Signal From Noise

December 14, 2023

Riding the Cybersecurity Surge: Finding Investment Gems in the Digital Ramparts

"Data is the pollution problem of the information age, and protecting privacy is the environmental challenge." ~ Bruce Schneier

In an era defined by technological quantum leaps, the ubiquity of data, and the interconnectedness of devices, the cybersecurity industry positions itself as the digital bulwark protecting businesses, governments, and individuals from an ever-evolving landscape of threats, some of them existential. As our lives become increasingly intertwined with digital platforms, the demand for robust cybersecurity solutions has skyrocketed, propelling this sector into a realm of practically unrivaled significance.

Within the labyrinth of code libraries, server farms, networks, and firewalls lie not only vital security measures but also lucrative investment opportunities that beckon astute investors. In this Signal From Noise, we explore the core trends shaping the cybersecurity industry, look at some of the key players leading and exploiting these trends, and unveil actionable investment ideas that promise to harness the potential of this booming sector.

The Cybersecurity Landscape: Navigating Complexity Amid Chaos

As technologies advance in their capability and complexity, so do the threats that seek to exploit them for profit or in service of an ideology. Whether preempting sophisticated breaches or mitigating crippling attacks, the cybersecurity industry seeks to be an agile and formidable force commanding a high-stakes battleground. To gain an investor's edge when approaching cybersecurity stocks, one needs to fully grasp the shifting dynamics of the industry's landscape.

- **The rise of nation-state attacks**. Governments and state-sponsored entities are increasingly deploying cyber-warfare tactics, targeting critical infrastructure and sensitive data. Tracking companies that specialize in fending off threats from nation states is a solid medium-term strategy, as governments worldwide prioritize the bolstering of their digital defenses.

- **AI and machine learning**. The cybersecurity industry has harnessed the power of artificial intelligence and machine learning to identify patterns, predict attacks, and muster responses faster than ever before. Investment in AI-driven cybersecurity solutions could yield significant returns, as automation – in the sense of ever-increasing delegation of low-level, high-volume decision-making to AI – becomes a cornerstone of defense mechanisms.
- **Zero-trust architecture**. Traditional perimeter-based security models are giving way to zero-trust architecture, which treats every user and device as potentially compromised. Companies offering zero-trust solutions are likely to experience increased demand, resulting in investment opportunities.

Geography, Infrastructure, Regulation, Opportunities

According to The Business Research Company's *Cybersecurity Global Market Report 2023*, the global cybersecurity market will grow to $223.7 billion in 2023 (from $201.3 billion the year before) at a CAGR of 10.9%. By 2027, it is expected to grow to $338.8 billion, maintaining roughly the same growth rate.

Asia, primarily driven by rapid digital transformation and integration, is due to see significant growth. India's expansive digital infrastructure projects underscore this trend, and so does China's commitment to becoming a global tech superpower – at least in the short term.

Asia Pacific was the largest region in the cybersecurity market, accounting for 38.7% of the total market share in 2022. Looking ahead, South America and the Middle East are forecast to be the fastest-growing cybersecurity markets.

Regulatory frameworks are evolving to address escalating cybersecurity concerns. For investors, understanding these regulations can unearth true opportunities.

GDPR and Data Protection. Recent surges in cyber-attacks, especially ransomware incidents, in Europe and beyond, as well as the rising cost of data breaches, have brought home in the starkest way possible the indispensable nature of robust cybersecurity frameworks. The General Data Protection Regulation (GDPR) imposes hefty fines in cases of compromised data. This has reshaped how businesses handle personal data; it's also pushed companies to make greater investments in cybersecurity.

Critical Infrastructure Protection. Governments worldwide are enacting regulations to safeguard critical infrastructure from cyber threats. It makes sense to keep an eye out for companies specializing in cybersecurity solutions made specifically for sectors such as energy, transportation, and healthcare.

U.S. Government Support. Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act and, through the State and Local Cybersecurity Grant Program, allocated $1 billion to address cybersecurity risks and threats to their information systems at the state and local levels. Another $600 million was set aside in cyber-related support for the power, water, and transportation infrastructures.

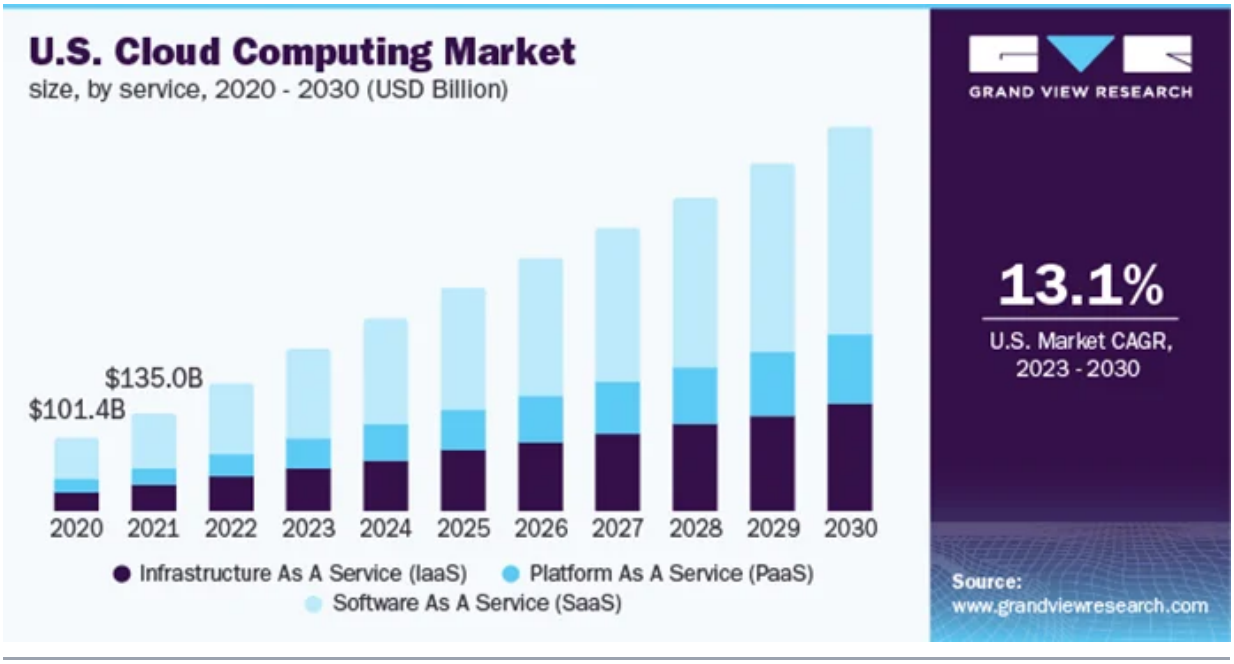
In early March of this year, the White House published a National Cybersecurity Strategy, laying out a plan to use executive orders and memoranda to improve cybersecurity for critical infrastructure control systems, move the U.S. government toward zero-trust cybersecurity principles, and promote U.S. leadership in quantum computing while mitigating risks to vulnerable cryptographic systems.

Investment Contours

The ramping up in cybersecurity infrastructure investment presents potential opportunities for companies in five of the seven primary industry subcategories outlined below. There is considerable overlap, with certain companies taking the lead in multiple subcategories.

Cloud Security

Cloud adoption is on the rise, with enterprise cloud migrations becoming business-critical initiatives. Evolving security capabilities mean that enterprises can retain control over their security posture, data protection programs, and application integrity. The leading players are architecting security solutions for the cloud, combining control and integrity with scalability and agility.



Key participants in this space include:

- Palo Alto Networks ($PANW)
- Zscaler ($ZS)
- Check Point Software Technologies ($CHKP)

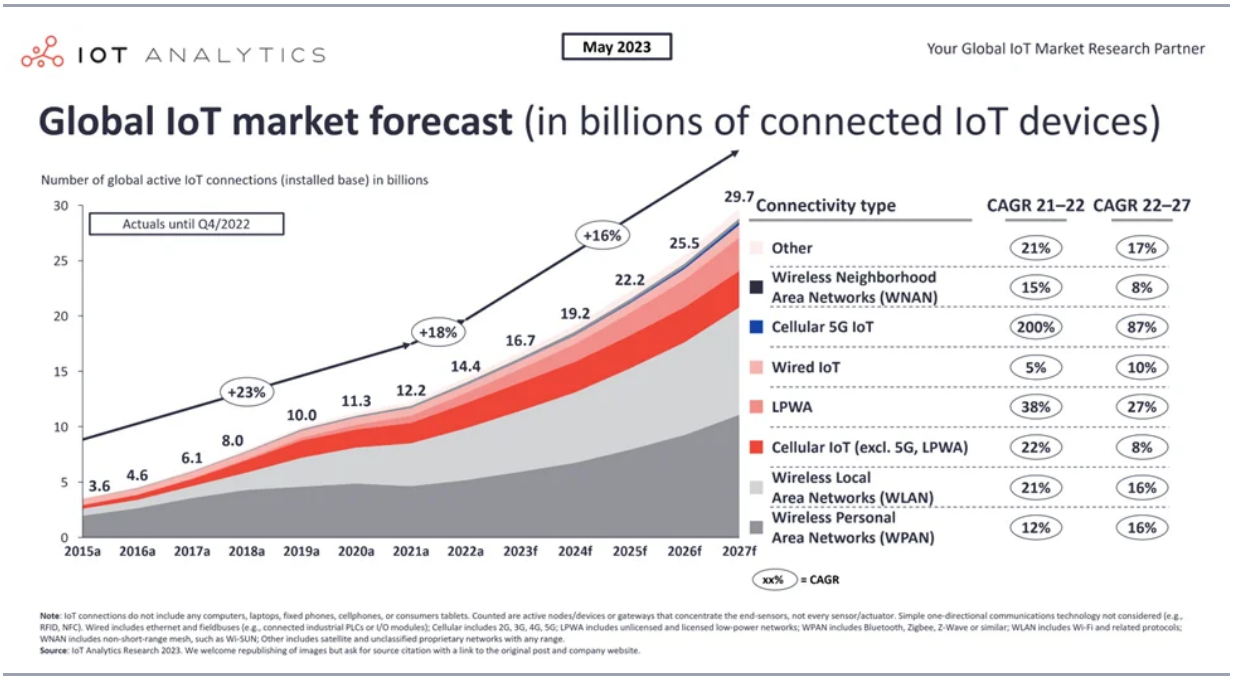
Security of Things

IoT device connectivity can unlock new business value, but as IT networks and operational technology (OT) networks have converge, the attack surface is now larger, and adversaries can threaten health and safety, not just steal data.

Ransomware and 5G are changing the OT threat landscape, with ramifications on the supply chain and physical world, including personal safety. New models and mindsets are needed to mitigate these new threats.

Key participants in this space include:

- CrowdStrike ($CRWD)

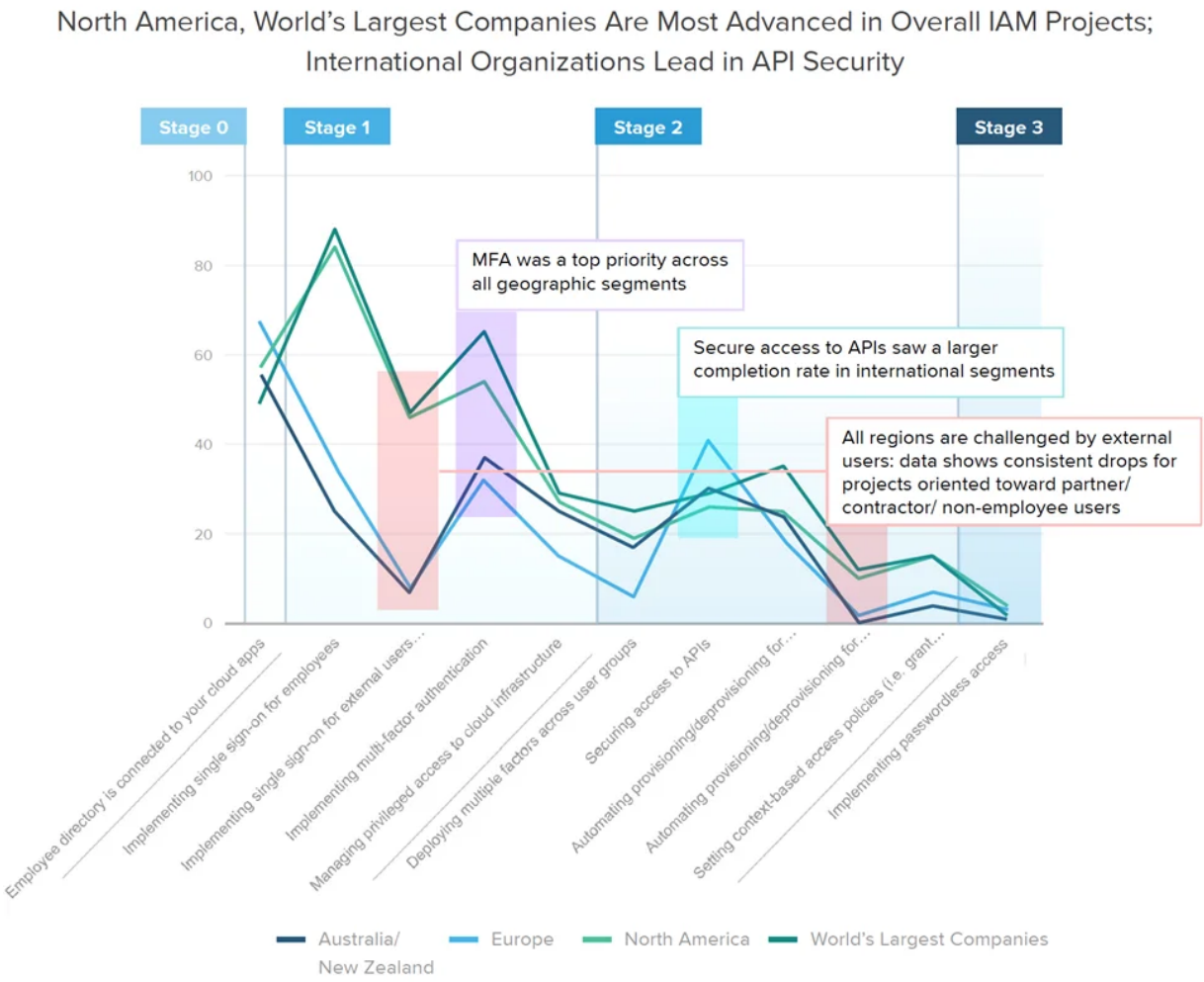


Perimeterless World

The enterprise perimeter is largely a beast of the past, nearly extinct. The shift to remote work post-COVID and the rise of SaaS – and the attendant greater reliance on the cloud, as well as the increased risk of insider threats – accelerate its demise. This makes identity and zero-trust architectures increasingly important in governing access management, to support new ways of doing business that drive growth, productivity, and competitive advantage.

Key participants in this space include:

- Zscaler ($ZS)
- Okta ($OKTA)



Source: Okta

Privacy & Digital Trust

Globalization and expanding digital commerce are on a collision course with emerging privacy regulations and consumer preferences, with resulting data breaches as well as large fines for non-compliance. The design of business processes and systems architecture needs to accommodate new privacy and zero trust-driven strategies.

Know your data (KYD), from knowing what you have, storing only what you need, and leveraging technologies that make it possible to do business without sharing data will become critical.

Resilience & Recovery

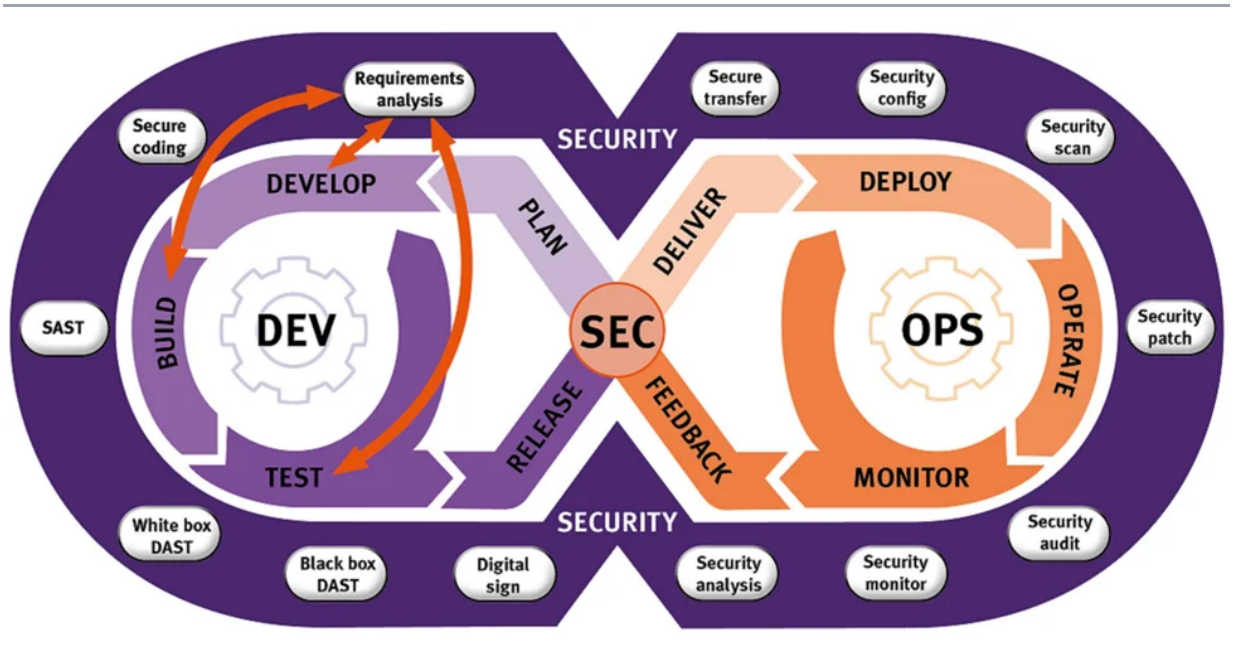
Digital infrastructure has become business-critical, which means that recovery from cyberattacks is now core to risk mitigation and business continuity. Operational resiliency, i.e. rapid recovery and reconstitution of assets and capabilities, must be part of any sound security strategy.

Shift-Left

Software development and management is becoming more agile than ever. Security cannot be an afterthought, but must be baked in, or 'shifted-left' to the developers, who will embed security considerations from the start in a DevSecOps model, with security-by-design and code-to-production being the new business standards. In other words, security professionals should understand coding, and developers need to code with security in mind.

Key participants in this space include:

- Palo Alto Networks ($PANW)



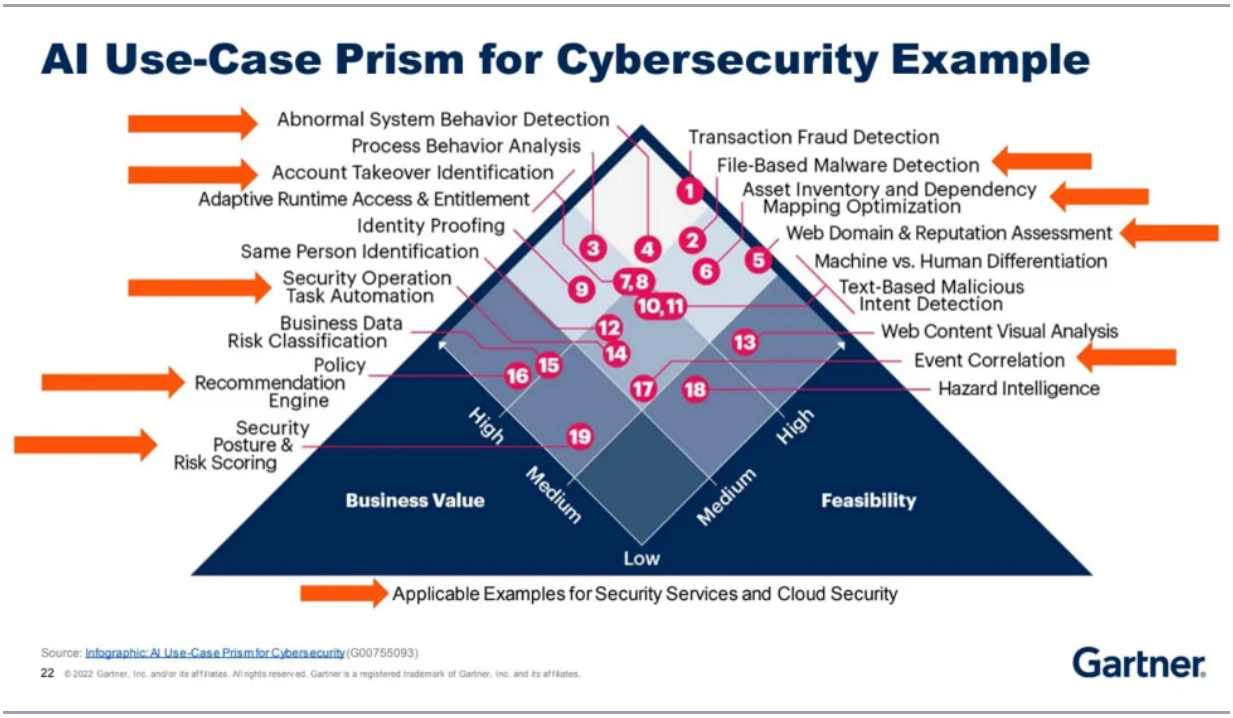
Source: LDRA

Smarter Security

As organizations face unprecedented security complexity, response capacity is stretched to its limits —an expanding enterprise network, unintegrated products, a cyber-talent shortage, and hackers with increasingly sophisticated capabilities. Smarter security solutions are leveraging automation, data, and AI to handle routine tasks, leaving humans with the bandwidth to focus on managing exceptions.

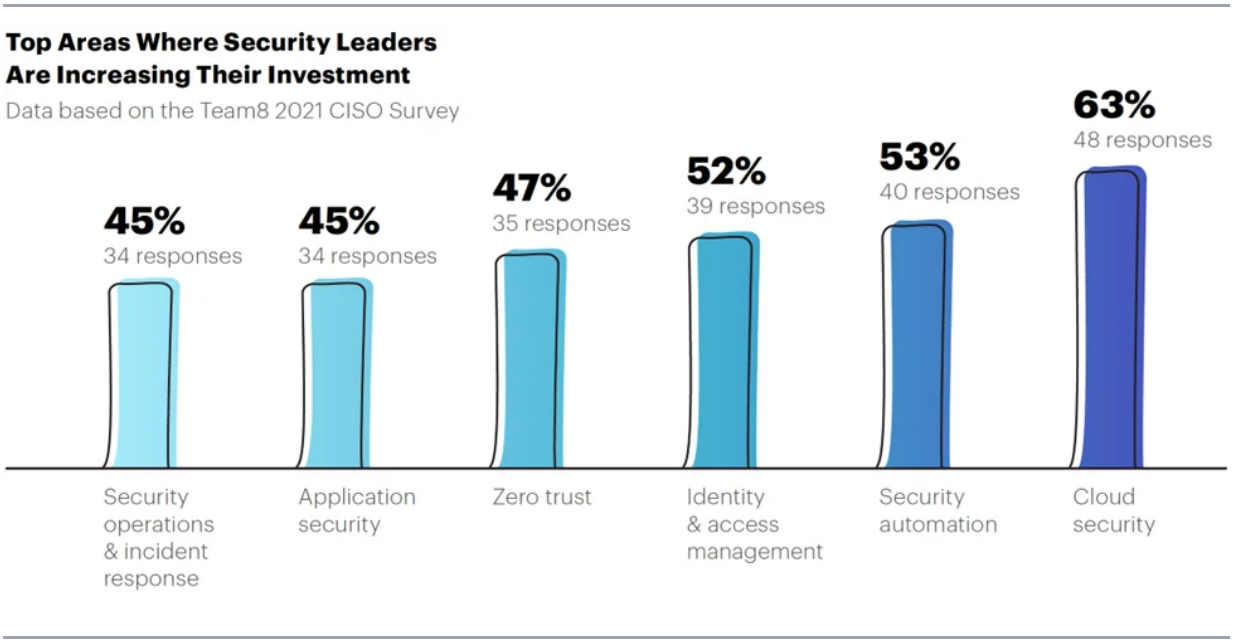
Key participants in this space include:

- Palo Alto ($PANW)
- Splunk ($SPLK)
- Datadog ($DDOG)



Riding the Investment Wave

Historically recession-resistant – and currently the fastest-growing, highest-priority subsector of the software sector – cybersecurity is seen by the c-suite at large companies as non-negotiable in terms of spending.



Source: Team8

Indeed, in our view, security is the fastest-growing top-priority concern for CIOs, with the hiring of a CISO (Chief Information Security Officer) becoming standard practice at large companies across the economy. Cyber also tends to be a non-discretionary budget item, which creates a large market opportunity – and, by extension, an attractive investment opportunity – specifically via these companies, all paragons of growth and profitability, as well as long-term outperformers.

- Cloudflare ($NET) – A leader in delivering cloud cybersecurity and DDoS mitigation.
- CrowdStrike ($CRWD) – Specialists in endpoint security using cloud-native architecture.
- Palo Alto Networks ($PANW) – Known for their next-generation firewalls and cloud-security solutions.
- ZScaler ($ZS) – Champions of Zero Trust Network Access solutions.
- Okta, Inc. ($OKTA) – An identity and access-management leader that provides cloud software that provides user-authentication management, including identity controls for applications.
- Check Point Software ($CHKP) – Innovators in firewall protection and VPN security.
- Splunk ($SPLK) – Analytics-driven security with real-time threat intelligence.

As does any industry, the cybersecurity domain faces obstacles. Rapid technological advancement implies that today's security solutions might become obsolete tomorrow. The industry also grapples with a shortage of skilled cybersecurity professionals.

To mitigate these challenges, firms are investing in AI and machine learning for proactive threat detection, exploring quantum cryptography to address future computing challenges, adopting zero-trust architectures to minimize internal vulnerabilities, and expanding cyber threat intelligence to provide real-time, global threat feeds.

Two high-tech titans enabling these companies' technologies include IBM ($IBM), which leads in quantum computing and its implications for security, as well as Granny Shots stalwart NVIDIA ($NVDA), which is aggressively expanding into AI-driven cybersecurity solutions.

A Secure Future with Lucrative Prospects

The relentless nature of the cybersecurity industry's expected growth trajectory paints a picture of unending opportunities. From defending against nation-state attacks to securing the IoT landscape, the sector is abuzz with innovative solutions and investment potential. Discerning the true value signal amid the noise of possibilities requires careful consideration, research, and a deep understanding of the industry's dynamics.

The industry has reason to be optimistic in the face of certain tailwinds, but it is also subject to uncertainty and growth limitations. On the one hand, cybersecurity is coming into the mainstream, with the CISO finally being viewed as a key decision-maker and profit enabler, not just risk-mitigation and cost-avoidance specialist. Due to the pandemic, organizations are now on high alert for phishing and other forms of attacks and scams that can lead to data breaches.

At the same time, as the industry matures, cybersecurity needs more standardization and compatibility, e.g. more intuitive application interfaces optimized for the behavior of security professionals, more security-by-design and greater collaboration with developers, more automation, consolidation, and less involvement of trust and the human factor. Ultimately, the companies that rise to the moment with workable, cost-effective solutions to these challenges are the ones to watch.

As usual, Signal From Noise should serve as a starting point for further research before making an investment, rather than as a source of stock recommendations. Although the names mentioned above each have the potential to benefit from increased government investment in cybersecurity infrastructure globally, this alone should not be the basis of a decision to invest.

We encourage you to explore our full Signal From Noise library, which includes deep dives on the the world of Big Data and opportunities arising from the global transition to electric vehicles. You'll also find a recent discussion on private-sector intelligence and the aging U.S. power grid.

Disclosures

This research is for the clients of FS Insight only. FSI Subscription entitles the subscriber to 1 user, research cannot be shared or redistributed. For additional information, please contact your sales representative or FS Insight at fsinsight.com.

Conflicts of Interest

This research contains the views, opinions and recommendations of FS Insight. At the time of publication of this report, FS Insight does not know of, or have reason to know of any material conflicts of interest.

General Disclosures

FS Insight is an independent research company and is not a registered investment advisor and is not acting as a broker dealer under any federal or state securities laws.

FS Insight is a member of IRC Securities' Research Prime Services Platform. IRC Securities is a FINRA registered broker-dealer that is focused on supporting the independent research industry. Certain personnel of FS Insight (i.e. Research Analysts) are registered representatives of IRC Securities, a FINRA member firm registered as a broker-dealer with the Securities and Exchange Commission and certain state securities regulators. As registered representatives and independent contractors of IRC Securities, such personnel may receive commissions paid to or shared with IRC Securities for transactions placed by FS Insight clients directly with IRC Securities or with securities firms that may share commissions with IRC Securities in accordance with applicable SEC and FINRA requirements. IRC Securities does not distribute the research of FS Insight, which is available to select institutional clients that have engaged FS Insight.

As registered representatives of IRC Securities our analysts must follow IRC Securities' Written Supervisory Procedures. Notable compliance policies include (1) prohibition of insider trading or the facilitation thereof, (2) maintaining client confidentiality, (3) archival of electronic communications, and (4) appropriate use of electronic communications, amongst other compliance related policies.

FS Insight does not have the same conflicts that traditional sell-side research organizations have because FS Insight (1) does not conduct any investment banking activities, and (2) does not manage any investment funds.

This communication is issued by FS Insight and/or affiliates of FS Insight. This is not a personal recommendation, nor an offer to buy or sell nor a solicitation to buy or sell any securities, investment products or other financial instruments or services. This material is distributed for general informational and educational purposes only and is not intended to constitute legal, tax, accounting or investment advice. The statements in this document shall not be considered as an objective or independent explanation of the matters. Please note that this document (a) has not been prepared in accordance with legal requirements designed to promote the independence of investment research, and (b) is not subject

to any prohibition on dealing ahead of the dissemination or publication of investment research. Intended for recipient only and not for further distribution without the consent of FS Insight.

This research is for the clients of FS Insight only. Additional information is available upon request. Information has been obtained from sources believed to be reliable, but FS Insight does not warrant its completeness or accuracy except with respect to any disclosures relative to FS Insight and the analyst's involvement (if any) with any of the subject companies of the research. All pricing is as of the market close for the securities discussed, unless otherwise stated. Opinions and estimates constitute our judgment as of the date of this material and are subject to change without notice. Past performance is not indicative of future results. This material is not intended as an offer or solicitation for the purchase or sale of any financial instrument. The opinions and recommendations herein do not take into account individual client circumstances, risk tolerance, objectives, or needs and are not intended as recommendations of particular securities, financial instruments or strategies. The recipient of this report must make its own independent decision regarding any securities or financial instruments mentioned herein. Except in circumstances where FS Insight expressly agrees otherwise in writing, FS Insight is not acting as a municipal advisor and the opinions or views contained herein are not intended to be, and do not constitute, advice, including within the meaning of Section 15B of the Securities Exchange Act of 1934. All research reports are disseminated and available to all clients simultaneously through electronic publication to our internal client website, fsinsight.com. Not all research content is redistributed to our clients or made available to third-party aggregators or the media. Please contact your sales representative if you would like to receive any of our research publications.