BIG DATA (CLOUD COMPUTING & CYBERSECURITY)

Perhaps no investment theme has been more important to the business world since the COVID-19 outbreak than Big Data. As workplaces went remote, access to key documents, applications, and computing resources made cloud computing essential. We expect the global economy to shift further into the cloud over time, though connectivity can be both a blessing and a curse, as readily accessible files can become an easy target for malicious actors. Fortifying cybersecurity measures are therefore necessary investments to protect remote treasure troves of sensitive data.

KEY TAKEAWAYS

- COVID-19 related pressure boosted the Big Data theme as it increased cloud utilization faster than previous estimates. Now an estimated 92% of enterprises use multiple cloud services, employing 2.6 public and 2.7 private clouds on average.[1]
- Cybersecurity spending is expected to increase significantly with the global economy going digital. Ninety-six percent of organizations increased their cybersecurity spending in 2020, according to a recent survey. And 91% increased their cybersecurity budgets in 2021.[2]
- Big Data's cloud computing and cybersecurity technologies integrate exceptionally well from a portfolio perspective, as the data-dense cloud necessitates ongoing cybersecurity spending and investment.

WHY CLOUD COMPUTING AND CYBERSECURITY ARE SUCH POWERFUL FORCES

Cloud computing offers proven efficiencies that modernize business practices.

Of all the investment themes that we track, the Cloud Computing theme likely accelerated the most due to COVID-19 because it became essential to business continuity. In a survey by computer software company Flexera, 29% of respondents said that they increased their cloud usage significantly more than expected during the pandemic, while 61% made slight increases due to pandemic-related operational changes.[3] Today, an estimated 92% of enterprises use multiple cloud services, employing 2.6 public and 2.7 private clouds on average.[4]

With growing demand attributed to lower operating costs, better collaboration, increased flexibility, and improved turnaround times for server expansion, the largest enterprises by revenue accounted for 51% of the cloud market in 2020.[5] These firms were not new to the cloud, having used it to build applications or host corporate infrastructure. The next push looks to modernize core business applications and processes. Technology conglomerate Cisco expects 94% of all corporate workflows to run through some form of cloud infrastructure by 2021, as servers dedicated to individual tasks quickly become relics.[6]

The next stage of the cloud's evolution looks to be omni-cloud solutions that stitch together multiple platforms and services to create more integrated data sharing and access. Managed multi-cloud environments should help assuage security, cost, and governance issues, the top concerns of enterprise cloud decision-makers.[7]

Currently, supply chain constraints, including the ongoing semiconductor shortage, are a challenge. But we believe the shortage can enhance the Cloud Computing theme. Under more normal conditions, corporations have a choice. They can build out their own personalized data centers, spending the time, resources, and expertise to customize servers. Or they can contract a cloud provider that offers a more general but rapid turnkey solution. Currently, high costs and long lead times due to supply constraints disincentivize personalized server builds, forcing organizations into the cloud to avoid the risk of delays.[8]

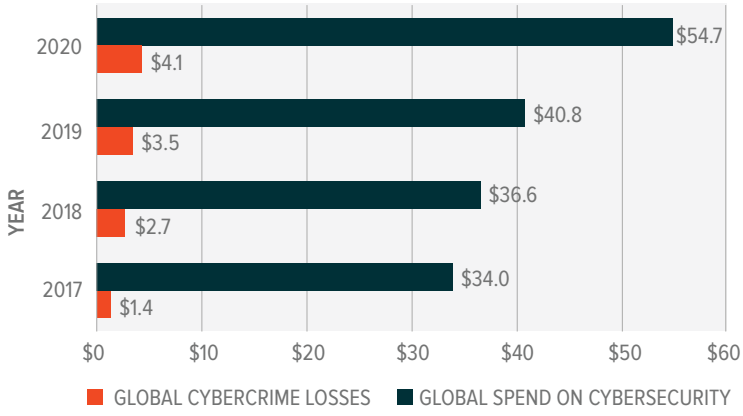
As the value of data increases, it requires more protections.

Cloud computing data centers aggregate and concentrate valuable data and processing power, increasing the speed and effectiveness of computing tasks. But that digitization makes protecting this valuable and sensitive data essential. The World Economic Forum marked cyberattacks as the 7th global risk by likelihood and 8th by impact in 2020.[9] It's estimated that global cybercrime costs will grow by 15% per year to $10.5 trillion annually by 2025.[10]

In 2020, ransomware attacks increased by 62% globally and 158% in North America compared to 2019.[11] These malicious attacks have real consequences for business, infrastructure, and end users beyond lost data and operational disruptions. According to FBI data, U.S. economic losses from more than 791,790 reported cybercrime incidents in 2020 exceeded $4.1 billion.[12] The effects of a successful breach, financial and otherwise, can be felt for years after the actual threat ends. As much as 22% of negative effects occur in the second year after the event, and another 11% surface in the third year.[13]

CYBER ATTACKS CONTINUE TO CAUSE DAMAGE EVEN AS SPENDING INCREASES DRAMATICALLY

Source: IC3, March 2021, Canalys, January 2021.

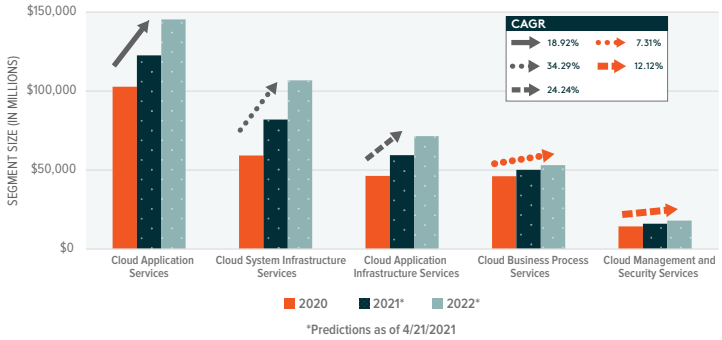


According to solutions provider Insight CDCT (Cloud + Data Center Transformation), 96% of surveyed organizations increased their cybersecurity spending in 2020, and 91% expanded their cybersecurity budgets in 2021. However, current solutions largely focus on closing immediate security gaps and addressing the easiest-to-deploy options first, not the most concerning threats, including state-sponsored corporate espionage, attacks on critical infrastructure, and disinformation campaigns.[14] For example, the Solar Winds hack discovered in December 2020 is believed to be the work of the Russian Foreign Intelligence Service. About 100 companies and a dozen government agencies were compromised, including the U.S. Treasury, Justice, and Energy departments, and the Pentagon.[15]

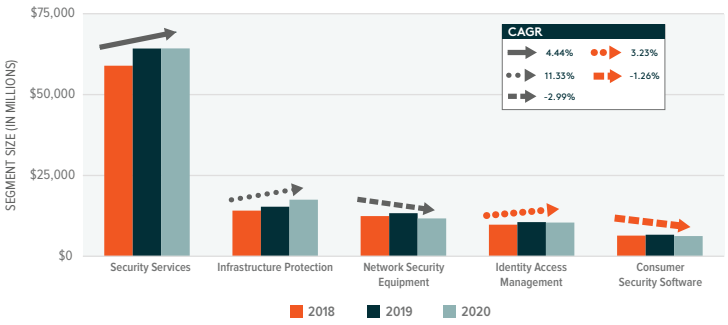
The increased sophistication of state-sponsored cyber threats requires equally sophisticated state responses. The Biden administration recently issued a new mandate for federal agencies to patch cybersecurity vulnerabilities in government software. This mandate covers about 200 known security flaws, making it one of the most widespread initiatives of its kind.[16] Additionally, the House passed the Small Business Administration (SBA) Cyber Awareness Act, requiring small businesses to notify Congress of cybersecurity breaches. A second component includes the Small Business Development Center Cyber Training Act for cybersecurity counseling certification programs.

VISUALIZING THE MARKET OPPORTUNITY

GLOBAL CLOUD COMPUTING SPENDING BY LARGEST SEGMENT
Source: Gartner data as of 4/21/2021.



GLOBAL CYBERSECURITY SPENDING BY LARGEST SEGMENT
Source: Embroker data as of 11/2/2021.



RISKS TO THE BIG DATA THEME

Supply chain disruptions could affect development of critical cloud infrastructure.

A concern for Big Data and the broader technology space is the supply chain constraints limiting the availability of certain types of semiconductors. This shortage has nuanced effects on the Cloud Competing theme as increased demand from end users is offset by capacity growth restrictions. Data center development is necessary for the continued expansion of service offerings and staying competitive in an industry with regular hardware advancements and data demand increases.

Shortages aren't affecting every type of semiconductor. High-margin microchips, such as the server-level central processing units (CPUs) and graphics processing units (GPUs) that make up the backbone of data centers, are generally available. But other necessary components like power supplies and network switches face lead times in the 40–60 week range, more than double the pre-pandemic norm.[17,18] Semiconductor foundry capacity is growing at 1–3% per year, but that growth is outpaced by the demand for computing power, so constraints are expected to persist. Industry leaders expect tightness through Q2 2022.[19,20]

Cybersecurity is an inherent risk in the digital age.

Data is gold today, which means data centers must become virtual fortresses. Concentrating such a valuable resource only increases the interest of malicious actors, and when they see an opening, they take it. For example, attacks on cloud infrastructure providers increased 630% between January and April 2020 compared to the previous four-month period as cyber criminals looked to exploit COVID-related confusion.[21]

Unauthorized access can occur even without malicious activity due to incorrect settings or user and employee errors. In 2019, more than 540 million user records from a large social media company were exposed by a leading cloud provider due to improper data protections.[22] Absolute protection of data is likely impossible because there is a direct trade-off between data security and accessibility, but many risks can be mitigated by adequate cybersecurity spending and security awareness training.

From a risk perspective, the Cybersecurity theme looks well-insulated. Cybersecurity technologies work to proactively shield against possible attacks while mitigating and repairing the damage from attacks that already occurred. As a result, there is little risk at the broad theme level because the factors spurring adoption are unlikely to ever wane. Risk remains acute at the individual company level, where malicious actors constantly stress-test specific cybersecurity approaches and tools.

Should a breach occur under a cybersecurity provider's nose, markets are likely to devalue that company compared to its peers. However, in such instances, interest actually increases for the space overall. Cybersecurity stocks and ETFs have a history of positive price performance following the announcement of large-scale hacks, including the Solar Winds incident. In a situation where a data center or application developer falls victim to a large breach, negative share performance could be offset by broader cybersecurity gains.

THEMATIC INTERSECTION: INTERNET OF THINGS AND ARTIFICIAL INTELLIGENCE

Internet of Things (IoT)

The proliferation and advancement of connected devices driven by IoT technology looks to enhance the opportunities for Big Data themes. The integration of microchips and networking into more products creates more opportunities for data collection, as well as unauthorized access. Distributed sensors require a central data processing location to receive and aggregate collected information. And as the number of connected devices expands alongside increasingly sophisticated data analysis, so does the need for processing power and cloud computing resources.

But sensors are next to useless if they aren't secure, so IoT also positively impacts the Cybersecurity theme. For a malicious actor, the IoT is a cornucopia of opportunities to attack. Ninety-eight percent of all IoT device traffic is unencrypted, which translates to 57% of IoT devices being highly vulnerable to cyberattacks that can expose personal and confidential data.[23] Successful IoT deployments require multi-layered, end-to-end security that ranges from upfront, baked-in security requirements to the ongoing management and protection of sensitive machine-generated data.[24]

Artificial Intelligence (AI)

The cloud and AI and are also a fitting match. The cloud can democratize access to AI, providing turnkey solutions without significant upfront investment or specialized experience. AI can enhance cloud infrastructure through computing resource management, streamlining workloads, and automating repetitive tasks without human interaction. Additionally, growth in AI capability and complexity requires expanded computing resources. In 2018, AI research lab OpenAI reported that the amount of computational power used to train the largest AI models doubled every 3.4 months, an appetite that cloud providers can quickly satisfy.[25]

AI technology is a boon for the Cybersecurity theme, given its use of pattern recognition and predictive intelligence to detect unusual network activity or penetration attempts. As cyberattacks grow in complexity, regularity, and intensity, AI can bolster human-based cyber defenses. Spending on AI cybersecurity tools is expected to grow faster in the coming five years than hardware or services, indicating wholesale adoption of the technology.[26]

BIG DATA IN A PORTFOLIO CONTEXT

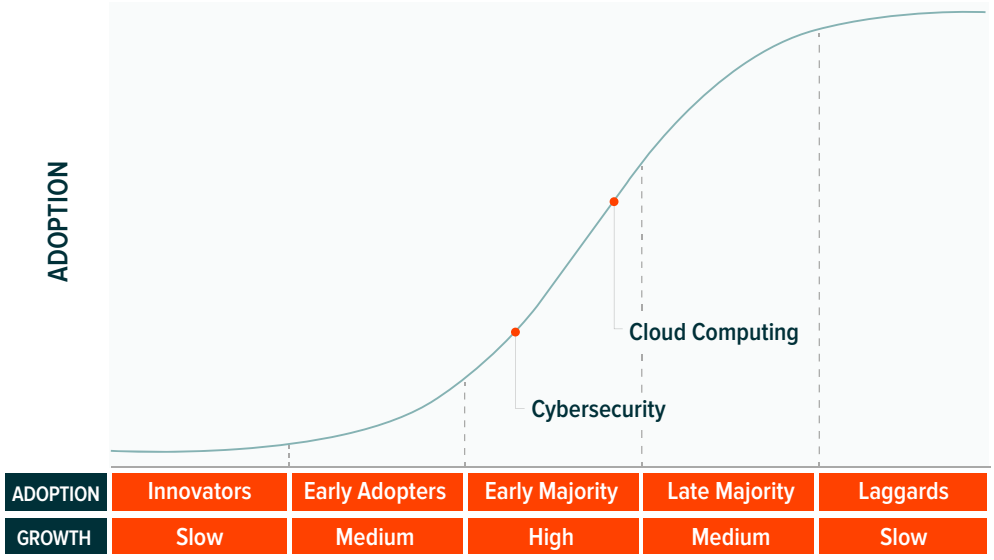
Big Data is foundational to our digital future, and is comprised of core themes that we believe have a place in most thematic portfolios. Both Cloud Computing and Cybersecurity fall squarely into the Early majority phase, indicating that adoption levels are high and rising, and that the market has begun to accept these themes at scale.

The companies that implementing Big Data technologies are global and stand to benefit as thematic adoption rises across the world. The pie charts below breaks down the geographic exposure of the largest Big Data ETF products. We believe there is ample innovation occurring outside of the states, and that limiting exposure to the U.S. will exclude key players to the detriment of investors over the long term.

In our view, thematic equity should be targeted, using screens to ensure the underlying companies provide the desired thematic exposure. This pure play exposure minimizes overlap between themes while also differentiating the exposure provided by the theme relative to broad beta products. An overlap analysis between Big Data thematic ETFs and XLK, the Technology Select Sector SPDR Fund, shows that average overlap by weight is 6.4% and 2.5% for cloud computing and cybersecurity funds, respectively.[27] As shown above, cloud computing scores higher on adoption than cybersecurity, and this is reflected in the theme's larger level of inclusion in broad tech sector ETFs. The names that overlap tend to be large, well known and active in many business segments, such as Microsoft and Cisco, while those that don't overlap are smaller and relate specifically to the theme. This highlights a key advantage of thematic investing - gaining exposure to key players early in their business lifecycles before they are included at any significant weight in broader indexes.

THEMATIC ADOPTION

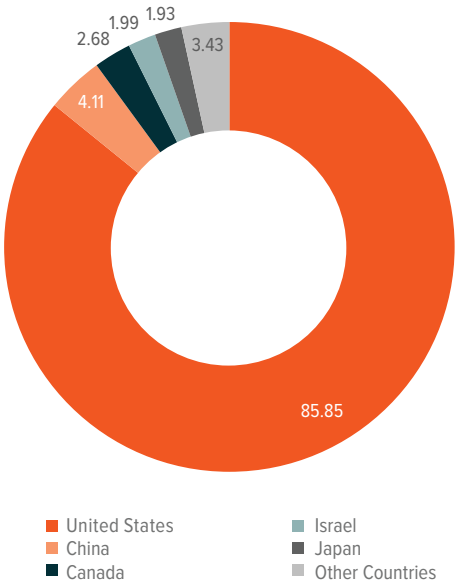
Source: EM Rogers, "Diffusion of Innovations", 1962, and Global X Research, 2021



We believe both Cloud Computing and Cybersecurity will grow in importance over the next decade. Migrating to cloud-based infrastructure and software affords enterprises greater flexibility, predictability, and scale. While the market nears mass adoption, opportunities remain for firms to expand Software-as-a-Service and Infrastructure-as-a-Service offerings. The cloud's effectiveness has been proven; the next leg will maximize its potential. Helping the cloud reach its potential will be the cybersecurity industry, which seems well-positioned to capitalize as people and economies move further online. Cyber threats continue to increase in occurrence and severity, demonstrating the permanent need for cybersecurity spending. Both these Big Data themes benefit from subscription revenue models, helping establish more stable and predictable income streams.

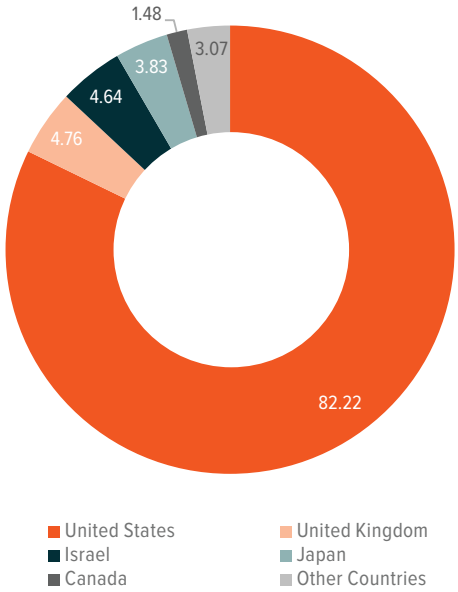
CLOUD COMPUTING: AVERAGE GEOGRAPHIC EXPOSURE BY THEME

Source: Morningstar data as of 12/31/21.



CYBERSECURITY: AVERAGE GEOGRAPHIC EXPOSURE BY THEME

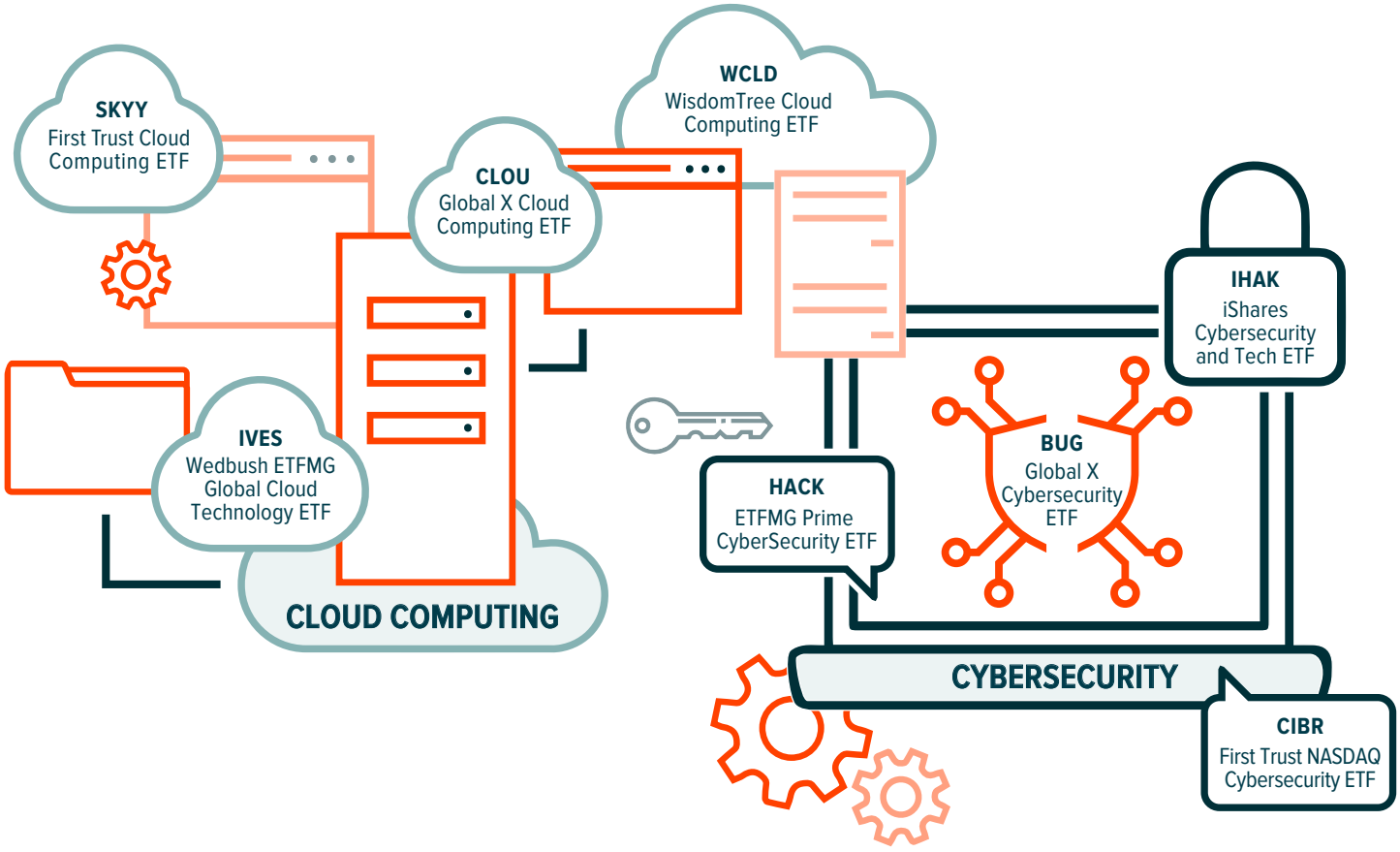
Source: Morningstar data as of 12/31/21.



Note: Pie charts include the largest four cloud computing and the largest four cybersecurity ETFs according to our thematic classification. All Thematic ETFs weighted the same.

HOW TO ACCESS BIG DATA

The graphic below identifies some U.S. listed ETFs that provide direct exposure to the Big Data theme through Cloud Computing and Cybersecurity technology.



BIG DATA FOOTNOTES

[1] Flexara, 2021 State of the Cloud Report, 3/15/21
[2] Insight CDCT, Cybersecurity at a Crossroads: The Insight 2021 Report, 2/24/21
[3] Flexera, 2021 State of the Cloud Report, 3/15/21
[4] Flexara, 2021 State of the Cloud Report, 3/15/21
[5] Grand View Research, Cloud Computing Market Size, Share & Trends Analysis Report By Service (SaaS, IaaS), By Enterprise Size (Large Enterprises, SMEs), By End Use (BFSI, Manufacturing), By Deployment, And Segment Forecasts, 2021 – 2028, July 2021
[6] Cisco, Global Cloud Index (2016-2021), 2/5/18
[7] Flexara, 2021 State of the Cloud Report, 3/15/21
[8] Logicalis, How The Global Chip Shortage Is Driving Data Center Projects To The Cloud, 6/23/21
[9] World Economic Forum, The Global Risks Report 2020, 1/15/20
[10] GlobalNewswire, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, 11/18/20
[11] Sonicwall, 2021 Sonicwall Cyber Threat Report, 8/29/2021
[12] FBI, Internet Crime Report: 2020, 3/17/21
[13] Embroker, 2021 Must-Know Cyber Attack Statistics and Trends, 11/2/21
[14] Insight CDCT, Cybersecurity at a Crossroads: The Insight 2021 Report, 2/24/21
[15] NPR, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, 4/16/21
[16] WSJ, Biden Administration Orders Federal Agencies to Fix Hundreds of Cyber Flaws, 11/3/2021
[17] The Register, 'This is the worst I've seen it' says Arista boss as entire network hardware sector battles component shortages, doubled lead times for semiconductors, 8/3/21
[18] DataCenter Knowledge, 'It's Little Things' – How the Chip Shortage Is Affecting the Data Center Industry, 5/17/21
[19] Logicalis, How the global chip shortage is driving data centre projects to the cloud, 6/15/21
[20] DataCenter Knowledge, 'It's Little Things' – How the Chip Shortage Is Affecting the Data Center Industry, 5/17/21
[21] McAfee, Cloud Adoption and Risk Report: Work from Home Edition, 5/27/21
[22] Varonis, 98 Must-Know Data Breach Statistics for 2021, 2021
[23] Palo Alto Networks, 2020 Unit 42 IoT Threat Report, 3/10/20
[24] IoT Cybersecurity Alliance, Demystifying IoT Cybersecurity, 2017
[25] MIT Technology Review, The computing power needed to train AI is now rising seven times faster than ever before, 11/19/19
[26] Markets and Markets, Artificial Intelligence in Cybersecurity Market by Offering (Hardware, Software, and Service), Deployment Type, Security Type, Technology (ML, NLP, and Context-Aware), Application (IAM, DLP, and UTM), End User, and Geography- Global Forecast to 2026, May 2019
[27] ETF Action data as of 2/9/22

605 THIRD AVENUE
43RD FLOOR
NEW YORK, NY 10158

1 (888) 493-8631
GLOBALXETFS.COM
@GLOBALXETFS