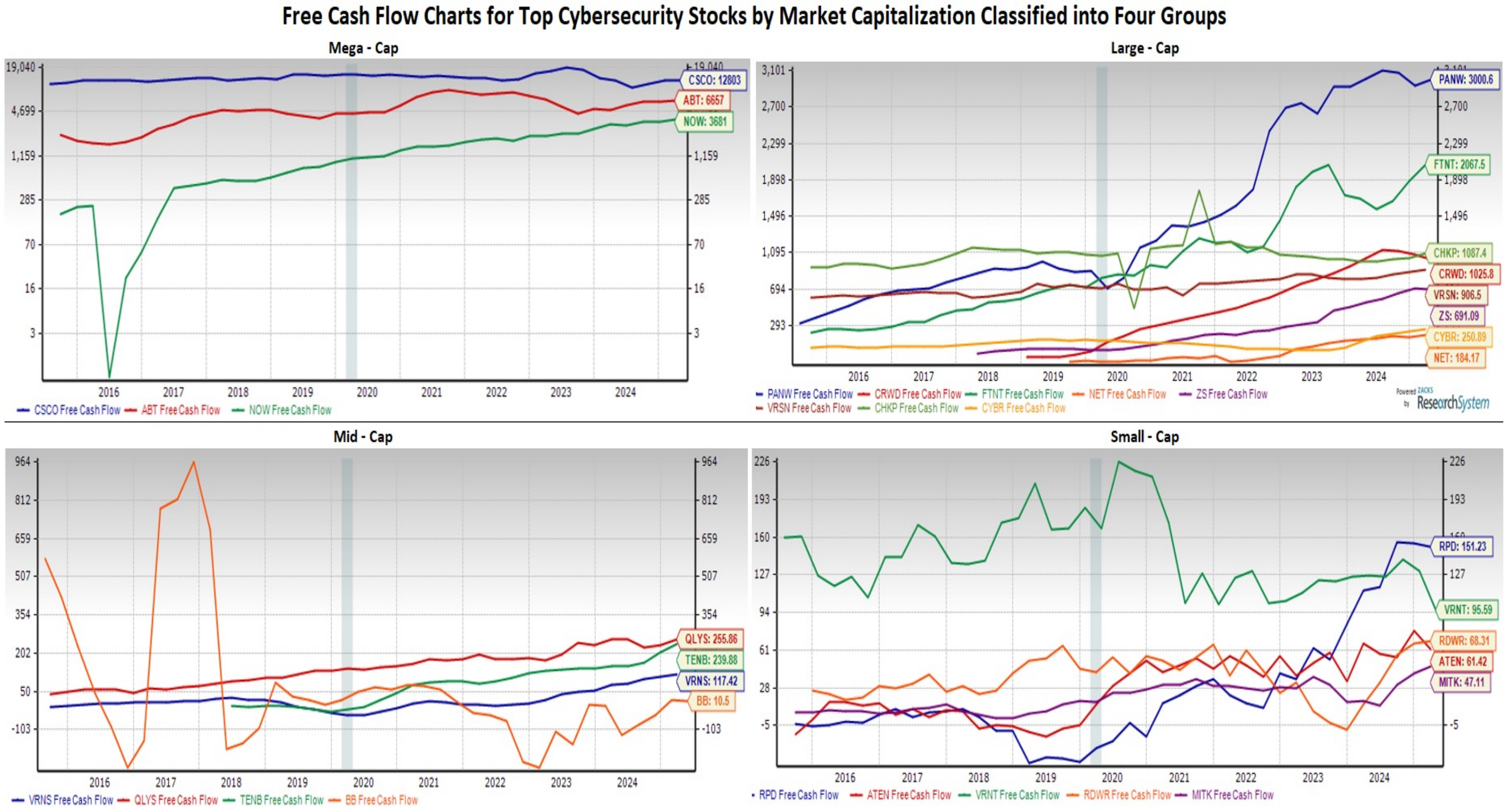


Rapid 7 (RPD)



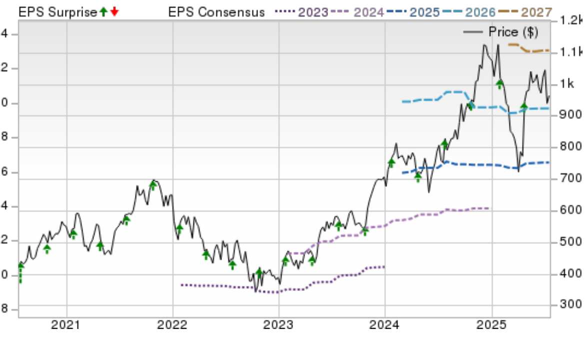
Free Cash Flow Charts for Top Cybersecurity Stocks

By Market Capitalization, Classified into Four Groups

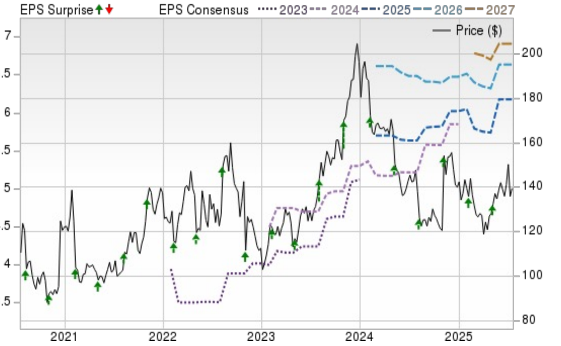


Free Cash Flow Charts for Top Cybersecurity Stocks by Market Capitalization Classified into Four Groups

ServiceNow (NOW)

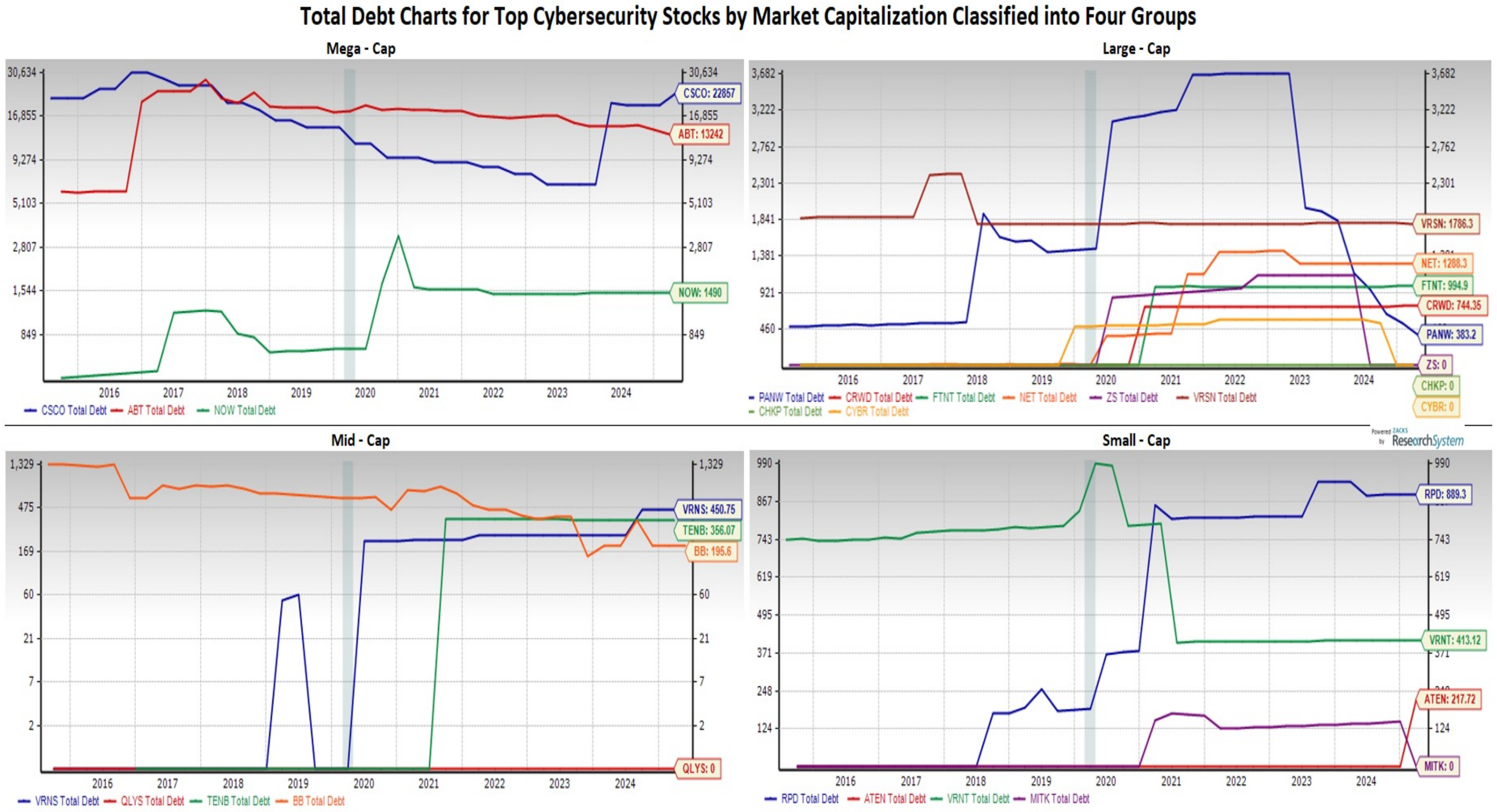


Qualys (QLYS)



Total Debt Charts for Top Cybersecurity Stocks

By Market Capitalization, Classified into Four Groups



Total Debt Charts for Top Cybersecurity Stocks by Market Capitalization Classified into Four Groups

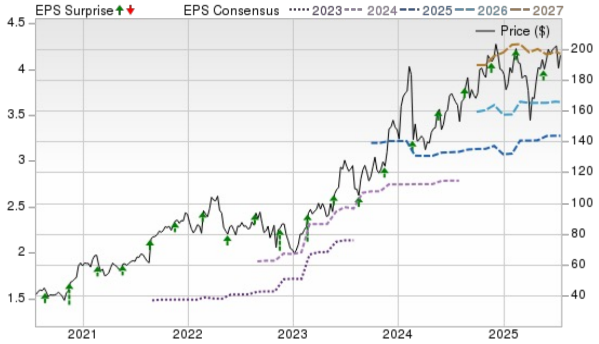
Mega - Cap

Large - Cap

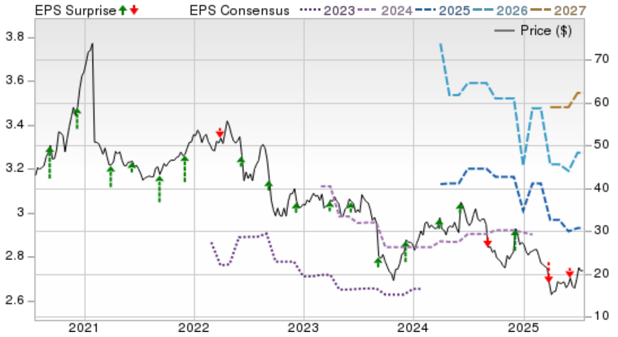
Mid - Cap

Small - Cap

Palo Alto Networks (PANW)



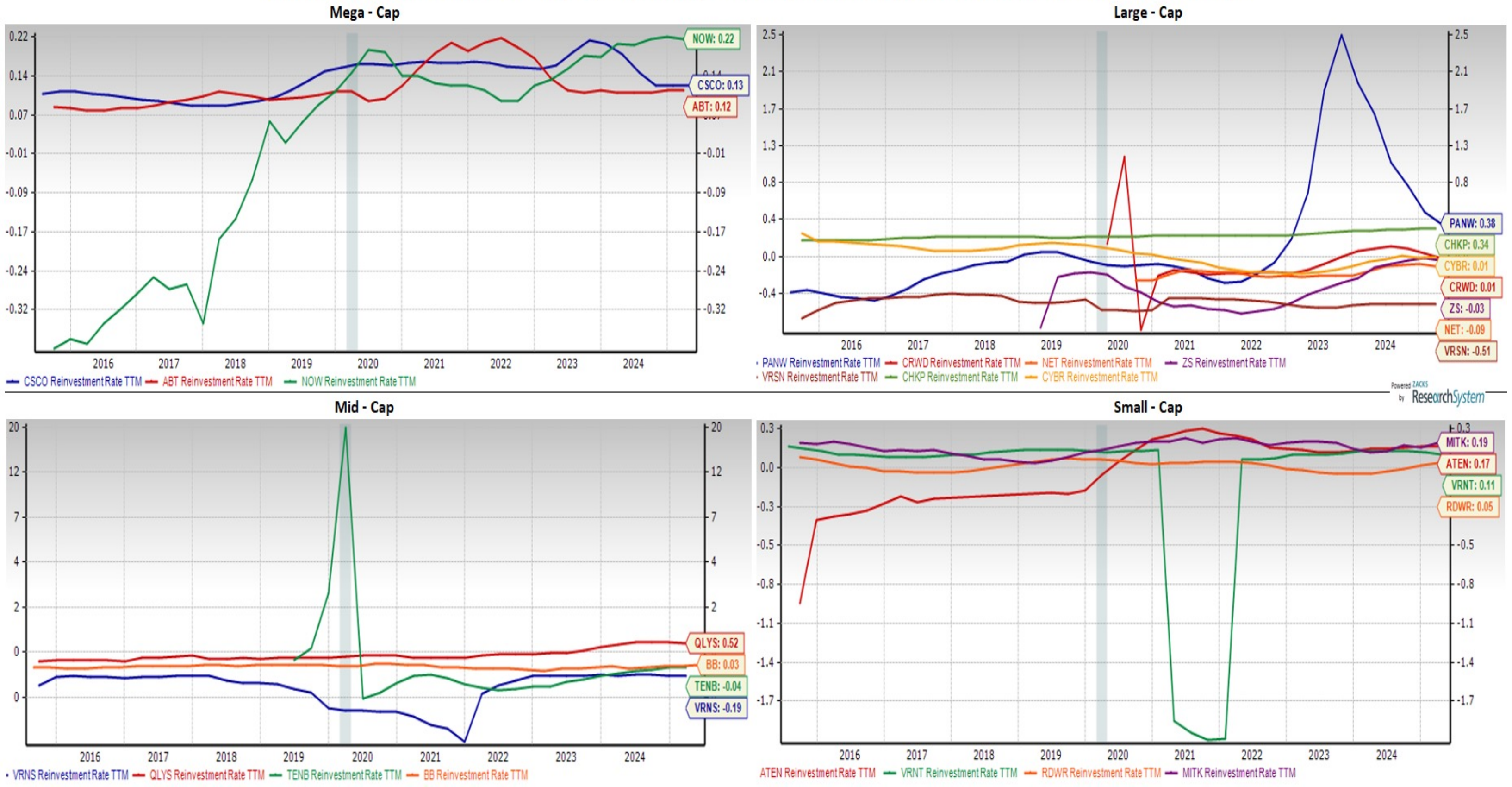
Verint Systems (VRNT)



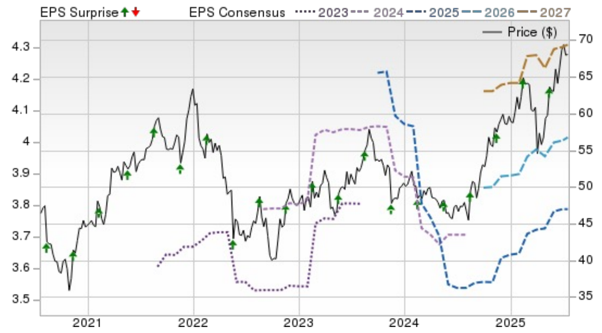
Reinvestment Rate Charts for Top Cybersecurity Stocks

By Market Capitalization, Classified into Four Groups

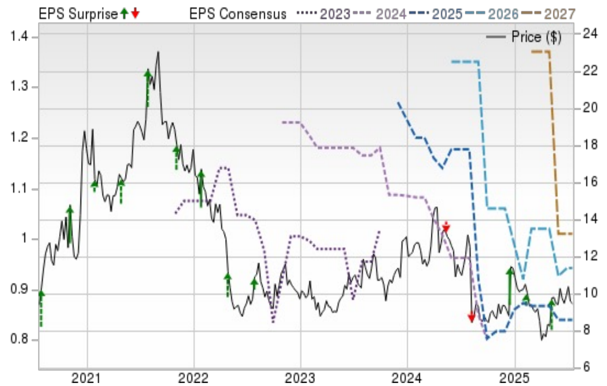
Reinvestment Rate Charts for Top Cybersecurity Stocks by Market Capitalization Classified into Four Groups



Cisco (CSCO)

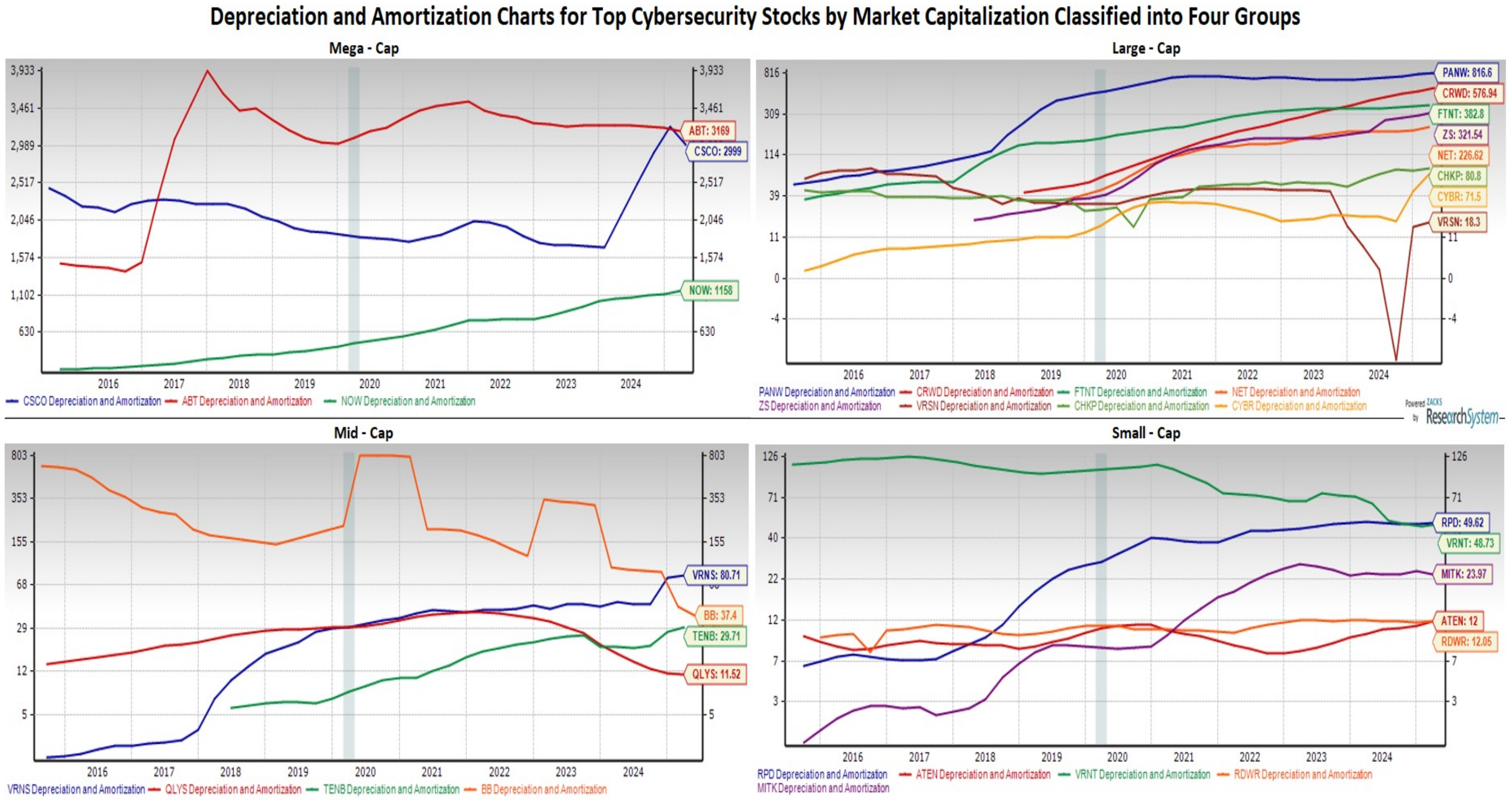


Mitek (MITK)

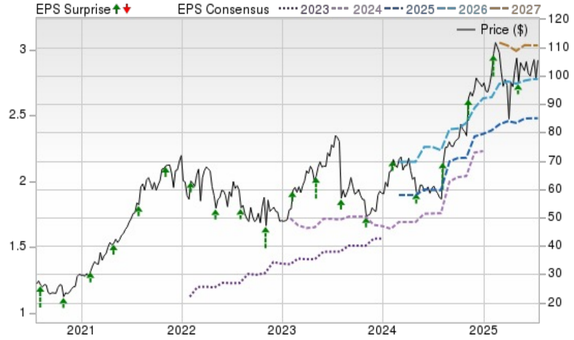


Depreciation and Amortization Charts for Top Cybersecurity Stocks

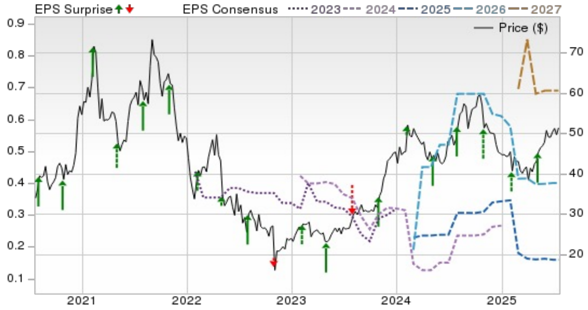
By Market Capitalization, Classified into Four Groups



Fortinet (FTNT)



Varonis Systems (VRNS)



Thank You for Attending!

John Blank, PhD
Zacks Chief Equity Strategist and Economist
Zacks Professional Services

866-794-6065

strategycall@zackspro.com

www.zackspro.com

in Zacks Professional Services

@ZATools