BBR T BULL & BEAR TECHNOLOGY

BBR BULL & BEAR RESEARCH

Fall 2024 Technology Outlook:

Cybersecurity

Contents

Tech Team

Andrew Shih
Director

Raahil Gunaratne
Associate

Sanjit Kosaraju
Analyst

Craig Ottaviano
Analyst

Rahul Yaganti
Analyst

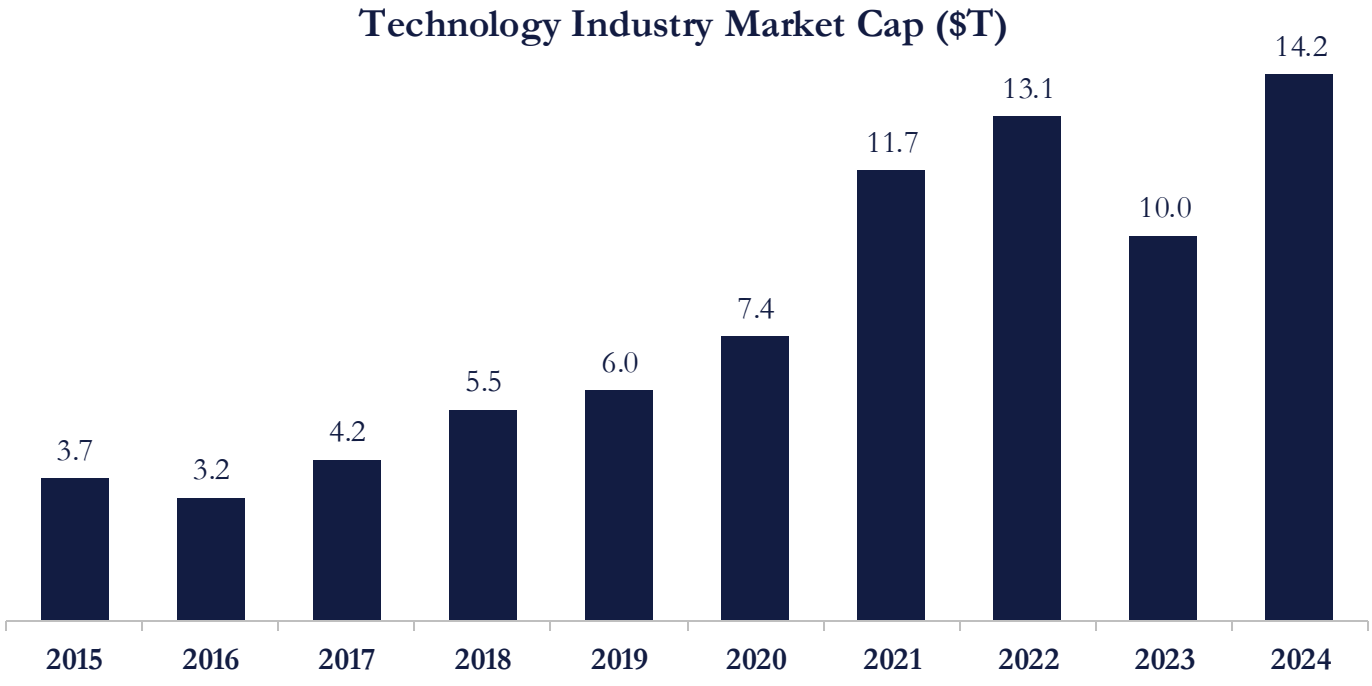
Technology Overview

The State of Tech

The technology sector, patented by rapid innovation and adaptation, has emerged as a driving force in the global economy, led by industries such as artificial intelligence (AI), cybersecurity, software, and cloud computing. During the early pandemic years, accelerated digital transformation efforts fueled significant market growth. However, more recently, high inflation, rising interest rates, and concerns over a potential economic slowdown have dampened global tech spending. This shift led to a 26% decline in tech job postings from 2022 to 2023. Additionally, rising financing costs and slowing revenue growth prompted investors to reduce their equity investments in technology by 30% - 40%, resulting in a total of $570 billion in 2023. In 2024, a rebound, driven by growth in sectors like AI, was spurred by advancements in digital transformation and automation. The AI market alone is projected to surge, reaching an estimated $780 - $990 billion by 2027, an increase from $185 billion in 2023. Although the projections for AI are undeniably strong, several critical concerns must be addressed for sustainable growth. These include regulatory and compliance challenges, cybersecurity and privacy risks, and the ethical implications surrounding AI's widespread adoption. As the technology sector charts its path to recovery and economists express increasing optimism about the broader US economy, it is strategically positioned to reaffirm its status as a pivotal driver of the global economy, presenting renewed opportunities for growth and investment.

The Magnificent 7

The technology sector is home to some of the largest, most innovative, and successful companies. Within this sector, the "Magnificent Seven" refers to a group of high-performing tech stocks that are household names. This elite group includes Microsoft Corp. (MSFT), Apple Inc. (AAPL), Nvidia Corp. (NVDA), Alphabet Inc. (GOOG), Amazon.com Inc. (AMZN), Meta Platforms Inc. (META), and Tesla Inc. (TSLA). Together, they represent 29.7% of the S&P 500's index weight and drive much of the market's performance this year. The year-to-date (YTD) return of the S&P 500 as of 10/18 stands at 23%, primarily fueled by strong returns from these companies: MSFT +11.08%, AAPL +22.37%, NVDA +179.00%, GOOG 17.31%, AMZN 25.36%, META 63.46, with TSLA as the exception at –10.72%. The substantial index weighting of these firms, combined with their impressive YTD performance (aside from Tesla), has directly contributed to market growth, reflecting strong investor confidence in the tech sector.



Sources: Deloitte, McKinsey, Bain & Company, Wall Street Journal, USA Today, Simply Wall Street

Tech Overview

Notable Industry Segments

When describing Technology, it is typically associated with buzzwords such as Artificial Intelligence or the Internet. In reality, the technology sector is a much larger environment that encapsulates several subindustries ranging from telecommunications to the blockchain and continues to expand yearly with innovations and use cases.

Industry Segments:

Software as a Service (SaaS)

- Companies that provide software solutions, such as CRM and ERP, to enterprises in order to streamline operations, reduce costs, and drive scalability.

Hardware

- Companies that produce the physical components that make up computers as well as consumer peripherals, such as Dell, Logitech, HP, Lenovo.

Cybersecurity

- Technology solutions focused on providing security to enterprises by protecting systems, networks, and data from potential breaches.

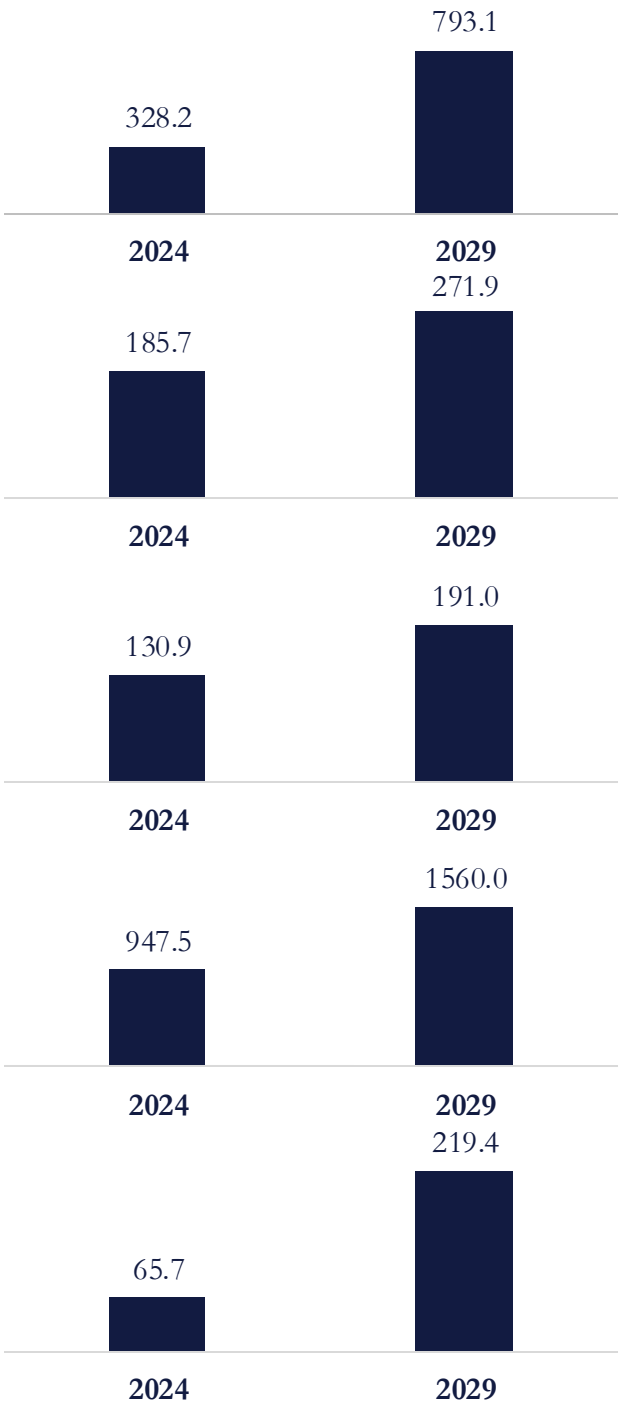
Internet of Things (IOT)

- Objects embedded within items, such as sensors, that exchange real-time data over the internet.

Data Analytics

- Solutions focused on analyzing large amounts of data to derive synergies that benefit top and bottom lines for an enterprise.

Projected Growth of Each Segment ($M):



Industry Segments:

Semiconductor Manufacturing
- Process of designing and producing semiconductor devices such as microchips and integrated circuits, critical to advancing technology

Telecommunications
- The transmission of information across global networks through electronic means, enabling voice, data, and video communication

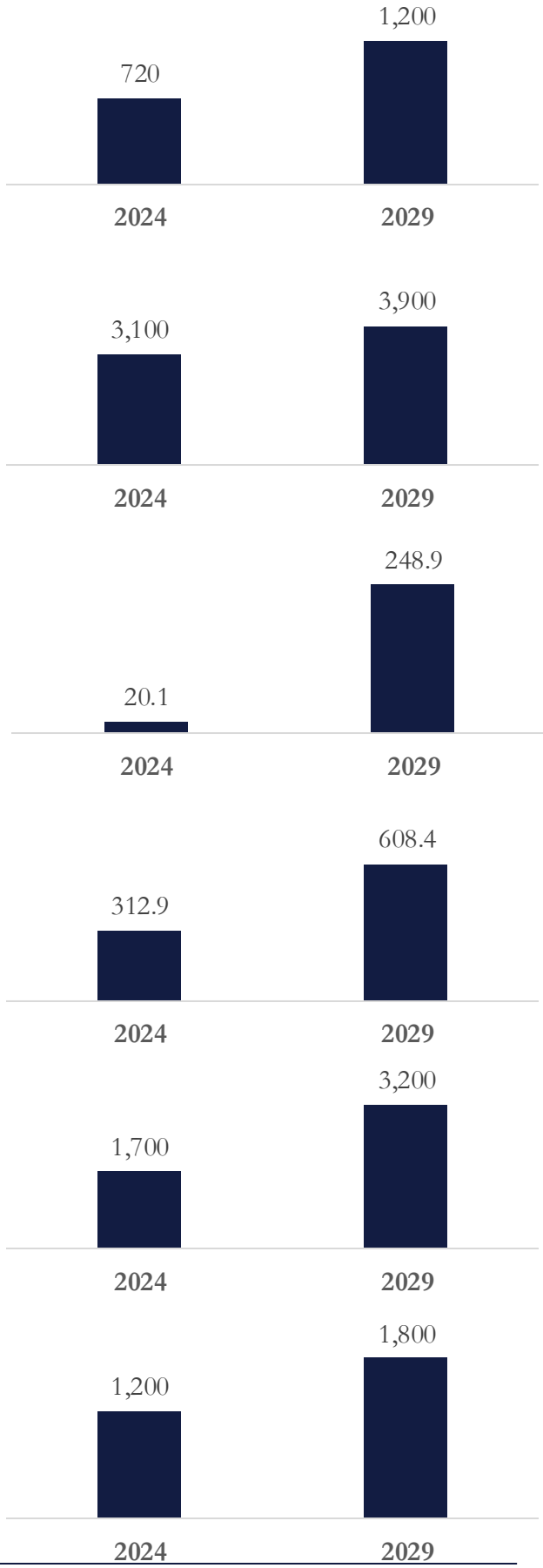
Blockchain
- A decentralized, distributed database that securely tracks, links, and traces transactions in a transparent and immutable way, enabling enterprises to share information securely

FinTech
- The integration of technology into financial services to enhance the delivery and use of financial products. Ex: Mobile Payments, Blockchain, Robo-Advisors

Biotech
- Use of biological processes and systems to develop products and technologies to improve human health, agriculture, and the environment

IT Services & Consulting
- Provides businesses with technical expertise and solutions to manage, optimize, and secure their IT infrastructure, guiding businesses in digital transformation

Projected Growth of Each Segment:



Sources: Fortune Business Insights, MarketsAndMarkets, PitchBook, Statista


BBR T BULL & BEAR TECHNOLOGY
BBR BULL & BEAR RESEARCH
Cybersecurity Overview

Cybersecurity Overview

The State of Cybersecurity

The cybersecurity industry is made up of several segments such as network security, application security, information security, cloud security, internet of things (IoT) security, and identity and access management, all of which play a role in the protection of devices, networks, programs, and data from digital attacks. In 2024, cybersecurity continues to be a priority for organizations and companies worldwide with several growth factors including technology reliance, a rise in cyber threats, increased data protection regulations, remote-work models, and adoption of emerging technologies. However, there are several challenges facing the cybersecurity industry such as the growing capabilities of cybercriminals, implementation and compatibility issues, and a shortage of talented labor. Some large players in the space include Palo Alto Networks (PANW), CrowdStrike (CRWD), and Fortinet (FTNT). PANW and FTNT primarily specialize in offering digital solutions and platforms that support network security enabling secure digital transformation for organizations while CRWD focuses on endpoint security protecting devices from threats like malware and ransomware. With the increased reliance on and adoption of technology across nearly every industry, the importance of digital security is recognized by company leaders and governments alike bolstering the implementation of cybersecurity solutions.

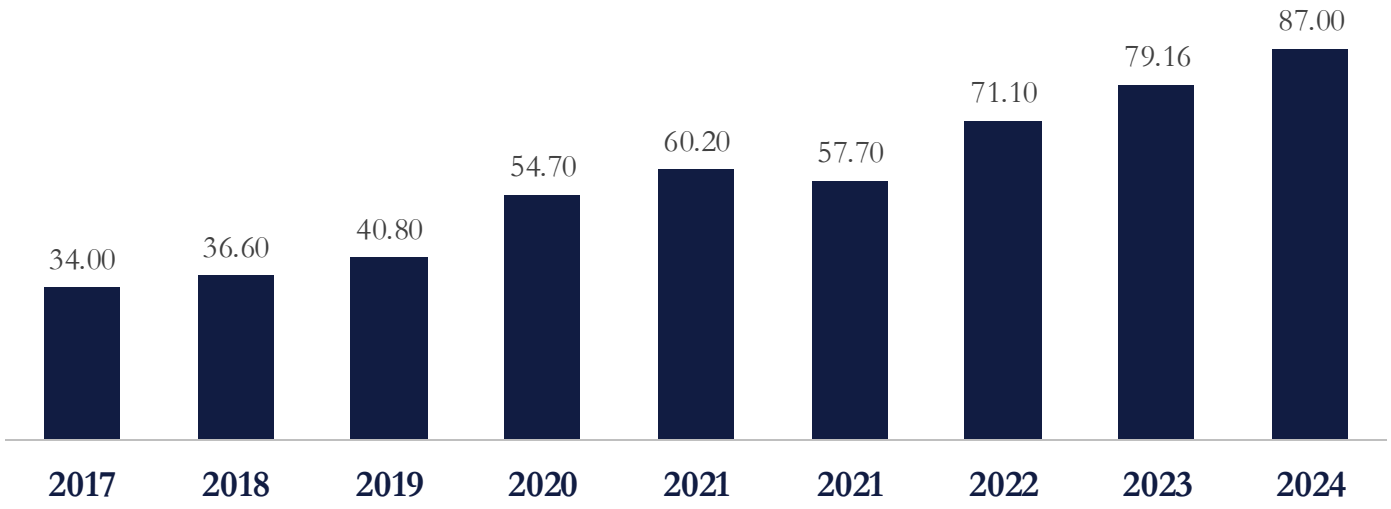
Market Size

The emergence of generative AI and intelligent technologies has increased the complexity and frequency of unprecedented cyber threats. The widespread adoption of emerging enterprise technologies has reinforced the need for digital trust and cybersecurity. The global cybersecurity market was estimated at USD 222.66 billion in 2023. North America held 35% of total market share in 2022 fueled by the expansion of IT companies and government support towards cybersecurity awareness. Continuous advancements in big data and the IoT is expected to fuel growth as an evolving technological landscape increases demand for digital trust technologies.

Growth Projections

The global cybersecurity market is expected to grow at a compound annual growth rate (CAGR) of 12.3% from 2023 to 2030. The proliferation of online data storage has exposed end users and enterprises to big data-focused cyber-attacks including ransomware and SQL injection. Within the past year alone, 93% of organizations reported two or more identity-related breaches. The rapid uptick in cyber-attacks and the everchanging technological landscape will continue to fuel growth as demand for digital security booms.

Worldwide Spending on Cybersecurity (in $B)



Sources: Statista, McKinsey, Fortune, Nasdaq, Cypher

Cybersecurity Overview

The Variety of Industry Segments

In the cybersecurity industry, a wide variety of subsegments exist. These subsegments specialize in distinct aspects of an organization's digital security. These include Application Security (AppSec), Cloud Security, Cryptography, Data Security, Endpoint Security, Governance, Risk, and Compliance (GRC), Identity and Access Management (IAM), Threat Detection and Incident Response (TDIR), Industrial Control Systems Security (ICS), Network Security, Penetration Testing/Ethical Hacking, Security Awareness Trainings, and Security Operations (SecOps). All of these subsegments are important when it comes to protecting against cybercrime and digital threats. Global cybercrime damages are projected to reach $9.5 trillion USD by the end of 2024, a figure so high that it would rank as the third-largest economy in the world, trailing only the U.S. and China. The jump in cybersecurity threats illustrates the need for increased spending on cybersecurity measures.

Industry Segments

Application Security (AppSec): Refers to the process of finding, fixing, and preventing security vulnerabilities and external threats. It protects software at various stages of its lifecycle, from development to deployment and beyond. Some of the most critical risks facing modern applications include Injection; malicious data is "injected" into a program, and Broken Authentication; applications authentication system is improperly implemented, which ultimately allows attackers to bypass security control and gain unauthorized access.

Cloud Security: Protocols, technologies, and practices used to protect data, applications, and infrastructure involved in cloud computing from unauthorized access, data breaches, malware, and other cyberthreats. Important because in 2024, 35% of organizations will have more than 50% of their workloads in the cloud, that number is increasing everyday due to digital transformation.

Cryptography: The process of encrypting information so that only the person a message was intended for can read it. Techniques include algorithms and ciphers that transform data into unreadable format, such as public key, secret key, and hash key that use a series of binary digits like 128-bit or 256-bit encryption keys that are considered virtually unbreakable.

Data Security: Safeguards digital information from corruption, theft, or unauthorized access throughout its life cycle, using tools and processes such as data masking, encryption, and redaction of sensitive information. Data security covers hardware, software, storage devices, and user devices.

Endpoint Security: Process of protecting devices such as desktops, laptops, phones and other connected equipment from malicious threats and cyberattacks. Enables businesses to protect devices that employees use for work purposes from ransomware, phishing and data breaches.

Governance, Risk, and Compliance (GRC): Governance refers to the processes, policies, and procedures that organizations put in place to manage cybersecurity risk. Risk refers to the identification, assessment, and prioritization of potential security risks to an organization's assets. Compliance ensures that an organization is complying with laws, regulations, and standards of cybersecurity.

Sources: Cybercrime Magazine, Checkpoint, Fortinet, Kobalt

Cybersecurity Overview

Industry Segments

Threat Detection and Incident Response (TDIR): Threat Detection is the process of identifying potential security threats and other types of cybersecurity attacks. Within Threat Detection, there are four methods. Signature-Based Detection, which utilizes predefines patterns or signatures to identify threats, Behavioral Analysis, which examines patterns of behavior to detect anomalies, Machine Learning-Based Detection, which employs algorithms to analyze data and learn patterns, and Threat Intelligence, which involved monitoring external sources for information on emerging threats. Incident Response refers to the strategic approach by organizations in response to cybersecurity threats found in the threat detection phase. The steps of this process include planning, detection, containment, eradication, recovery, and remediation.

Identity and Access Management (IAM): A critical component of network security, IAM enables organizations to manage their digital identities and control user access to critical corporate information. IAM has five core responsibilities, which include authenticating user contextually by factors such as roles, location or time, logging users access events to track, administer the identity database, control user permissions, and empower administrators to oversee and adjust user access. These functions help organizations enforce secure, controlled and auditable access to resource

Network Security: Refers to the technologies, policies, people, and procedures that protect network infrastructure data, and resources from cyberattacks, unauthorized access, and data loss. Some types of Network Security solutions include Firewalls, Intrusion Prevention Systems (IPS), Antivirus and Sandboxing, Web and DNS Filtering. Attack Surface Management, Remote Access VPNs, and Network Access Control (NAC). These are put in place by organizations to protect the integrity of the firm's network.

Penetration Testing/Ethical Hacking: Penetration Testing, a cybersecurity assessment technique, is used to identify potential vulnerabilities in networks, applications, and computer systems. Some key components of Penetration Testing are planning and reconnaissance, scanning, exploitations, maintaining access, and analysis and reporting. Ethical Hacking is the practice where experts deliberately test cybersecurity defenses by simulating real life cyberattacks. This helps find security weaknesses and help organizations fix them before it's too late.

Industrial Control Systems Security (ICS): Focuses on ensuring the security of industrial control systems used in critical infrastructure and manufacturing processes. This includes the hardware and software, the system, and its operators. Refers to systems that manage and operate infrastructure such as power, manufacturing, water, transportation, and other critical services.

Security Awareness Training: Focuses on educating employees and users about security risks and best practices. Ultimately designed to help users understand their role in protecting against security breaches. More than 90% of security breaches involve human error. Which reiterates the importance and need of learning proper cyber hygiene.

Security Operations (SecOps): The practice of combining security and IT operations teams to create a unified approach that continuously monitors, detects, responds to, and prevents security threats while maintaining efficient IT operations.

Sources: Fortinet, SwimLane, Indusface, Mimecast

Cybersecurity Overview

2024 CrowdStrike Incident

On July 19, 2024, CrowdStrike released a content configuration update (Channel File 291) for its Falcon endpoint detection and response agent. This update contained a flaw that led to widespread system crashes, particularly affecting Windows-based systems. The defective update caused millions of Windows computers worldwide to experience blue screens of death (BSOD), rendering them unusable and often forcing them into bootloops, which is when a device repeatedly restarts during its startup process and cannot complete a stable boot cycle.

The outage had far-reaching consequences across various sectors. Major disruptions occurred in the airline industry, with thousands of flights canceled or delayed. Delta Air Lines, for instance, reported over $500 million in losses due to the outage, as it crippled their operations for several days. Financial institutions experienced significant operational challenges, affecting transactions and customer services. Hospitals and clinics faced disruptions in their digital health systems, impacting patient care and administrative functions. News outlets and broadcasters, including Sky News, were temporarily taken offline, affecting news dissemination.

CrowdStrike's CEO, George Kurtz, publicly apologized for the incident. The company also offered $10 Uber Eats gift cards to affected channel partners as a gesture of goodwill. CrowdStrike issued a patch to address the faulty update. Systems that could connect to the internet were able to download and install this patch. For systems stuck in a bootloop or those unable to connect to the internet, manual remediation was necessary. This involved booting into safe mode or Windows Recovery Mode and manually deleting the problematic Channel File 291. Microsoft provided guidance on this process. CrowdStrike is currently facing legal repercussions. In October 2024, Delta Air Lines filed a lawsuit against CrowdStrike, alleging that the cybersecurity firm's negligence resulted in the outage, which caused significant financial losses for the airline.

Cyber Attacks on US Infrastructure

Recently, cyber attacks on U.S. infrastructure have increased in frequency and sophistication, with critical sectors like water, electricity, and transportation often targeted.

In early 2023, the city of Oakland suffered a ransomware attack that affected city services, including online payment systems and public record access. The attack forced the city to declare a state of emergency as IT teams scrambled to restore systems, resulting in significant service delays. Oakland's experience highlighted vulnerabilities in local government networks, where outdated systems often make cybersecurity challenging.

In January 2023, a water facility in a midwestern state experienced a cyber intrusion targeting operational technology. Attackers attempted to manipulate chemical levels used in water treatment, posing a public health risk. While the intrusion was detected before any significant harm occurred, it underscored the vulnerability of water infrastructure to cyber threats and prompted further scrutiny on protective measures in water facilities.

Minnesota's power grid faced an attempted cyber attack in late 2023, where hackers tried to breach the supervisory control and data acquisition (SCADA) systems that manage electricity distribution. Although the attempt was blocked, it highlighted the grid's exposure to potential disruptions. The incident prompted utility providers and state agencies to enhance cybersecurity monitoring and increase information sharing with federal authorities to prevent future incidents.

Sources: AP News, Bleeping Computer, Crowdstrike, Port Technology International, The Scottish Sun, WSJ

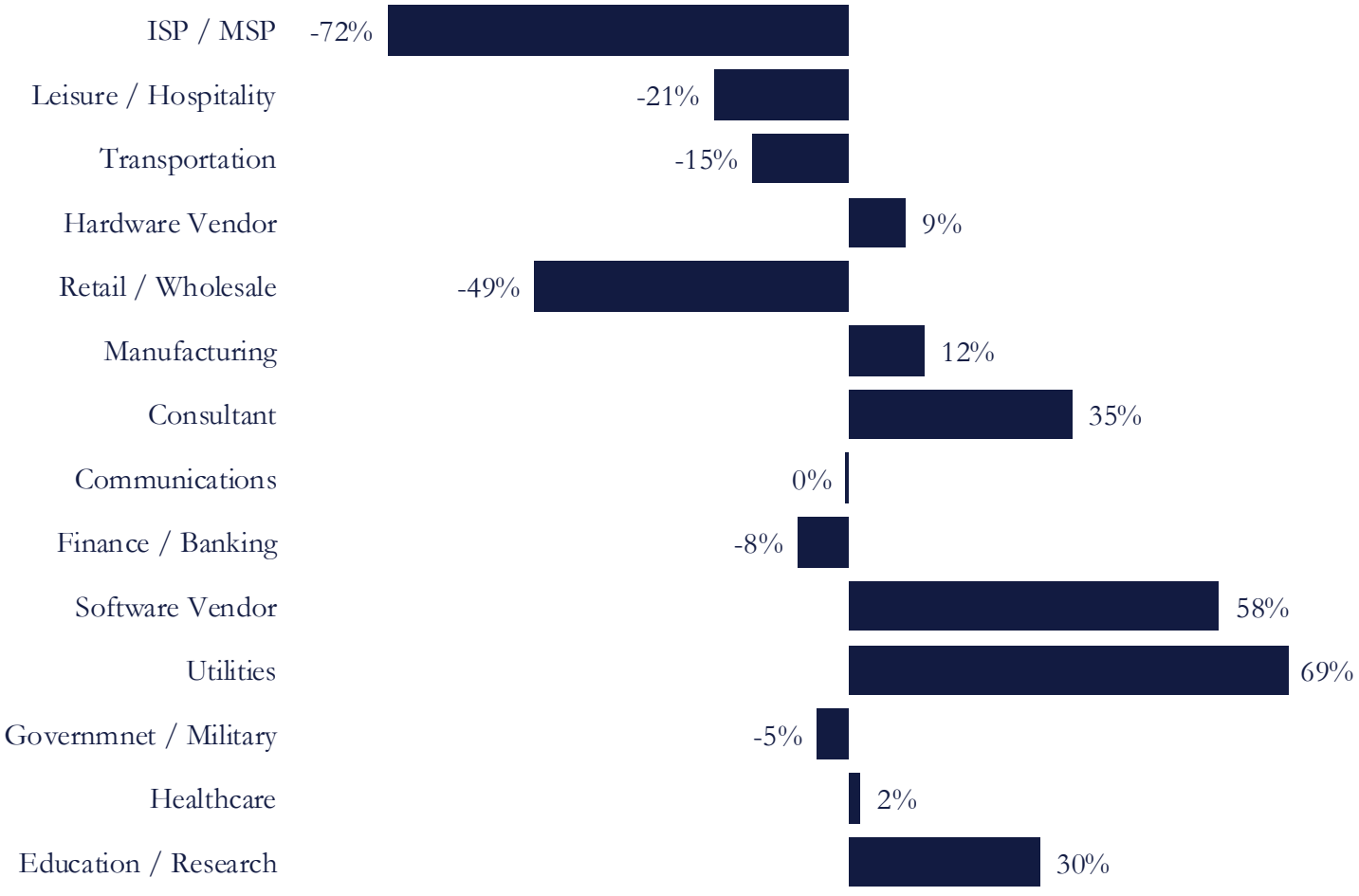
Cybersecurity Overview

The Port of Houston, a critical infrastructure hub, experienced a cyber intrusion in 2023. Attackers attempted to gain control over port logistics systems, which could have disrupted shipping operations. Quick detection and response by the port's cybersecurity team minimized damage, but the incident underscored the critical role of cybersecurity in maritime infrastructure, which is essential for trade and economic stability.

Early 2024 saw an attempted intrusion into a major gas pipeline's IT systems. Although the attempt was thwarted before damage occurred, it spurred federal agencies to update cybersecurity protocols specifically for the energy sector. It also prompted calls for increased cybersecurity investment to protect gas and oil distribution networks.

This string of attacks from cybercriminals highlights the potential public safety threat and a way that hackers can cause physical damage. With infrastructure systems connected to corporate IT networks and the internet, hackers can take advantage of weaknesses commonly found in infrastructure networks such as outdated software, poor password management, and limited resources for system updates. Resources and attention committed to cybersecurity capabilities within infrastructure facilities are often limited with facility managers facing competing priorities such as maintenance and operations. On a broader scale, company and organization leaders are increasing attention towards implementing up-to-date solutions that can protect data and information from modern-day cyber attack techniques as legacy systems leave vulnerabilities.

Average Weekly Cyber Attacks per Organization in the US (% Change in YoY)



Sources: AP News, Bleeping Computer, Check Point Research, Crowdstrike, Port Technology International, The Scottish Sun, WSJ

Trends

Identity and Access Management

Identity and Access Management (IAM) serves to provide enterprises with a way to have systems be secured while providing employees and customers off-premises access. Prior to COVID-19, employees would log in to access company servers through an on-premise computer, which allowed them to bypass the firewall in which company resources were kept behind. With remote and hybrid work being more common than ever, IAM is necessary to make sure enterprises are only letting verified employees and customers access their systems while keeping breachers out.

AI/ML in Threat Detection

With increased prevalence and use-cases of AI within enterprises, Cybersecurity firms have also adopted this trend. AI is pivotal in threat detection for these firms as they deal with massive volumes of threat intelligence inputs, and AI allows them to automate these inputs and decide on response strategies that are suitable for them. Adding ML into these services allows the AI systems to adaptively learn from new threats and attacks and continuously trains the model to improve its capabilities. Finally, these services also reduce false positives of threats, which saves the security team time, allowing them to focus on larger threats at hand.

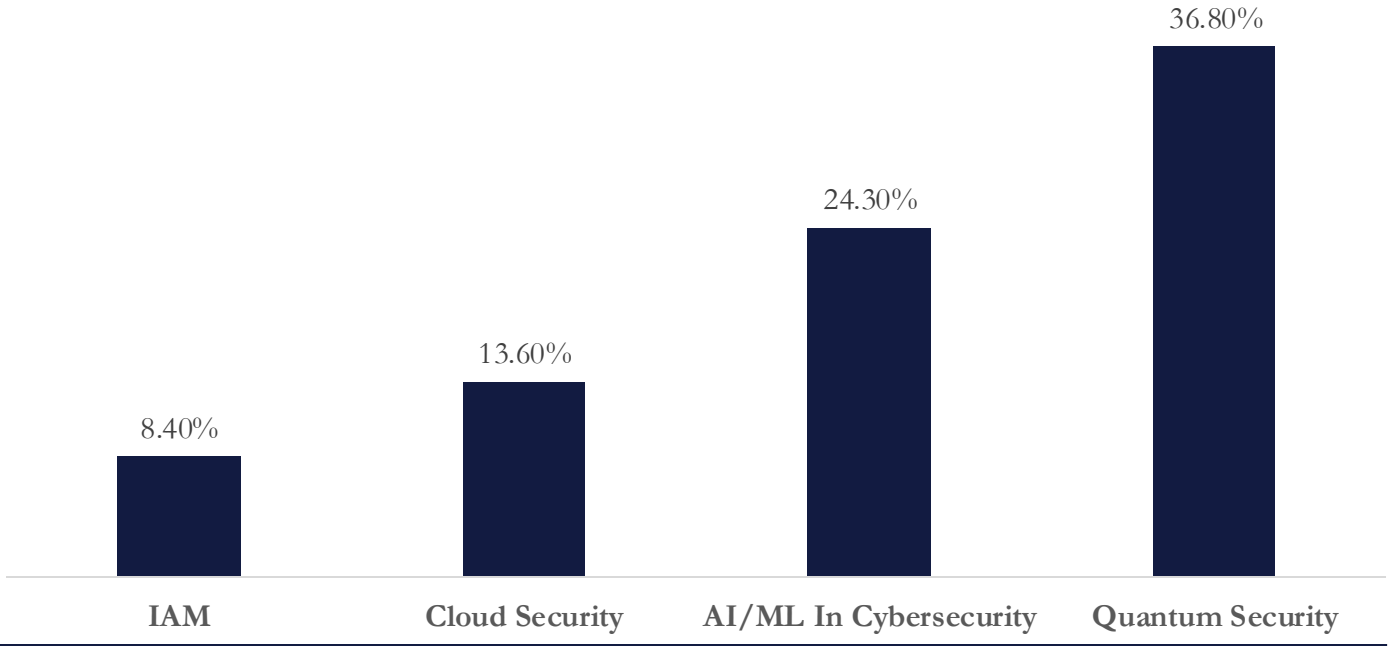
Cloud Security

Cloud Security is one of the fastest growing trends within cybersecurity with increased adoption of the cloud by enterprises. Cloud security allows for companies that have cloud environments to secure their data within these environments. Depending on the type of service your enterprise offers (IaaS, PaaS, SaaS), cloud security providers tune their offerings to best secure their data. Cloud security is growing so fast that there are some cybersecurity firms whose offerings are entirely cloud-native and don't feature any legacy products, such as Zscaler.

Quantum Security

Quantum computing allows breachers to undermine encryption, meaning that they can break through modern encryption systems which rely on complex mathematical problems to build security systems. Quantum security refers to the field in which companies attempt to build quantum-resistant algorithms that act the same as traditional mathematical problems in regard to security but are harder to breach through quantum computing. Quantum-safe network designs continue to be implemented in large-scale business in order to make sure their data and infrastructure is immune to quantum computing breaches.

CAGR of Trends



Sources: Gartner, Microsoft, Palo Alto Networks, Google Cloud, Carnegie Mellon University, Grand View Research

Headwinds

Increased Cybercriminal Sophistication

Cyber-attacks are becoming more common and costly as cybercriminal methods are becoming increasingly sophisticated with capabilities of breaking through traditional security measures. The movement towards cloud-based data management and hybrid working models opens several vulnerabilities to cyber-attacks. Because of this company leaders are finding the need to implement current and up-to-date solutions to protect company and customer data.

Cybersecurity Talent Shortage

In the trend of companies moving towards digitalization, the demand for talented candidates who can protect company data and information has increased with job postings for digital trust and cybersecurity increasing by 123% from 2019 to 2023. Because of this demand for talent, the cybersecurity industry faces a labor shortage with 54% of organizations currently struggling to recruit talent with in-demand skills such as cloud security, malware analysis, and cyber threat intelligence.

Implementation Challenges

There are several internal challenges in implementing up-to-date cybersecurity measures including lack of available talent, aligning new security measures with complex IT systems, and the process of migrating from legacy systems. External factors that generate further challenges for implementation include the evolving cyber threat landscape and changing regulatory requirements.

Budget Constraints

The cybersecurity industry is facing a multitude of challenges concerning budgeting. With the immense increase in cybercrime, the mere 9% of IT budget spending allocated to cybersecurity is no longer keeping pace. Many organizations are prioritizing budget allocation more conservatively, focusing on essential needs rather than focusing on new initiatives. Nearly 40% of CISOs say that the funding they receive falls short of what is needed to fight against cybercrime and keep their assets and citizens safe.

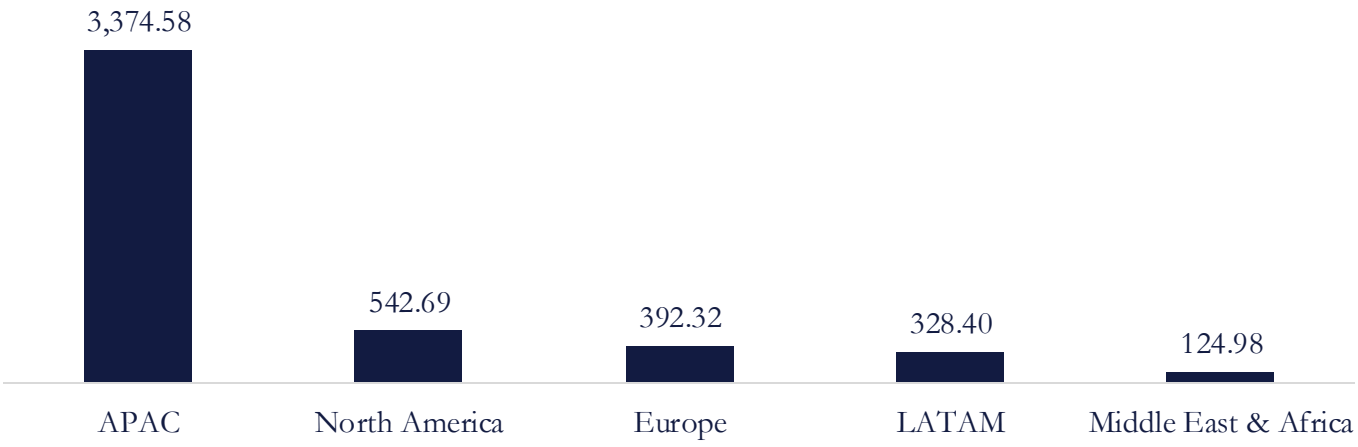
Supply Chain Vulnerabilities

There has been an increase in cybercriminals targeting third-party vendors and suppliers to breach larger systems. These attacks plot the weaknesses in the vendor systems, which causes a significant amount of risk for all the firms reliant on them. The complexity of supply chains complicates visibility and risk assessment, as well as organizations lacking the ability to scrutinize third-party practices and security protocols.

Customer Fatigue and Solution Overlap

Companies require several types of cybersecurity measures to secure sensitive information and data including network, cloud, and end-point security. With each data touchpoint requiring a different solution, organizations are forced to juggle multiple vendors and systems. This creates a customer fatigue problem where the use of several systems can create security overlap leading to inefficiencies and integration challenges.

Cybersecurity Workforce Gap Worldwide 2024 (in thousands)



Sources: EMA, Fortinet, Statista, Pew Research Center, Deloitte, Cyberdefense Magazine, Fortinet, World Economic Forum, YCharts

Tailwinds

Data Privacy Concerns

The ever-increasing amount of personally identifiable online data has bolstered market anxiety surrounding data utilization. A survey involving 5100 U.S. adults in 2023 revealed that 81% of Americans are concerned about how companies use their personal data. Another 71% shared the same fear regarding government data usage, while 67% of the public increasingly say they "don't understand what companies are doing with their data." Data security concerns are also caused by a lack of trust in the leadership of companies collecting consumer data. Meta (META) recently settled a $1.4 billion lawsuit with Texas regarding the non-consensual sale of biometrics including faces and fingerprints. Users continue to demand innovative cybersecurity as concerns perpetuate the need for digital privacy.

Regulatory and Compliance Pressure

In December of 2023, the SEC ruled that public companies must disclose material cyber-attacks within 4 days of determining any operational impacts. Many firms believe that the 4-day reporting turnover is unrealistic as it does not give compliance enough time to assess the full materiality of a given attack. The SEC reinforced their ruling by arguing that companies managing vast amounts of consumer data should already have preexisting security infrastructure capable of complying within this time frame. Regulatory and compliance pressure on companies is ultimately shaping a new standard within data management forcing companies to allocate towards their cyber security architecture.

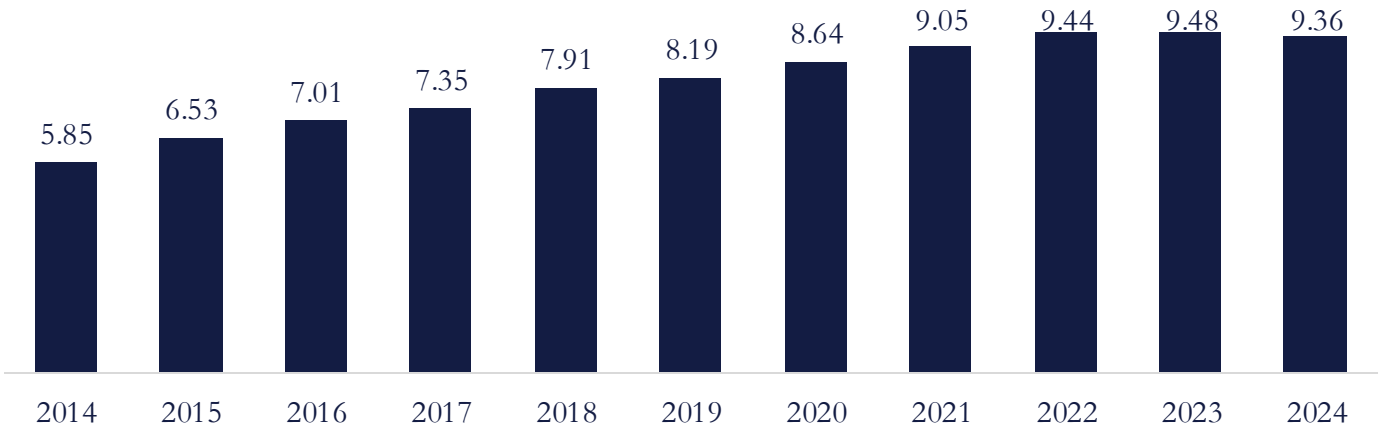
Remote and Hybrid Work Schedules

In 2024, we are seeing organizations allow their employees to work from home, either on a hybrid week to week basis, or for extended periods of time. There has been roughly a 17% increase to 37% in 2024, of US companies now working off a hybrid structured model. With the workplace schedule becoming more flexible, and digital transformation increasing, firms are more susceptible to cybersecurity threats. This is leading to firms needing to implement secure remote access solutions for employees working outside the traditional, controlled office environment, increasing the need for endpoint security, such as laptops, mobile devices, and having secure virtual private networks (VPN) for their employees. These hybrid and remote work models have helped propel growth and innovation in the field.

Digital Transformation and Cloud Adoption

The rapid adoption of digital transformation and cloud-services increases the need for cloud security. With digital transformation spending In tech expected to reach $2.5 trillion in 2024 and forecasted to reach $3.9 trillion by 2027, organizations across sectors are accelerating their transition to cloud-based systems and modernizing their infrastructure. With more sensitive data and critical applications continue to move to cloud environments, the risks associated with cyber threats escalates. This is leading to an increased investment in cybersecurity solutions, driving growth and innovation within the sector.

Average Cost per Data Breach in the US ($M)



Sources: Pew Research Center , Office Space, Backlinko

Industry Analysis

Impact on Key Sectors

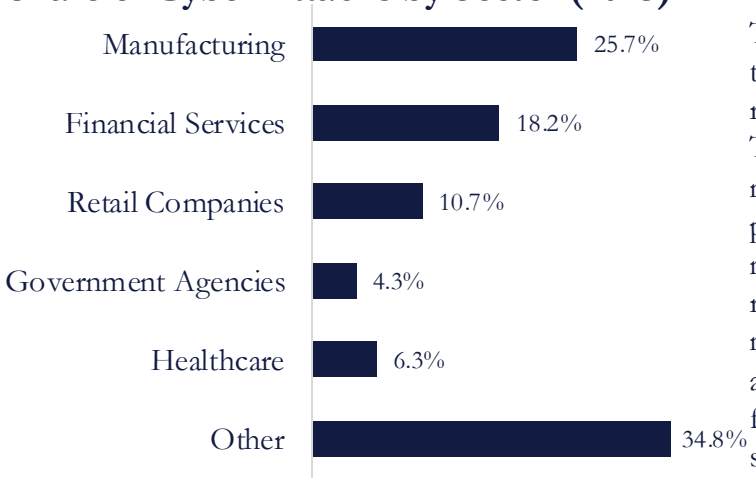
Healthcare

The healthcare industry is heavily affected by cybercrime every year due to the vulnerable nature of the sector. Organizations are primarily experiencing ransomware incidents, supply chain attacks, Spoofing/impersonation attacks, and compromised cloud-based user accounts, with cloud-based user account attacks significantly leading. The lack of employee awareness has become a main risk; therefore, firms are mandating security training awareness programs, simulating phishing attacks, using anti-virus / anti-malware, and monitoring their employees with audits and assessments in the areas most vulnerable to employees' lack of awareness.

Retail Companies

Retailers are heavily affected by cybercrime, as they handle vast amounts of sensitive customer data which include payment information, personal details, and purchasing history. This industry faces challenges with high turnover rate, and seasonal workers making cybersecurity a low priority. Attacks such as phishing, ransomware, advanced persistent threats, and supply chain attacks are among the most common threats. These attacks can be very expensive with the average cost of a data breach costing $3.28 million. Some ways retailers are combatting against cybercrime are by collecting, storing, and migrating data to more secure platforms and systems, vetting third-party data controllers and software and IT systems, trainings.

Share of Cyber Attacks by Sector (2023)



Government Agencies

Government agencies are one of the most targeting sectors by cybercriminals. Cybercriminals target these organizations because they often rely on legacy systems and outdated software and lack resources and internal expertise to improve their security posture. The costs of these attacks can total millions and affect tens-of-thousands. A few factors that can significantly improve their cybersecurity are implementing security awareness trainings that focus on phishing threats, conducting basic file backups to limit the impact of ransomware , and secure the cloud. Although, the threats are not going away, government agencies can help mitigate the successful attacks with these safeguards.

Financial Services

The financial services sector is one of the most targeted industry, accounting for nearly one-fifth of the total attacks. Financial firms, such as banks, credit unions, insurance companies, and investment firms are the targeted due to the large amounts of money, sensitive data, and transactions they handle. Over the last 20 years, the cybercrime damages in the financial sector has been over $12 billion in losses. Financial institutions are preventing these threats and safeguarding from financial losses, losing consumer trust, and sensitive data loss by implementing web application firewalls, DDoS protections, anti-fraud and online fraud prevention, and security awareness and training programs.

Manufacturing

The manufacturing sector is consistently the most targeted sector, with malware attacks and ransomware attacks making up the majority threats. The low tolerance for downtime in the industry makes it an attractive target to criminals as production halts are not an option for organizations making companies more likely to pay attacks to relent rather than combat with attackers for an even more costlier downtime period. Ways manufacturers are fighting against these attacks are by installing firewalls and antivirus software as well as anti-spyware and educating their employees.

Sources: Sources: Ponemon Institute, Artic Wolf, IMF, Imperva, Statista, Cybermagazine

Regional Analysis

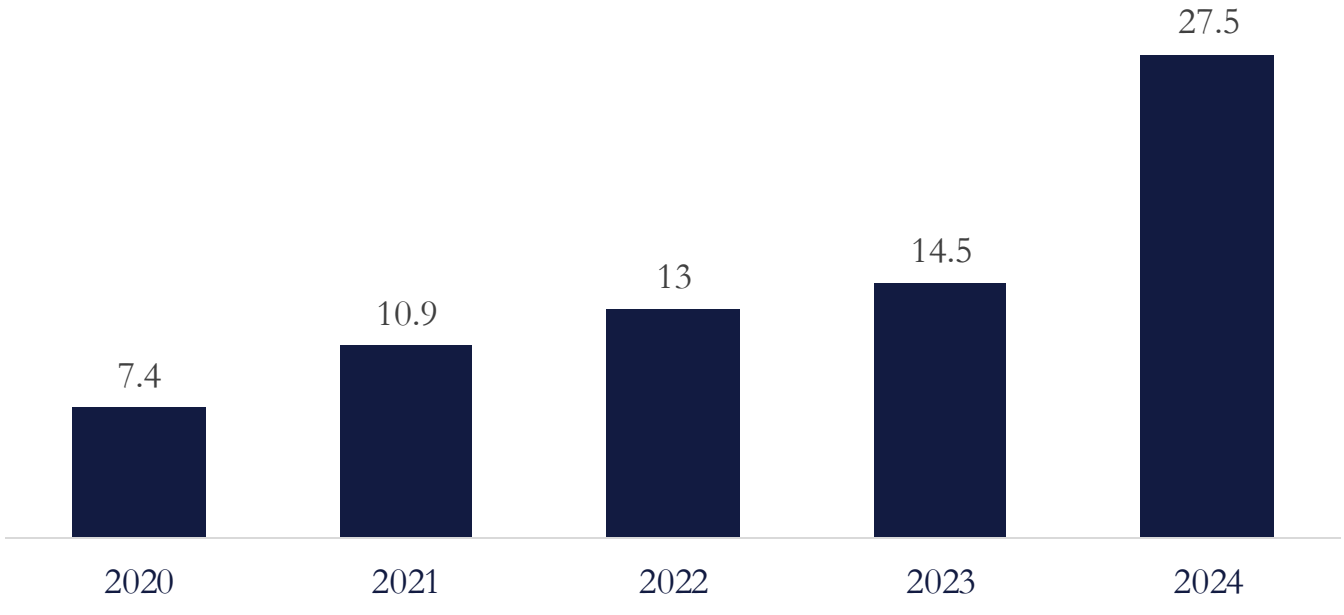
United States

- The United States employs a wide variety of measures to protect data through Cybersecurity, including legislation, federal agencies, and subsidiaries/grants
- The Health Insurance Portability and Accountability Act (HIPAA) is an example of legislation the United States has passed, with this act requiring healthcare providers on the cloud to adhere to specific healthcare cybersecurity regulations in order to protect patient data.
- Another example is The Federal Information Security Modernization Act (FISMA), which requires government agencies, such as state and federal governments, to employ specific cybersecurity methods in order to safekeep their data and information systems against breaches.
- Additionally, the United States employs various federal agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), which was founded in order to protect key infrastructure sectors, such as energy, from cyber attacks.
- Finally, the United States also offers grants and subsidies to entities who work to address cybersecurity risks for local, state, and tribal governments.

European Union

- Similar to the United States, the European Union also deploys various measures of legislation in order to promote data privacy and infrastructure protection through Cybersecurity.
- Compared to the United States, the EU is more regulatory and rights-focused regarding heir broader approach for Cybersecurity.
- The first piece of legislation within the EU that is enforced is the General Data Protection Regulation (GDPR) and is focused on protection of civilian data. This was enforced in 2018, and not only applies to companies within the EU but also any company that process data related to EU civilians. Key principles of the GDPR include only accessing the data that is needed, must be processed only for the specific reasons the company needs it, and all processing of the data must be done ethically and transparently.
- Another piece of legislation enacted was the NIS2, which was revamped in 2022 in order to include new industries and specific verticals within the scope. Through this act, it made sure key infrastructure segments are adhering to Cybersecurity safeguards and are implementing policies enforced by NIS2 into their business.

US Budget for Cybersecurity ($B)



Sources: Statista, GSA.gov, ConnectWise.com

Largest US Cybersecurity Companies

Public cybersecurity companies continue to grow in size, as notable names like Palo Alto Networks and CrowdStrike have had their respective stock price's grow by over 45% over the last year, and over 360% in the last 5 years. These companies continue to have increased implementation in a world where companies are either completely internet based or have critical business components that are internet based. These companies typically trade at extremely expensive multiples due to the market being willing to pay extra for a segment with continually increasing adoption, therefore driving growth. Among public cybersecurity firms, revenue multiples increased by 22% at the median, and up to 65% for industry leaders, exhibiting the large multiple expansion in public markets.

Logo	Company	Ticker	Description	Market Cap
	Cisco Systems	CSCO	Technology conglomerate that offers numerous IT solutions, including cybersecurity	$221.22B
	Palo Alto Networks	PANW	Firm that offers its flagship product of firewalls, but has expanded into endpoint security	$118.08B
	CrowdStrike	CRWD	Firm that focuses specifically on endpoint security, making that its flagship product	$74.31B
	Fortinet	FTNT	Firm that offers numerous avenues of cybersecurity as an integrated solution	$60.27B
	Zscaler	ZS	Firm that focuses on cloud-native and zero-trust cybersecurity	$27.84B
	Leidos	LDOS	Firm that primarily focuses on offering solutions to government and defense organizations	$24.41B
	Check Point Software	CHKP	Firm that allows for management of all cybersecurity solutions under one platform	$18.75B
	Cloudflare	NET	Firm that is widely known for traffic regulation on websites, such as bot identification	$29.92B
	Gen Digital	GEN	Firm that focuses on anti-malware and antivirus solutions for individuals	$17.40B
	Akamai Technologies	AKAM	Leading provider of content delivery networks, lowering latency for users when accessing websites	$15.24B

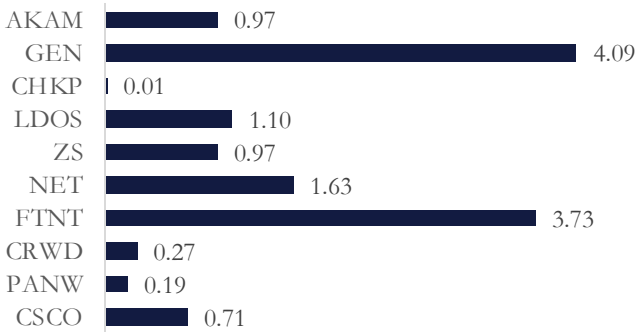
Sources: Strategy of Security, Google Images, Yahoo Finance

Liquidity and Leverage

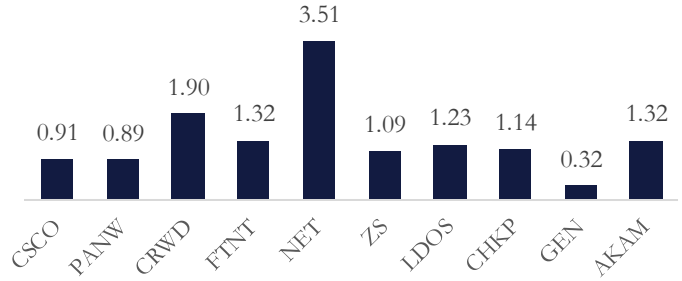
Company	Operating Cash Flow	Current Assets	Current Liabilities	Total Liabilities	Liquidity			Leverage		
					Current Ratio	Quick Ratio	Cash Ratio	Debt / Equity	Debt / Assets	Debt / Inv. Capital
CSCO	10.88	36.86	40.58	78.96	0.91	0.71	0.19	0.71	0.25	0.32
PANW	3.26	6.85	7.68	14.82	0.89	0.77	0.20	0.19	0.07	0.21
CRWD	1.33	4.76	3.70	4.31	1.90	1.72	1.09	0.27	0.12	0.21
FTNT	1.92	4.43	3.72	7.72	1.32	1.19	0.59	3.73	0.14	0.65
NET	0.30	1.98	0.57	1.99	3.51	3.39	0.26	1.63	0.52	0.41
ZS	0.78	3.40	3.11	3.43	1.09	1.01	0.46	0.97	0.26	0.49
LDOS	1.40	4.01	2.99	8.44	1.23	1.03	0.31	1.10	0.41	0.37
CHKP	1.05	2..26	1.92	2.87	1.14	1.08	0.32	0.01	6.18	0.93
GEN	2.14	1.36	2.65	13.58	0.32	0.27	0.19	4.09	0.55	0.45
AKAM	1.53	1.80	0.84	5.30	1.32	1.20	0.23	0.97	0.12	0.13
Lower	1.12	2.05	2.10	3.65	0.96	0.83	0.21	0.38	0.13	0.24
Median	1.47	4.01	3.05	6.51	1.19	1.06	0.29	0.97	0.26	0.39
Mean	2.46	6.77	6.78	14.14	1.36	1.24	0.38	1.37	0.86	0.42
Upper	2.09	4.68	3.72	12.30	1.32	1.20	0.43	1.50	0.49	0.48

CSCO's high OCF in comparison with peers would initially illustrate robust financial solidity. Even though CSCO's OCF is nearly 5x the industry mean of 2.46, current liabilities of 40.58 and current assets of 36.86 have CSCO's current ratio falling short of 1 at 0.91. This demonstrates a -24.56% decline contrasted against CSCO's 12-month average current ratio of 1.20. This drastic decline could mark the beginning of a consistent decline in liquidity for CSCO unless the growing difference in asset value and liabilities is properly mitigated.

Debt/Equity Ratio



Current Ratio



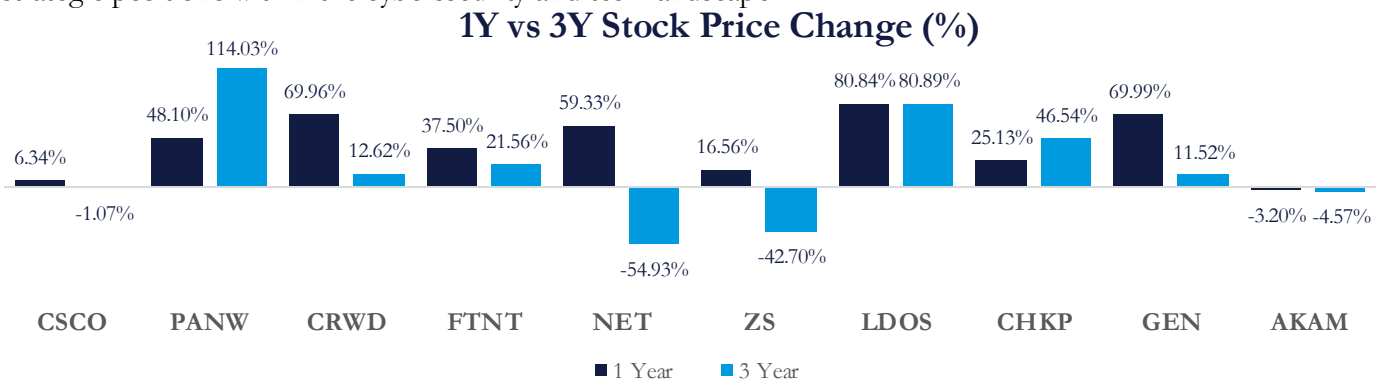
Many of the firms within this set display strong liquidity ratios as seen with NET and CRWD. With a current ratio of 3.51 and a quick ratio of 3.39, NET triples the respective industry means and is poised to comfortably handle short-term debts. GEN, however, has comparatively deflated current and quick ratios raising concerns surrounding short-term solvency. Coupled with low liquidity ratios, GEN is heavily levered with a debt-to-equity ratio of 4.09. Unlike FTNT, who also possesses a high debt-to-equity ratio of 3.73, GEN does not indicate strong liquidity ratios raising market speculations regarding GEN's ability to gradually de-lever their capital structure.

Sources: Yahoo Finance

Profitability and Growth

Company	Revenue	EBITDA	Net Income	Total Assets	Total Equity	EBITDA / Revenue	ROA	ROE	1 Year	3 Year
CSCO	56,998	19,677	15,981	124,413	45,457	0.35	22.73%	9.40%	6.34%	(1.07%)
PANW	8,027	2,348	1,948	19,990	5,169	0.29	15.07%	71.95%	48.10%	114.03%
CRWD	3,516	978	927	7,202	2,890	0.28	2.72%	7.55%	69.96%	12.62%
FTNT	5,537	1,815	1,489	8,052	288	0.33	17.30%	7947%	37.50%	21.56%
NET	1,477	298	236	2,916	881	0.20	(3.75%)	(13.48%)	59.33%	(54.93%)
ZS	2,167	504	508	4,704	1,274	0.23	(1.44%)	(5.94%)	16.56%	(42.70%)
LDOS	16,277	2,097	1,345	13,338	4,667	0.13	9.29%	27.66%	80.84%	80.89%
CHKP	2,524	1,097	1,034	5,512	2,828	0.43	15.12%	29.85%	25.13%	46.54%
GEN	3,857	2,317	1,324	15,471	2,098	0.60	3.91%	27.94%	69.99%	11.52%
AKAM	3,927	1,656	1,011	10,087	4,754	0.42	6.57%	13.91%	(3.20%)	(4.57%)
Lower	1,477	298	236	2,916	288	0.13	(3.75%)	(13.48%)	(3.20%)	(54.93%)
Median	3,892	1,736	1,179	9,070	2,859	0.31	7.93%	20.79%	42.80%	12.07%
Mean	10,431	3,279	2,580	21,169	7,031	0.33	8.75%	811.58%	41.06%	18.39%
Upper	56,998	19,677	15,981	124,413	45,457	0.60	22.73%	7947.00%	80.84%	114.03%

The chart above summarizes key financial metrics of several major cybersecurity companies, including Cisco Systems, Palo Alto Networks, CrowdStrike, and others. Cisco Systems leads in revenue, EBITDA, and net income, highlighting its dominant market position with $56,998 million in revenue and $15,981 million in net income. Companies such as Palo Alto Networks and Gen Digital exhibit robust return on equity (ROE) with 71.95% and 27.94%, respectively, suggesting strong profitability relative to their equity. Meanwhile, some firms like Cloudflare and Zscaler have negative ROA and ROE, indicating challenges in generating returns from their assets and equity. EBITDA margins range significantly across the companies, with Gen Digital having the highest EBITDA/Revenue ratio at 0.60, while Leidos has the lowest at 0.13. Performance over the past year varies, with exceptional growth seen in Palo Alto Networks (48.10%) and significant declines in Cloudflare (-59.33%) over three years. Median financials indicate a typical company in this sector has around $3,892 million in revenue, an EBITDA of $1,736 million, and an ROE of 20.79%. The diversity in metrics underscores the varying levels of financial health and strategic positions within the cybersecurity and tech landscape.



Sources: Yahoo Finance

Valuation Ratios

Company	Market Cap ($B)	Enterprise Value ($B)	Diluted EPS (TTM)	EV / Revenue	EV / EBITDA	Trailing P/E	Forward P/E	Price / Sales (TTM)	Price / Book (MRQ)
CSCO	221.22	234.33	2.54	4.36	14.88	21.85	15.60	4.19	4.87
PANW	118.67	117.44	7.29	14.63	92.01	49.81	57.47	15.99	22.96
CRWD	74.31	71.06	0.70	20.21	167.43	439.32	72.46	21.41	26.05
FTNT	60.27	57.93	1.69	10.46	34.19	46.63	34.25	11.04	209.14
NET	29.92	29.60	-0.30	20.03	746.80	--	104.17	20.01	33.94
ZS	27.84	26.67	-0.38	12.30	411.37	--	63.69	12.60	21.85
LDOS	24.41	28.37	8.78	1.74	13.75	20.82	17.86	1.54	5.29
CHKP	18.75	17.28	7.30	6.85	16.79	23.36	16.95	7.73	6.63
GEN	17.42	25.27	0.99	6.54	12.57	28.56	12.79	4.63	8.30
AKAM	15.21	18.22	4.03	4.64	13.34	24.96	14.66	3.99	3.21
Lower	20.17	25.62	0.77	5.12	14.03	22.98	15.94	4.30	5.63
Median	28.88	28.99	2.12	8.66	25.49	26.76	26.06	9.39	15.08
Mean	60.80	62.62	3.26	10.18	152.31	81.91	40.99	10.31	34.22
Upper	70.80	67.78	6.48	14.05	148.58	47.43	62.14	15.14	25.28

The growing need and demand for cybersecurity in the shift towards digitalization is reflected through several valuation metrics including price-to-earning ratios, price-to-sales and book ratios, and enterprise value-to-revenue multiples showing high investor expectations for future growth. Notable trailing price-to-earnings (P/E) ratios include Palo Alto Networks (PANW), CrowdStrike (CRWD), and Fortinet (FTNT) with ratios of 49.81, 439.32, and 46.63 respectively, reflecting the significant share price premiums investors are willing to pay, indicating confidence in the industry's growth. High growth expectations and premium valuations throughout the cybersecurity industry are also shown through high enterprise value to revenue multiples of CrowdStrike (CRWD), Cloudflare (NET), and Palo Alto Networks (PANW) with multiples of 20.21, 20.03, and 14.63 respectively. With investors expecting future earnings and growth, this creates a general trend in the data forecasting a lower forward P/E as these companies continue to scale and achieve higher profitability. Cybersecurity companies tend to be asset-light with many of them relying on software or intellectual property, this allows them to generate revenue without needing large capital expenditures keeping more cash in reserves, resulting in a smaller enterprise value relative to market cap which is seen through the data. Through the analysis of valuation ratios, it is evident that cybersecurity's importance in protecting an organization's digital assets is realized by the market and investors through the premiums on several valuation metrics.

Sources: Strategy of Security, Google Images, Yahoo Finance

M&A Activity

Deal Flow Commentary

Broader deal market activity within the Cybersecurity landscape continues to heat up as larger cybersecurity firms such as Palo Alto Networks, CrowdStrike, Fortinet, and Cisco look to expand their moat within the industry. Although cybersecurity deal activity is lower compared to 2021, it is believed that it is a reflection of broader market trends with higher interest rates, making deal activity more infrequent.

Deal Amount: $215M

FORTINET

Acquired

LACEWORK

08/02/2024

Advisors

FENWICK

GS

Deal Synopsis:
Fortinet, a leader in driving the convergence of networking and security, acquired Lacework, a data-driven cloud security company, in efforts to offer a more comprehensive solution by integrating cloud security into their offerings. The deal is expected to close in the back half of 2024, and hopes to drive revenue synergies for Fortinet by penetrating into the cloud-native vertical of Cybersecurity

Deal Amount: $200M

CROWDSTRIKE

Acquired

FLOW SECURITY SYSTEMS

03/05/2024

Advisors

WHITE & CASE

EBN Erdinast Ben Nathan Toledano

Deal Synopsis:
CrowdStrike, a leader in endpoint security and currently one of the largest publicly-traded cybersecurity firms, announced a deal to acquire Flow Security, the industry's first and only cloud data security runtime solution. Through this acquisition, CrowdStrike aims to deliver flow security solutions, allowing customers to consolidate cloud point solutions and have greater visibility into data flows for customers.

Deal Amount: $28B

CISCO

Acquired

splunk>

03/18/2024

Advisors

Morgan Stanley

Qatalyst PARTNERS

Deal Synopsis:
The largest cybersecurity acquisition recorded to date, Cisco agreed to acquire Splunk for $28B. The deal was announced in September of 2023, and was closed by March of 2024. Although Splunk is not a cybersecurity firm and does not provide cybersecurity offerings, Cisco aims to utilize Splunk by leveraging their data analytics to provide users a more comprehensive security platform and improved threat detection.

Sources: Fortinet, Crowdstrike, Cisco, WSJ, SEC Edgar

IPO Activity

Deal Flow Commentary

The cybersecurity industry saw a resurgence of IPO activity in early 2024, with Rubrik making their public market debut, marking a shift from the sectors quiet period over the previous few years. With the increasing threats of cybercrime, we are seeing more firms looking to go public such as Cato Networks, who are in the midst of hiring banks for a 2025 IPO.

$752 Million

Rubrik

$32 / Share

April 2024

Lead Underwriters

Rubrik is an American cybersecurity firm backed by Microsoft (MSFT), which focuses on cloud data management and security. The company went public due to experiencing rapid growth, up 47% in subscriptions in 2024, due to increases in cybercrime and other threats. With 752 million raised, they plan to continue to expand their market position and continue to invest in the firm, expanding their AI and Machine Learning capabilities as they note that risks could be more significant as AI develops.

$1.2 Billion

SentenielOne

$35 / Share

June 2021

Lead Underwriters

SentinelOne is an American cybersecurity firm that specializes in Endpoint Security, which protect devices such as laptops and phones that employees use. By raising $1.2 billion and having an implied valuation of $8.9 billion, this became the highest-valued cybersecurity IPO in history. They went public due to their continued rapid YoY revenue growth and their strategic objectives such as M&A where they acquired Attivo Netorks (2022) which diversified their offerings.

$800 Million

GitLab

$77 / Share

October 2021

Lead Underwriters

GitLab is a leading provider of the DevOps platforms that enables professionals to perform all the tasks in a project. GitLab went public almost 10 years from their start date because of revenue scale, revenue predictability and compliance. This 100% full remote company raised $800 million which has helped them convert users from their free product offerings to paying customers by selling addition products and services. This has helped scale their business and increase their YOY revenues

Sources: Pitchbook, Reuters, Investopedia, CNBC, Forex, Techcrunch

Emerging Companies

Deal Flow Commentary

With cybercrime and cyber threats increasing YoY companies are forced to spend millions of dollars a year to safeguard against these attacks, leading to the growth of many startups and developing cybersecurity firms. These emerging companies have faced multiple challenges including more sophisticated threats, talent shortages, and supply chain constraints but still have had a strong year financially and even brighter futures ahead.

Snyk

1,226 Employees

$1.07B Raised to Date

Notable Investors

Lone Pine Capital

QIA Qatar Investment Authority

Tiger Global

Snyk is a developer of security analysis tools designed to identify open-source vulnerabilities. Their software helps find, fix, and monitor known threats in open-source dependencies, secure authoring and consumption of open-source code, allowing firms and enterprises to use open source without compromising security. Snyk recently acquired the developer security firm, Probely, and partnered with Orca Security to strengthen holistic application security. Reports suggest an IPO as soon as 2025.

Tanium

2,094 Employees

$997.3M Raised to Date

Notable Investors

Fidelity Investments

Wellington Management

Geodesic Capital

Tanium is a developer of an endpoint management and security platform that enables firms to monitor their digital environments effectively while responding to cyber threats swiftly. In 2024 alone, Tanium has launched new products in patch management and AI endpoint management and confirmed their involvement in the general availability of Microsoft's newly offered products. These advancements hold a bright future for the firm.

Nozomi Networks

280 Employees

$257.1M Raised to Date

Notable Investors

Lux

Notable Capital

Mitsubishi Electric

Nozomi Networks is a developer of online cybersecurity platforms that provides real-time visibility into process network communications and configurations. They are entering the generating revenue stage, with their seventh round of funding this year totaling $100M. The funding will be used to help scale product development and efforts as well as its go-to-market approach. Recently, they have collaborated with cyber defense company "Mandiant" to deliver comprehensive solutions for OT, IT, and IoT threat detection and responses.

Sources: Pitchbook

BBR T BULL & BEAR TECHNOLOGY

BBR BULL & BEAR RESEARCH

Initiating Coverage:

Palo Alto Networks

Palo Alto Networks

Company Overview

Palo Alto Networks, established in 2005 by Nir Zuk, is a leading cybersecurity company headquartered in Santa Clara, California. The company offers a comprehensive platform encompassing network security, cloud security, and security operations. Serving over 80,000 enterprise customers worldwide, including more than 75% of the Global 2000, Palo Alto Networks is recognized for its advanced threat detection and prevention capabilities. The company's innovative approach integrates artificial intelligence and automation, enforcing Zero Trust principles to enhance cybersecurity across various industries.

Latest News

- Reported fiscal Q4 2024 net income of $358M, adjusted earnings of $1.51 per share, and $2.19B in revenue, exceeding expectations.
- Acquired Dig Security for $400M and Talon Cyber Security for $625M to enhance cloud and device security.
- Launched AI-driven solutions in May 2024 to address advanced threats and secure AI adoption.
- Partnered with IBM to integrate WatsonX AI models and offer AI-powered security consulting.

Market View

Market Bulls View

- Institutional investment in PANW has remained robust, with institutions holding approximately 79.82% of the company's stock.
- PANW's reported 1,100+ platformizations across its customer base, indicating successful adoption of their product ecosystem.
- Speculation suggests Palo Alto Networks may continue pursuing strategic acquisitions to further strengthen its position, following recent high-profile purchases of Dig Security and Talon Cyber Security.

Market Bears View

- Fear that PANW's stock valuation may have surged too rapidly, potentially outpacing the company's earnings growth. This rapid increase raises concerns about the sustainability of its current market price.
- PANW experienced a 14% decline in billings, missing investor expectations. This decline has raised concerns about the company's ability to generate new business at a sufficient pace.
- PANW's strategic shift towards platformizations and long-term deals involves transitioning from traditional hardware-based solutions to cloud-based and software-defined offerings. This transition carries risks, including potential challenges in managing the shift and retaining customers.

Thesis

PANW has displayed strong financial performance with revenue growth of 25.29% and 16.46% YoY in FY 2023 and FY 2024 respectively. Expected future growth is justified by the 30% YoY increase in their annual recurring revenue providing top-line stability and future cross and up-selling opportunities. With tailwinds such as the increased prevalence of cyber threats and a shift towards digitalization, PANW is well-positioned for long-term growth and is capable of delivering future shareholder value, justifying a buy rating.

Sources: Cyber Magazine, PitchBook, Bloomberg, MarketWatch, Palo Alto Networks

Stock Rating: BUY

Price Target: $436.97

Price (11/29/24): $386.44

Upside: 12.82%

Ticker: PANW

Research Team

Andrew Shih

Raahil Gunaratne

Sanjit Kosaraju

Craig Ottaviano

Rahul Yaganti

EV: $125.76B

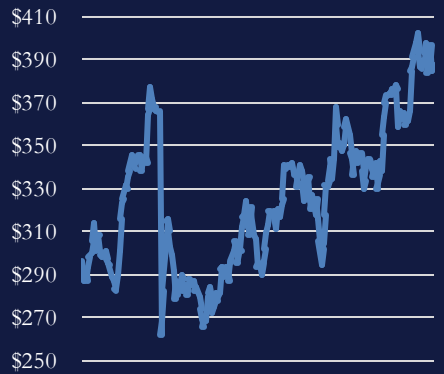
Market Cap: $126.99B

EV/ Revenue: 15.67

P/E: 53.30

P/BV: 24.40

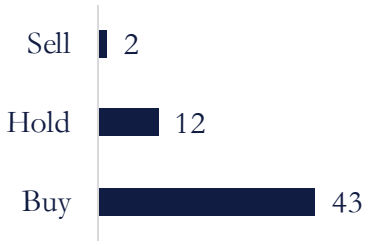
PANW 52wk Range



Alternative Valuations

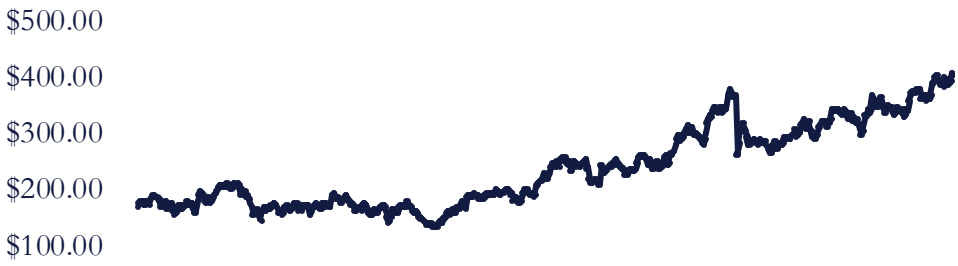
Palo Alto Networks

Consensus Rating



12M Price Target: $420.13

Price Analysis (3Y, USD)



Firm	Broker	Date	Analyst Rating	Price Target	Comparative Analysis
BBR	Tech Coverage	11/29/24	Buy	$436.97	
BMO	Keith F Bachman	11/21/24	Outperform	$425.00	
Morgan Stanley	Hamza Fodderwala	11/21/24	Overweight	$446.00	
WEDBUSH	Daniel Ives	11/21/24	Outperform	$400.00	
Scotiabank	Patrick Colville	12/02/24	Sector Outperform	$400.00	
Deutsche Bank	Brad A Zelnick	11/21/24	Buy	$415.00	
Goldman Sachs	Gabriela Borges	11/21/24	Buy	$421.00	
J.P.Morgan	Brian Essex	11/21/24	Overweight	$449.00	
Jefferies	Joseph Gallo	12/05/24	Buy	$450.00	

Select Commentary

Needham Bank **Rating**: Buy **Price Target**: $450.00

- ARR/Revenue of 4.52B/2.14B grew 40% YoY beating the Street by 3.5%/1%
- PANW can produce solid revenue and FCF/share gains over the coming years
- Growth upside, accelerated efficiency initiative, and slowing headcount growth should drive upside to margins and free cash flow
- PANW can drive incremental FCF/share growth over the coming years as a platform of choice while focusing on profitable growth and leading the change in security consolidation

Research Team:

Mike Deszort, CFA

Mike Cikos, CFA

Jeffrey Hopson

Sources: Bloomberg Terminal


BBR T BULL & BEAR TECHNOLOGY
BBR BULL & BEAR RESEARCH
Initiating Coverage:
CrowdStrike

CrowdStrike

Company Overview

CrowdStrike, founded in 2011 by George Kurtz, is a leading cybersecurity company headquartered in Austin, Texas. The company specializes in endpoint protection, cloud workload security, and threat intelligence. Serving over 29,000 customers globally, including numerous Fortune 500 companies, CrowdStrike is recognized for its AI-driven real-time threat detection and response capabilities. With a cloud-native approach and a focus on automation, CrowdStrike continues to redefine cybersecurity standards, helping organizations across industries stay protected from advanced cyber threats.

Latest News

- On November 21, 2024, Push Security appointed Kevin Arsenault, a former sales leader at CrowdStrike, as its new Chief Revenue Officer.
- Following the July 2024 incident, CrowdStrike faces multiple lawsuits. Notably, Delta Air Lines filed a lawsuit seeking over $500 million in damages due to operational disruptions caused by the faulty update.
- Competitors like SentinelOne have capitalized on CrowdStrike's recent challenges. SentinelOne's market position has strengthened, as evidenced by its stock value and strategic partnerships

Market View

Market Bulls View

- Annual recurring revenue (ARR) grew to $3.15 billion, with a customer base exceeding 23,000, reflecting a 41% year-over-year growth. The company's gross margin remained robust at 76%, indicating operational efficiency.
- CRWD continues to enhance its Falcon platform by integrating new features like AI Security Posture Management (AI-SPM) and Data Security Posture Management (DSPM). These improvements provide streamlined threat detection, expanded response capabilities, and comprehensive cloud security.
- CRWD has expanded partnerships with Cloudflare to enhance device-to-network security and Google Cloud for multi-cloud AI-powered protection.

Market Bears View

- Analysts have expressed concerns that CrowdStrike's premium pricing strategy may face pressure as customers seek alternatives or demand concessions following the outage.
- Speculation that the company's ARR metrics may include overly optimistic assumptions about contract renewals and ongoing negotiations. This scrutiny raises doubts about the transparency and reliability of its financial disclosures.

Thesis

In FY 2024 CRWD showcased a top-line increase of 36.33% YoY reaching $3.05B with 83.77% coming from recurring revenue signifying top-line stability. Expectations for continued success are driven by CRWD's dominance in the expanding cybersecurity industry through strategic acquisitions and proven record in retaining and up-selling to current customers. CRWD is poised for long-term growth through its strong financials and scalable technology supported by secular tailwinds that enable CRWD to capture much of the expanding total addressable market while increasing margins on current customers.

Sources: Yahoo Finance, PitchBook, New York Post, WSJ, MarketWatch

Equity Research
Technology | Cybersecurity
Fall 2024

Stock Rating: BUY

Price Target: $377.57

Price (11/29/24): $345.97

Upside: 9.13%

Ticker: CRWD

Research Team

Andrew Shih

Raahil Gunaratne

Sanjit Kosaraju

Craig Ottaviano

Rahul Yaganti

EV: $83.39B

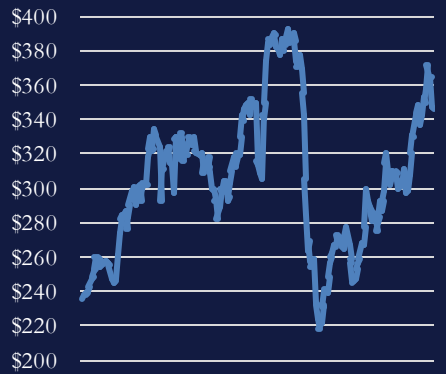
Market Cap: $86.60B

EV/ Revenue: 23.72

P/E: 512.01

P/BV: 30.35

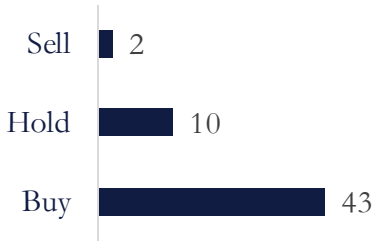
CRWD 52wk Range



Alternative Valuations

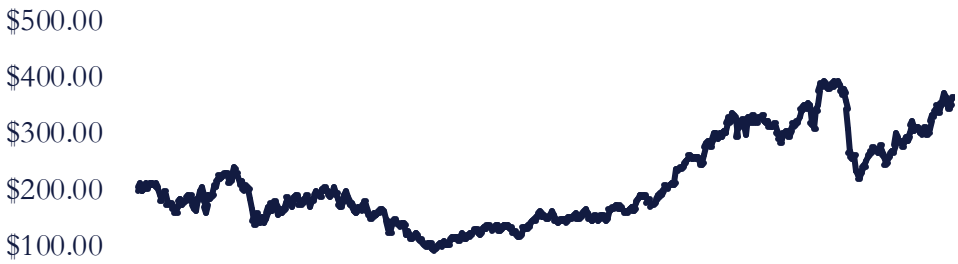
CrowdStrike

Consensus Rating



12M Price Target: $382.13

Price Analysis (3Y, USD)



Firm	Broker	Date	Analyst Rating	Price Target	Comparative Analysis
BBR	Tech Coverage	11/29/24	Buy	$377.57	
MIZUHO	Gregg Moskowitz	12/06/24	Outperform	$385.00	
Morgan Stanley	Hamza Fodderwala	12/05/24	Overweight	$390.00	
WEDBUSH	Daniel Ives	12/05/24	Outperform	$390.00	
Scotiabank	Patrick Colville	12/02/24	Sector Perform	$300.00	
Deutsche Bank	Brad A Zelnick	11/27/24	Hold	$355.00	
Goldman Sachs	Gabriela Borges	11/27/24	Buy	$372.00	
J.P.Morgan	Brian Essex	11/27/24	Overweight	$372.00	
Jefferies	Joseph Gallo	11/27/24	Buy	$415.00	

Select Commentary

Wells Fargo **Rating**: Overweight **Price Target**: $400.00

- CRWD can continue to fuel its growth by taking share from the vast installed base of legacy vendors
- CRWD has extended its platform beyond traditional endpoints to protect cloud workloads, which should further augment growth
- CRWD's emerging solutions should continue to add growth
- CRWD can continue generating strong FCF growth at scale

Research Team:

Andrew Nowinski

Vinod Srinivasaraghavan CFA

Sources: Bloomberg Terminal

Team Outlook

The future of cybersecurity remains promising as the process of securitizing data and information only becomes more important to organizations. The cybersecurity space will continue to grow, riding on the trend toward digitalization as companies continue to move to cloud-based data solutions and hybrid work models necessitating the need for cloud and end-point security solutions. As cyber threats and cybercriminal capabilities continue to evolve, cybersecurity companies will be forced to continue innovation through continuous research and development spending as well as the addition of modern features such as AI-integrations and quantum security measures.

In the competitive landscape, we expect large amounts of M&A and private investing activity to occur throughout 2025. Larger players will continue acquiring specialized companies to enhance service offerings and incorporate advanced security features aiming to become a comprehensive all-in-one security platform. Similarly. private investors will further capitalize on the growing demand for digital security recognizing the industry's potential for growth, consolidation, and strong exit opportunities.

In the long run, we believe that cybersecurity's substantial growth will be able to be sustainably held once at scale. One of the factors enabling future stability is government regulations, with governments throughout the world recognizing the need to protect sensitive information in several industries, it forces businesses and organizations to adopt modern cybersecurity measures. Another is that cybersecurity is a necessary tool for any company to operate as leadership within organizations recognizes that the cost to recover after a data leak and loss in customer trust can lead to significant costs. Lastly, customer retention after the adoption and integration of cybersecurity products is extremely high because once implemented it can be complex, costly, and time-consuming for companies to switch platforms due to the deep-rootedness of cybersecurity platform integration.

Overall the cybersecurity industry remains a resilient and critical industry driven by its indispensable role in protecting sensitive information and data in a world increasingly driven by technology. As innovation and adoption continues, cybersecurity will sustain its growth and evolve into a necessity in modern business operations and security.

Let's Talk

Andrew Shih
Director

Shih.an@northeastern.edu
+1 (973) 369-3510

Raahil Gunaratne
Associate

Gunaratne.ra@northeastern.edu
+1 (908) 307-0724

Sanjit Kosaraju
Analyst

Kosaraju.s@northeastern.edu
+1 (925) 913-9652

Craig Ottaviano
Analyst

Ottaviano.c@northeastern.edu
+1 (203) 964-7703

Rahul Yaganti
Analyst

Yaganti.r@northeastern.edu
+1 (203) 873-1121