

# WisdomTree – Cybersecurity: The Megatrend that EVERY Business must Consider

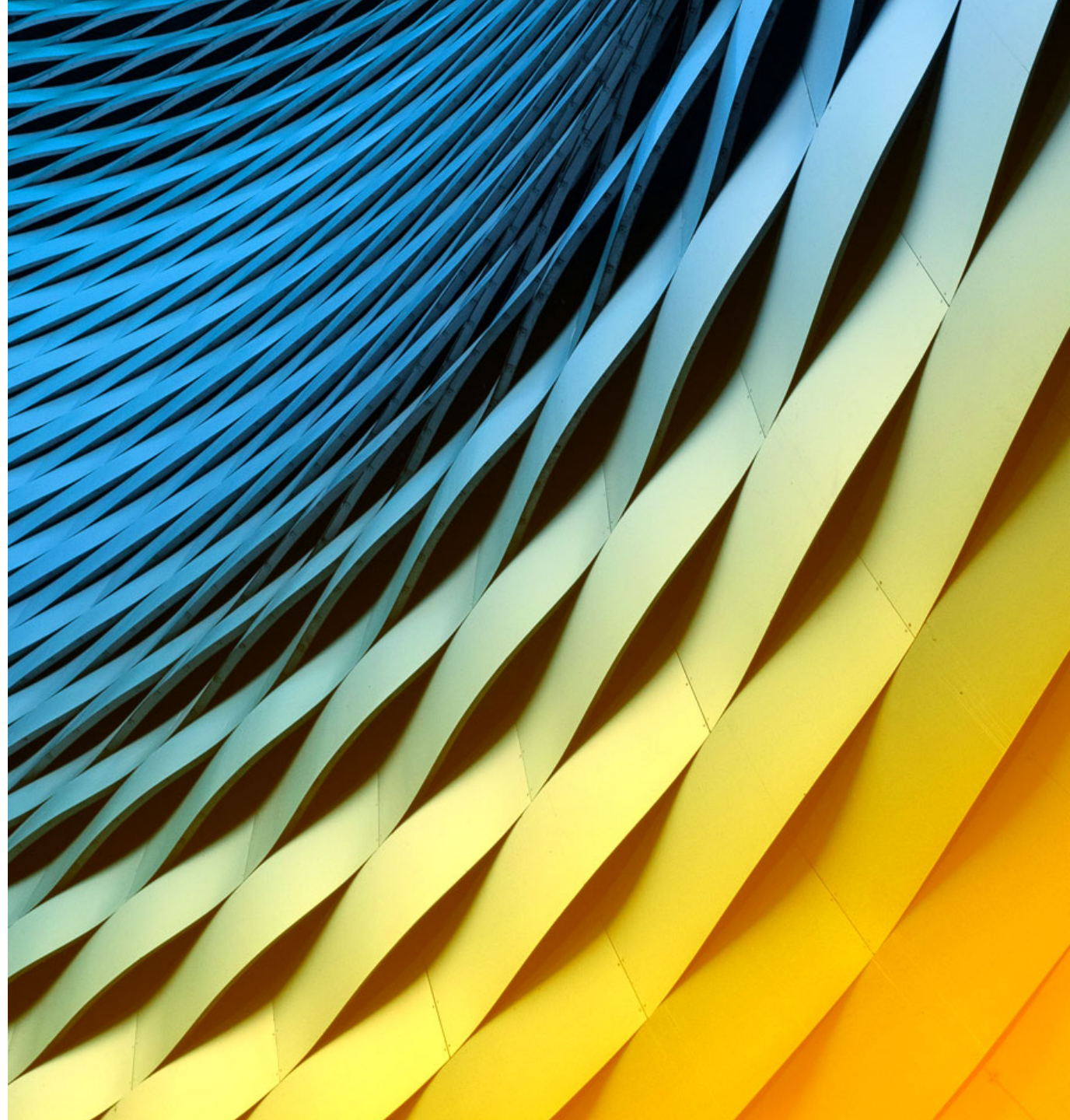
---

**Christopher Gannatti, CFA,**  
Head of Research, Europe,  
WisdomTree

**May 6, 2021**



Exchange and Industry Sponsored Webinars are presented by unaffiliated third parties. Interactive Brokers LLC is not responsible for the content of these presentations. You should review the contents of each presentation and make your own judgment as to whether the content is appropriate for you. Interactive Brokers LLC does not provide recommendations or advice. This presentation is not an advertisement or solicitation for new customers. It is intended only as an educational presentation.



# Disclosures

Options involve risk and are not suitable for all investors. For information on the uses and risks of options, you can obtain a copy of the Options Clearing Corporation risk disclosure document titled [Characteristics and Risks of Standardized Options](#) by calling (312) 542-6901.

Futures are not suitable for all investors. The amount you may lose may be greater than your initial investment. Before trading futures, please read the [CFTC Risk Disclosure](#). For a copy visit [interactivebrokers.com](#).

Security futures involve a high degree of risk and are not suitable for all investors. The amount you may lose may be greater than your initial investment. Before trading security futures, please read the [Security Futures Risk Disclosure Statement](#). For a copy visit [Interactivebrokers.com](#).

There is a substantial risk of loss in foreign exchange trading. The settlement date of foreign exchange trades can vary due to time zone differences and bank holidays. When trading across foreign exchange markets, this may necessitate borrowing funds to settle foreign exchange trades. The interest rate on borrowed funds must be considered when computing the cost of trades across multiple markets.

The Order types available through Interactive Brokers LLC's Trader Workstation are designed to help you limit your loss and/or lock in a profit. Market conditions and other factors may affect execution. In general, orders guarantee a fill or guarantee a price, but not both. In extreme market conditions, an order may either be executed at a different price than anticipated or may not be filled in the marketplace.

There is a substantial risk of loss in trading futures and options. Past performance is not indicative of future results.

Any stock, options or futures symbols displayed are for illustrative purposes only and are not intended to portray recommendations.

IRS Circular 230 Notice: These statements are provided for information purposes only, are not intended to constitute tax advice which may be relied upon to avoid penalties under any federal, state, local or other tax statutes or regulations, and do not resolve any tax issues in your favor.

Interactive Brokers LLC is a member of [NYSE FINRA SIPC](#)



# Cybersecurity: The Megatrend that EVERY Business must Consider

May 2021

# 2021: Current Landscape

## The Top 20 Passwords of 2020

- + 123456
- + 123456789
- + picture1
- + password
- + 12345678
- + 111111
- + 123123
- + 12345
- + 1234567890
- + senha
- + 1234567
- + qwerty
- + abc123
- + Million2
- + 000000
- + 1234
- + lloveyou
- + aaron431
- + password1
- + qqww1122

Source: Shebu, Sherin. "2020's Most Common Passwords are Laughably Insecure." [UK PCMag.com](https://www.pcmag.com)

# Most Vulnerable Part of Most Systems: PEOPLE



Meet **Jenny Radcliffe**, the People Hacker. She's a social engineer and physical penetration tester. Which means she gets paid to break into buildings and test their security. In this episode she tells us a few stories of some penetration testing jobs she's done.

Source: <https://darknetdiaries.com/episode/90/>

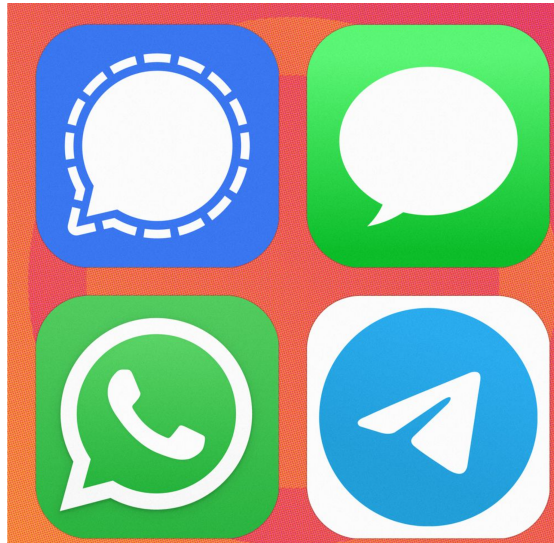
## Making Encryption Tangible: Widely Used Chat Applications

### + Signal

- Open-source encryption
- Doesn't have the userbase of WhatsApp or iMessage

### + WhatsApp

- Use Signal's peer-reviewed encryption
- More than 2 billion users
- Owned by Facebook



### + iMessage

- Works well on more than 1 billion iPhones
- Only works on Apple devices

### + Telegram

- Up to 200,000 members in a group
- Must turn on encryption for each chat
- Not as transparent using 'open-source' encryption

Source: Nguyen, Nicole. "WhatsApp, Signal, Telegram & iMessage: Choosing a Private Encrypted Chat App." [Wall Street Journal](#). 15 January 2021.

# The Threat of Quantum Computing to Traditional Encryption

- +  $593 \times 829 = 491,597$ .
  - It is simple to multiply 2 prime numbers to get an answer.
  - Going in reverse is much more difficult, especially as the numbers grow in size.
- + Nearly impossible for a classical computer to factor a number that is 2048 bits, the basis for commonly used RSA encryption protocols
- + 2015: One billion qubits needed to reliably break 2048 bit encryption
- + 2019: Newer researched showed that 20 million qubits and 8-hours were all that was needed to do this job
- + Companies looking to secure data in the coming decades are looking at this issue

Source: Emerging Technology from the arXiv. "How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours." [MIT Technology Review](#). 30 May 2019.



# Basic Infrastructure, like Water Resources, is Vulnerable to Hackers



- + Hacker briefly increased the level of lye in the water—was immediately caught and reversed
- + City was Oldsmar, Florida, which has 15,000 residents and is close to Tampa Bay.
- + The remote access tool 'TeamViewer' was used for access. The utility had switched to a different tool, but did not disable this older access tool.

Source: Camp-Flores, Arian. "Hacker Changed Chemical Level in Florida City's Water System." [Wall Street Journal](#). 8 February 2021.

## Facebook Hack in 2019 Led to Data from Approximately 533 Million Accounts made Public

- + Cybersecurity experts have created sites for users to check if their accounts were impacted
- + '2FA' or 'Two-Factor-Authentication' was emphasized as important
- + Stolen data could potentially be used for:
  - Robocalls
  - Spam emails
  - Malicious texts
  - Swapping phone numbers onto a different device 'SIM swapping'
- + Remember: Old Data is not Bad Data
  - Guild of Grumpy Old Hackers used data from a LinkedIn hack in 2010 to guess former President Trump's Twitter credentials in 2016

Source: Ziobro, Paul. "Was My Facebook Data Leaked? What You Need to Know." [Wall Street Journal](#). 6 April 2021.

## Cyberattacks are a Venue for Nation States to Skirmish outside Conventional Warfare: The China vs. India Case

- + There was tension on the India/China border in June 2020—there were casualties
- + Did Chinese Cyberattacks cause an October 2020 blackout in Mumbai?
  - There was evidence of more than a dozen Trojan horse attacks
- + In June 2020, Maharashtra's Cyber Department Collated information on possible Chinese cyber intrusion
  - Large scale phishing attacks—at least 40,300 over 5 days
  - Infrastructure targets
  - IT targets
  - Banking Targets
  - Origin could be traced to Chengdu, China in many cases

Source: Bellman, Eric & Rajesh Roy. "India Suspects China may be Behind Major Mumbai Blackout." [Wall Street Journal](#). 1 March 2021.

# Ransomware has become a Larger Problem

- + In 2020, waves of attacks hit:
  - Healthcare networks
  - Hospitals
  - Schools
  - Businesses
- + Antivirus firm Emsisoft found the 'Average Requested Fee' was:
  - Roughly \$5,000 in 2018
  - Roughly \$200,000 in 2020

Source: Hay Newman, Lily. "Ransomware is Headed Down a Dire Path." [WIRED](#). 29 December 2020.

# Quantifying the Threat of Ransomware FireEye's Perspective...

## The Growing Ransomware Threat

### PROLIFERATING DEMAND

Mandiant ransomware response engagements increased **10x** in 2020 from 2018

### RAPID DEPLOYMENT

Median of only 3.5 days from intrusion to deployment

### AVERAGE COST

Wide range from **\$250,000 to \$50 million USD**

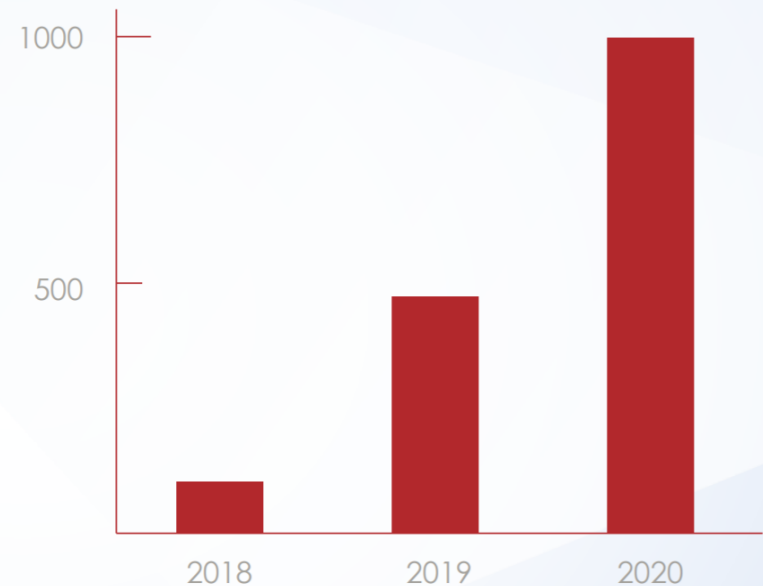
### RISING PAYMENTS

Average payment increased upwards of **180%** from March 2019 to March 2020

### BUSINESS IMPACT

**1 in 10** businesses close due to a ransomware attack

Ransomware Incident Response Investigations by Mandiant



Source: FireEye 2021 Corporate Presentation.

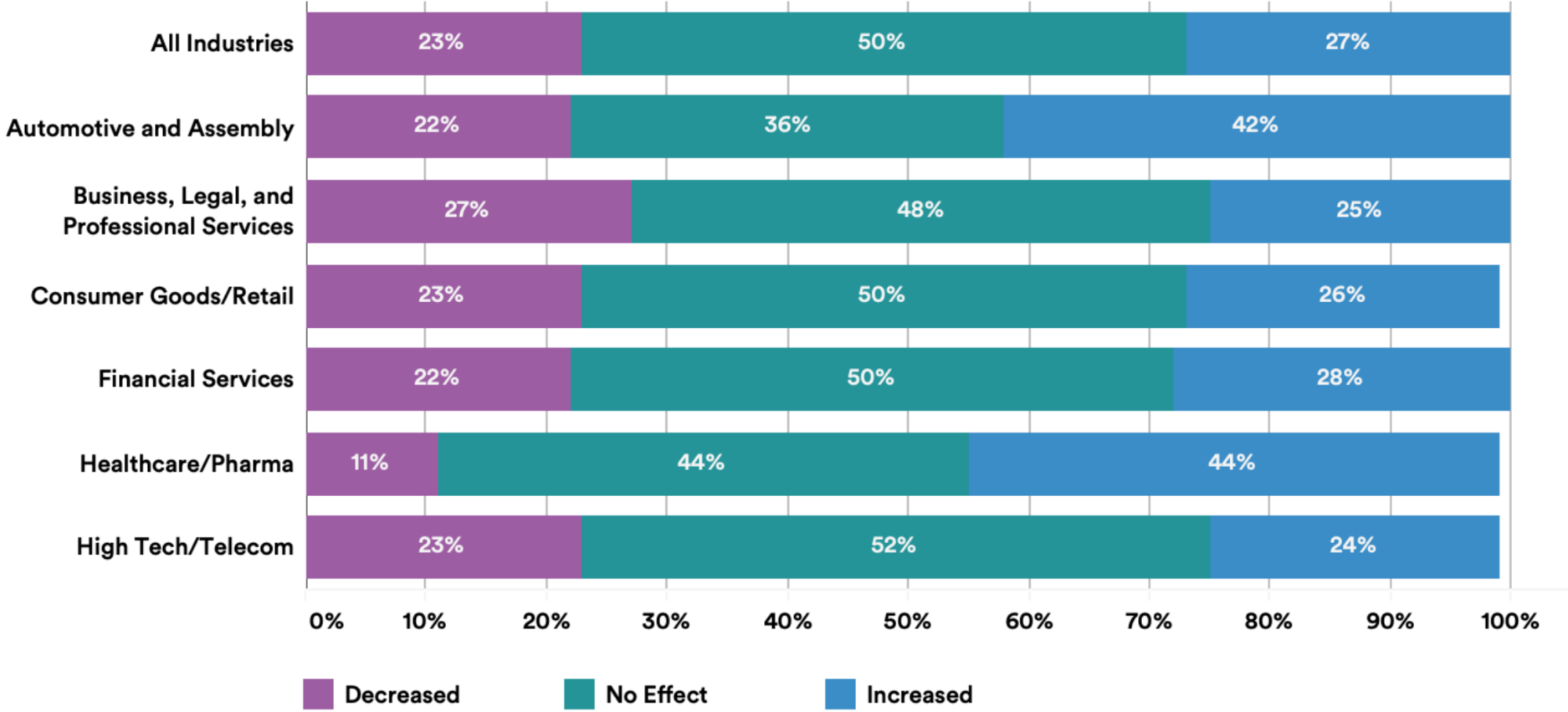
# Artificial Intelligence & Cloud Computing

*Close Relationship to  
Cybersecurity*

# The Pandemic has Not Dampened Investment Enthusiasm in Most Cases

## CHANGES in AI INVESTMENTS AMID the COVID-19 PANDEMIC

Source: McKinsey & Company, 2020 | Chart: 2021 AI Index Report

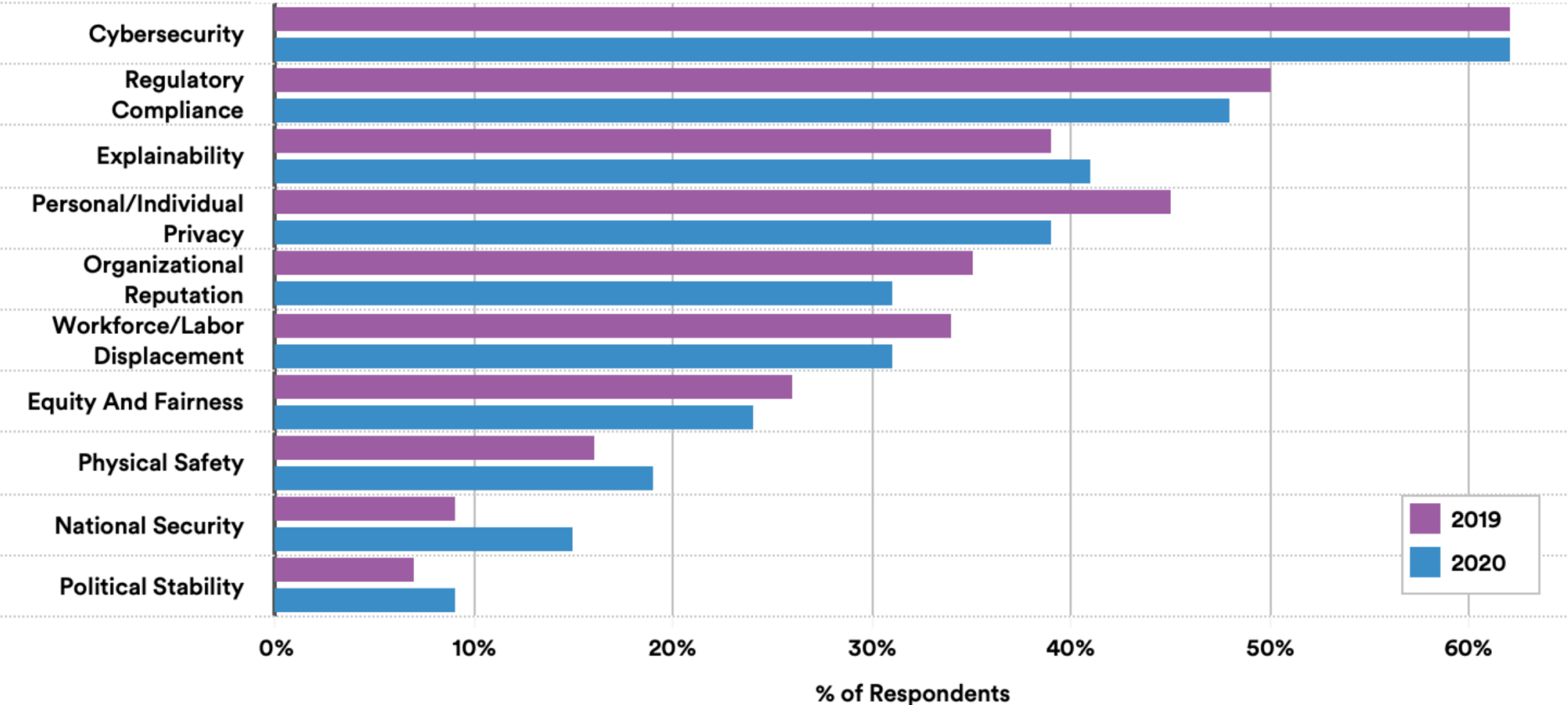


Source: Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Nieves, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault, "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March 2021.

# The Risks that Companies see in ADOPTING AI

## RISKS from ADOPTING AI THAT ORGANIZATIONS CONSIDER RELEVANT, 2020

Source: McKinsey & Company, 2020 | Chart: 2021 AI Index Report



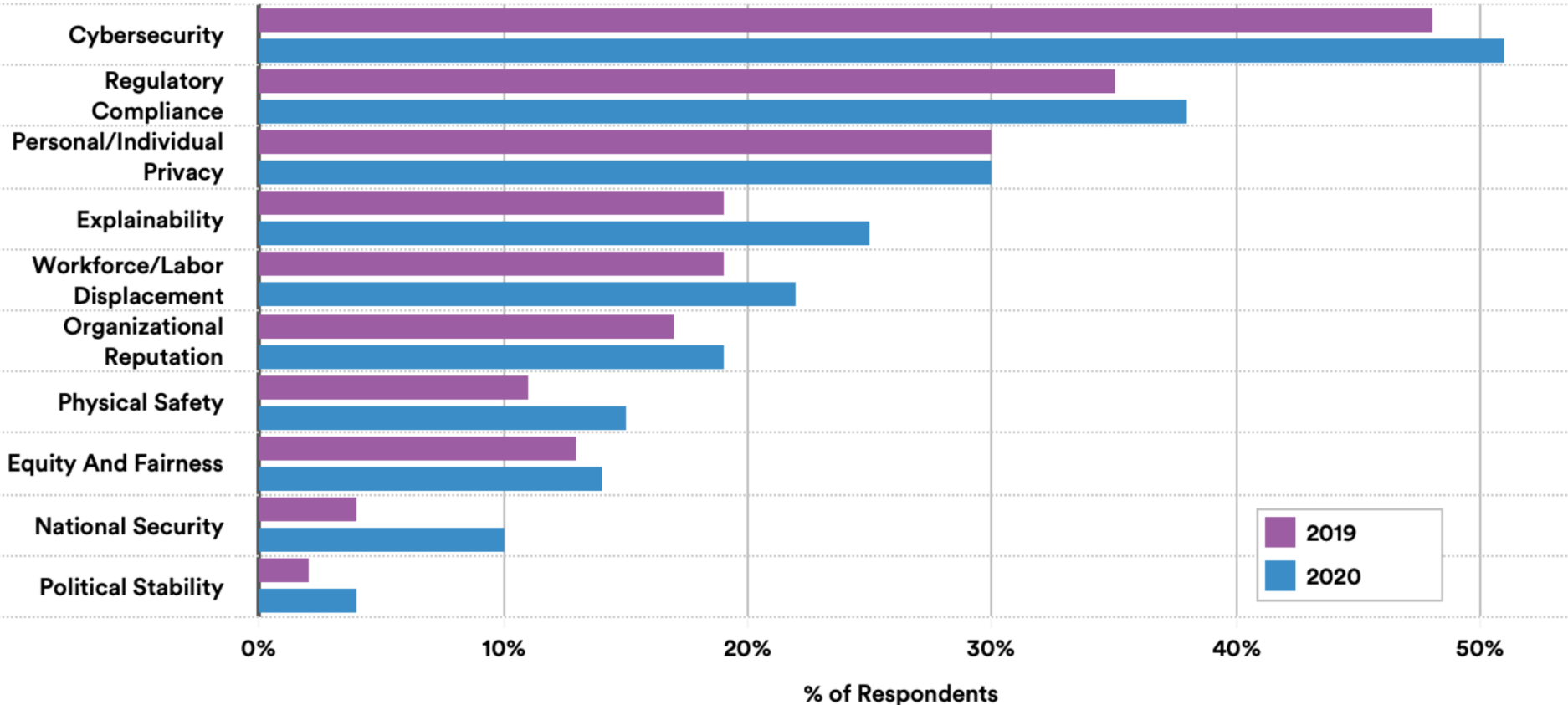
Source: Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault, "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March 2021.



# The Risks that Companies see in ADOPTING AI that they are MITIGATING

## RISKS from ADOPTING AI THAT ORGANIZATIONS TAKE STEPS to MITGATE, 2020

Source: McKinsey & Company, 2020 | Chart: 2021 AI Index Report

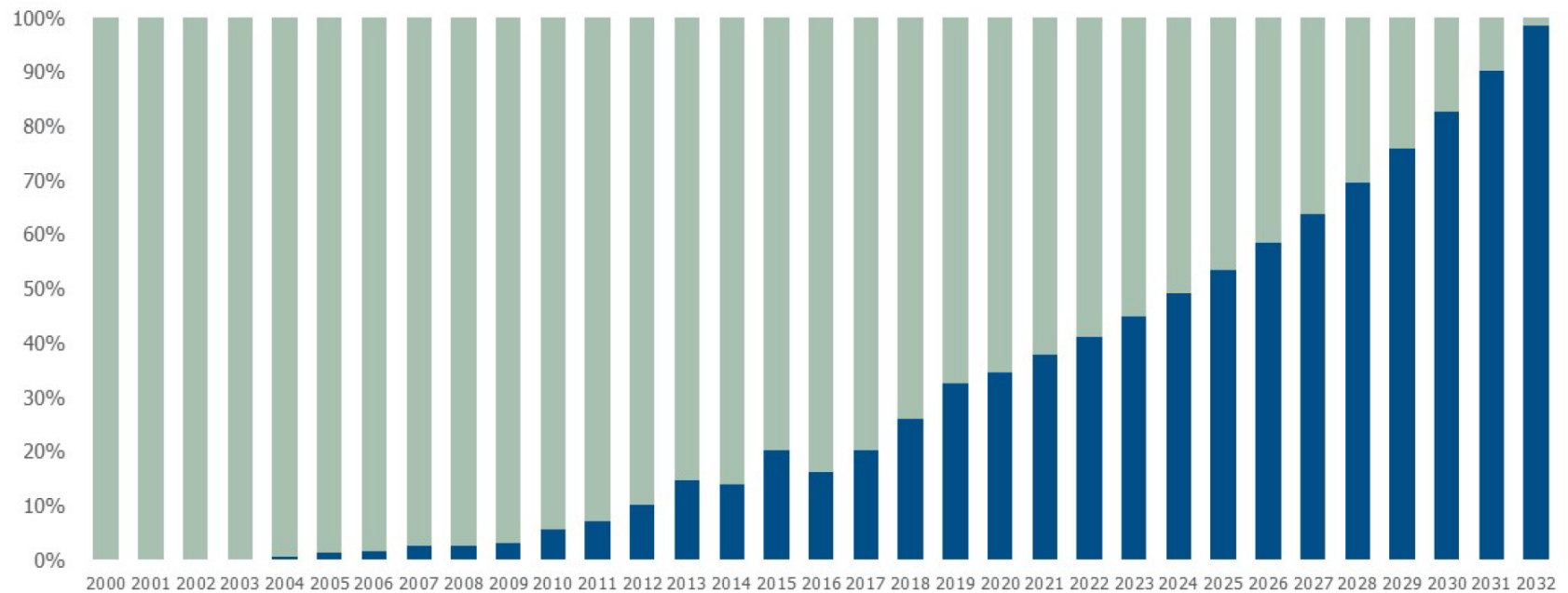


Source: Daniel Zhang, Saurabh Mishra, Erik Brynjolfsson, John Etchemendy, Deep Ganguli, Barbara Grosz, Terah Lyons, James Manyika, Juan Carlos Niebles, Michael Sellitto, Yoav Shoham, Jack Clark, and Raymond Perrault, "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford, CA, March 2021.

We Believe that Cloud will Represent the Primary Means of Software Delivery within the next Decade

# Cloud is eating software

Cloud will become majority of software market within 5 years



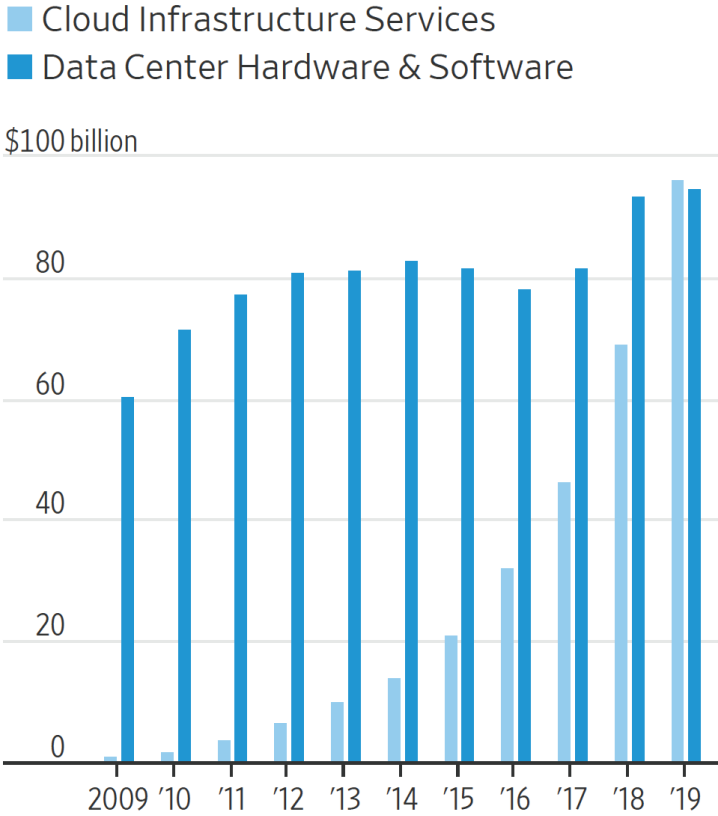
Source: CapIQ; Bessemer Venture Partners analysis;  
Cloud CAGR – 20%, Software CAGR – 10%

■ Software ■ Cloud

Sources: Capital IQ (CapIQ) & Bessemer Venture Partners Analysis, as published in Deeter et al. "State of the Cloud 2020." Bessemer Venture Partners, April 2020. **Forecasts are not an indicator of future performance and any investments are subject to risks and uncertainties.**

# Cloud Spending Hits Record Amid Economic Fallout from Covid-19

## Enterprise spending on cloud and data centers

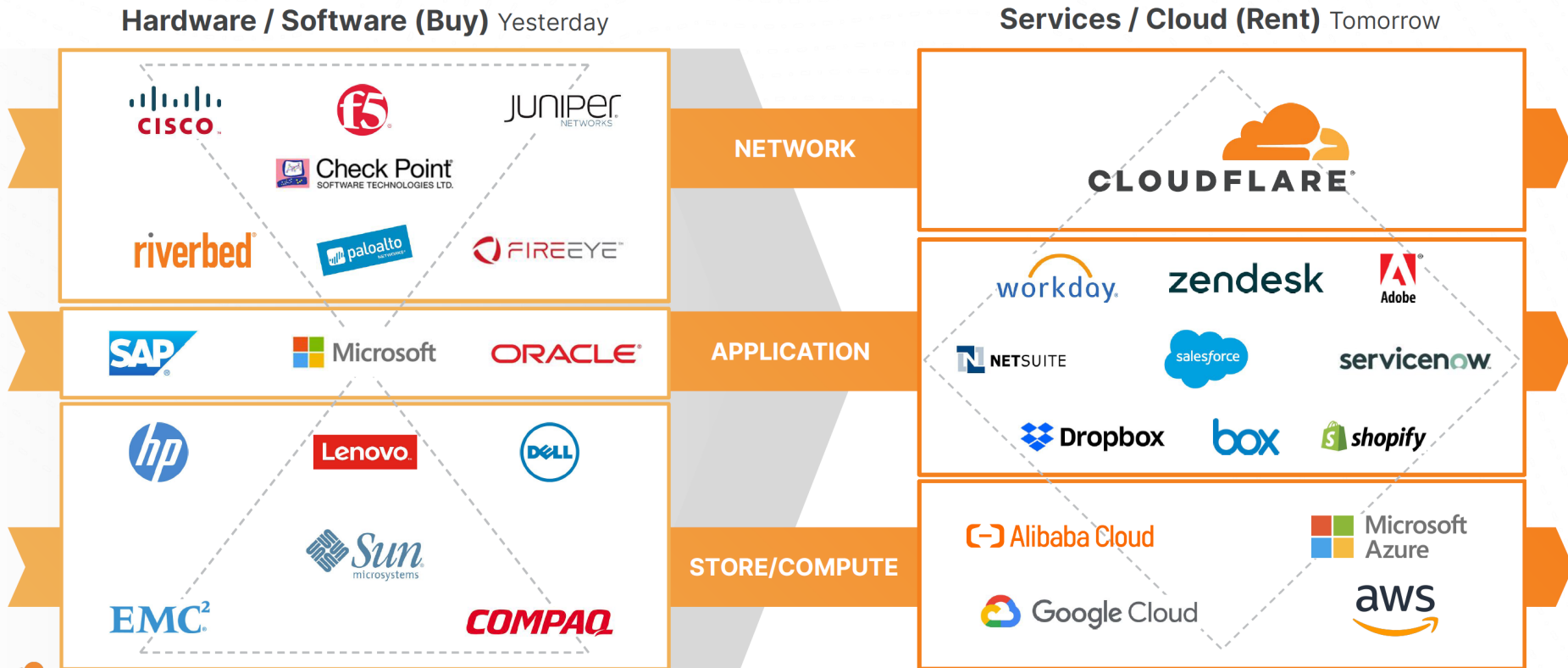


Source: Synergy Research Group

Sources: Synergy Research Group, as cited from Loten, Angus. "Cloud Spending Hits Record Amid Economic Fallout from Covid-19." Wall Street Journal. 3 August 2020.

# How the Picture of Software & Hardware is Changing The Cloudflare Perspective...

## Evolution of Enterprise Stack




# WisdomTree & Team8

*Partnership that Drives  
Expertise in Cybersecurity*



# Introducing Team8 – our partner with deep expertise in cybersecurity space



**TEAM8™**

- Leadership team**
  - + Former Director of NSA
  - + Former Commander of IDF Unit 8200
  - + Former CISO of Citi Group
  - + Cyber Intelligence Community leaders at Fortune 500 companies and leading technologists
- Cyber security experts**
  - + Team8 works closely with their cybersecurity experts, many from Israel's elite 8200 military intelligence unit, and their global advisors

- + Team8 community of **350+ C-level security executives** from **300 enterprises across 20 countries**, **25%** of which are **Fortune 500** and **55%** are **Forbes Global 2000**
- + **Access** to and **collaboration** with leading **Fortune 500 enterprises** around their toughest **cyber challenges**
- + **Companies in Team8 portfolio** hold **leading positions** in multiple cyber markets including **threat detection, IoT security, endpoint isolation, encryption** and **cyber risk management**

Source: Team8.








# Team8 Cyber development themes for 2021

- + **Cybersecurity** market and supply chain is **far broader than solutions purely focused on cyber defence.**
- + **The life cycle and efficacy** of different products is **accelerating** due to the fast pace of **technology innovation** and **rapid evolution of the threats.**
- + Team8 and WisdomTree believe that **the best way to capture the changes in the market is to understand the trends** that are driving it and to **identify the products and services** that are positioned to provide creative and effective solutions.
- + **Team8 outlines the themes, products, and services** that they believe will be **of critical importance** to the industry **in the coming years.**
- + **Each theme** includes the **threats** and **technology trends** driving the theme, as well as some suggested **products and services** that can serve as **solutions to the challenges** created.



Source: Team8, WisdomTree.








# Some drivers behind Team8 Cyber themes

<p><b>Privacy &amp; Digital Trust</b></p> 	<p>Gartner estimates that <b>65%</b> of the world's population will have its <b>personal data</b> covered under modern <b>privacy regulations</b> in the next 2 years, up from <b>10% in 2020</b>.</p>	<p><b>Cloud Security</b></p> 	<p><b>Cloud security</b> is the <b>number one investment area for 2021</b> according to the <b>Team8 2021 CISO Survey</b>, followed by Security Automation and Identity and Access Management.</p>
<p><b>Shift-Left</b></p> 	<p>According to Forrester <b>42% of organizations</b> that experienced an <b>external attack</b> blame the incident on a <b>software security flaw</b> and <b>35%</b> blamed a <b>buggy web application</b>.</p> <p>Yet, the <b>migration</b> of a <b>developer-driven security paradigm</b> has been <b>slow</b> as Google reports <b>only 20% of firms</b> are considered <b>"elite performers" with DevOps</b>.</p>	<p><b>Smarter Security</b></p> 	<p>Organizations are deploying and managing an <b>increasing number of security tools</b>. On average <b>larger organizations</b> estimated to be using <b>130 cyber tools</b>.</p> <p>The global shortage of cyber talent exacerbates the problem. <b>By 2022</b>, the <b>global cybersecurity workforce shortage</b> has been projected to reach upwards of <b>1.8 million</b> unfilled positions.</p>
<p><b>Security of Things</b></p> 	<p>There's an <b>explosion of connected devices</b>, with IDC predicting <b>55.7 billion connected devices worldwide by 2025</b>.</p>	<p><b>Perimeterless World</b></p> 	<p>The <b>COVID-19 pandemic</b> accelerated the trend of <b>working from home</b>. The global workforce is now reliant on at-home WiFi networks and non-hardened work devices.</p>
<p><b>Resilience &amp; Recovery</b></p> 	<p>In 2015, Kaspersky reported that <b>ransomware</b> was doubling every year, but <b>2020 has seen a seven-fold increase</b> according to Bitdefender.</p> <p>Coalition reports <b>65% rise</b> in average severity of <b>insurance claims</b>, from 2019 to 2020, driven largely by the <b>rising costs of ransomware</b>.</p>		<p><b>Remote-first work</b> will remain with us in a post pandemic environment, with <b>72% of office workers</b> indicating a desire to retain the <b>flexibility to work remotely</b> according to PwC's US Remote Work Survey.</p>

Source: Team8, Gartner, PwC, IDC, Bitdefender, Coalition, Forrester, DORA & Google Cloud, RSA Conference 2019, Center for Strategic & International Studies. Forecasts are not an indicator of future performance and any investments are subject to risks and uncertainties.









# Breaking down Team8's cyber themes 1/2

 <b>Cyber theme</b>	 <b>Driver</b>	 <b>Solutions</b>
<p>Cloud adoption is on the rise, and enterprise cloud migrations are expanding from experiments to business critical initiatives. Security capabilities are evolving so that enterprises can retain control over their security posture, data protection programs, and application integrity.</p>	<p><b>Cloud Security</b></p> 	<ul style="list-style-type: none"> <li>+ Reliance on cloud as a business critical system</li> <li>+ Ubiquity of container technology (e.g., Kubernetes)</li> <li>+ Complex hybrid and multi-cloud environments</li> </ul> <ul style="list-style-type: none"> <li>+ Cloud Workload Protection Platform (CWPP)</li> <li>+ Cloud Security Posture Management (CSPM)</li> <li>+ Container Security</li> <li>+ Cloud Infrastructure Entitlement Management</li> <li>+ Cloud Access Security Broker (CASB)</li> <li>+ Extended Detection and Response (XDR)</li> </ul>
<p>IoT device connectivity unlocks new business value in the industrial economy. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and adversaries can move from stealing data to threatening health and safety.</p>	<p><b>Security of Things</b></p> 	<ul style="list-style-type: none"> <li>+ Explosion of connected devices</li> <li>+ Convergence of IT and OT</li> <li>+ Ramifications on the supply chain and physical world, including personal safety</li> </ul> <ul style="list-style-type: none"> <li>+ Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP)</li> <li>+ Vulnerability Management</li> <li>+ IoT Security</li> <li>+ Deception</li> <li>+ Managed Detection and Response (MDR)</li> <li>+ User Behaviour Analytics</li> <li>+ OT Security</li> <li>+ Antivirus</li> </ul>
<p>The enterprise perimeter is nearly extinct and the shift to remote work during the pandemic is accelerating its demise. Identity and zero trust architectures will become increasingly important in governing access management.</p>	<p><b>Perimeterless World</b></p> 	<ul style="list-style-type: none"> <li>+ Remote work</li> <li>+ SaaS</li> <li>+ Cloud migration</li> <li>+ Insider threats</li> </ul> <ul style="list-style-type: none"> <li>+ Identity Access Management</li> <li>+ Zero Trust</li> <li>+ User Entity Behaviour Analysis</li> <li>+ Secure Access Server Edge (SASE)</li> <li>+ Software Defined Perimeter (SDP)</li> <li>+ Cloud Access Security Brokers (CASB)</li> </ul>
<p>Response capacity is stretched to its limits as organizations face immense security complexity – dozens of products that aren't integrated, an expanding enterprise network, a cyber talent shortage, and an adversary leveraging increasingly sophisticated capabilities. Smarter security can plug the gaps.</p>	<p><b>Smarter Security</b></p> 	<ul style="list-style-type: none"> <li>+ Growing attack surface</li> <li>+ Increase in number of security tools</li> <li>+ Shortage of cyber talent</li> <li>+ Pace of attacks</li> </ul> <ul style="list-style-type: none"> <li>+ Security Orchestration, Automation and Response (SOAR)</li> <li>+ Security Information and Event Management (SIEM)</li> <li>+ Robotic Process Automation (RPA)</li> <li>+ Logging &amp; Analytics</li> <li>+ Security Policy Automation</li> </ul>

Source: Team8, WisdomTree.

# Breaking down Team8's cyber themes 2/2

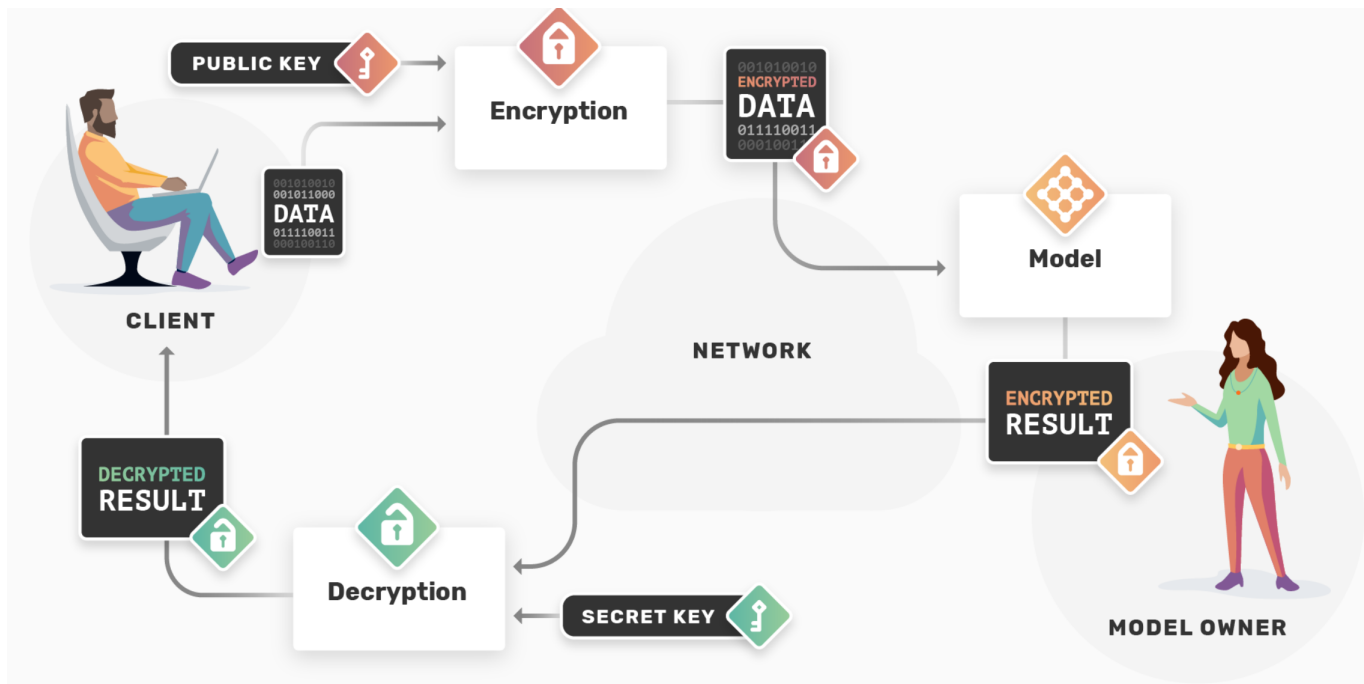
 Cyber theme	 Driver	 Solutions
<p>Globalization and growth of the digital economy are colliding with emerging privacy regulations and consumer preferences, providing users with more control over their data. Architectural design and business processes must accommodate new privacy- and zero trust-driven strategies.</p>	<p><b>Privacy &amp; Digital Trust</b></p>  <ul style="list-style-type: none"> <li>+ Globalization combined with different geopolitical approaches to privacy and data protection</li> <li>+ Growth in data breaches</li> <li>+ Growth in privacy regulations</li> <li>+ Changing consumer preferences</li> </ul>	<ul style="list-style-type: none"> <li>+ Data Discovery</li> <li>+ Data Classification</li> <li>+ Privacy Rights (DSAR)</li> <li>+ Data Protection and Compliance</li> <li>+ Homomorphic Encryption</li> <li>+ Anonymization &amp; Synthetic Data</li> <li>+ Distributed Machine Learning</li> <li>+ Multi-Party Computation</li> </ul>
<p>Digital infrastructure is now business critical, and therefore recovery from cyberattacks is now a core tenet of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery and reconstitution of assets and capabilities.</p>	<p><b>Resilience &amp; Recovery</b></p>  <ul style="list-style-type: none"> <li>+ Increasing pace of cyber attacks</li> <li>+ Ransomware</li> <li>+ Not just about security but also relates to operational resiliency</li> <li>+ Getting it wrong could be fatal</li> </ul>	<ul style="list-style-type: none"> <li>+ Backup and Disaster Recovery</li> <li>+ Application Performance Monitoring</li> <li>+ Self-Healing Systems</li> <li>+ Cyber Exercise Facilitation</li> <li>+ Cyber Ranges</li> </ul>
<p>Developing and managing software is becoming more agile and faster than ever. Security can't come after the fact, but needs to be shifted-left to the developers, embedding security considerations from the start in a DevSecOps model.</p>	<p><b>Shift-Left</b></p>  <ul style="list-style-type: none"> <li>+ Code to production is the new pace of business</li> <li>+ DevSecOps</li> <li>+ Security by Design</li> </ul>	<ul style="list-style-type: none"> <li>+ Static Application Security Testing (SAST)</li> <li>+ Dynamic Application Security Testing (DAST)</li> <li>+ Interactive Application Security Testing (IAST)</li> <li>+ Software Composition Analysis (SCA)</li> <li>+ Secure Development Lifecycle</li> <li>+ Developer Security Training</li> <li>+ Container Security</li> </ul>

Source: Team8, WisdomTree.

**DSAR** is Data Subject Access Requests. **DevOps** is software development (Dev) and IT operations (Ops). **DevSecOps** is the integration of security (Sec) into DevOps processes.

# Homomorphic Encryption

## Performing Calculations on Encrypted Data



### + Advantages:

- Can perform inference on encrypted data, so the client's private data is not exposed and cannot be leaked or misused
- Doesn't require interaction between the data and model owners to perform computations

### + Disadvantages

- Computations are expensive
- Restricted to certain kinds of computations

Source: <https://blog.openmined.org/what-is-homomorphic-encryption/>

# Cloud Security in Focus



- + Cloud Workload Protection Platform (CWPP)
- + Cloud Security Posture Management (CSPM)
- + Container Security
- + Cloud Infrastructure Entitlement Management
- + Cloud Access Security Broker (CASB)
- + Extended Detection and Response (XDR)

## Cloud Security

- + Buoyed by tailwinds from the pandemic and remote work, cloud adoption is on the rise and enterprise cloud migrations are expanding from fringe applications and experiments to business critical initiatives. As such, security capabilities are evolving to allow enterprises to reap the benefits of moving to the cloud while retaining control over their security posture, data protection programs, and application integrity.

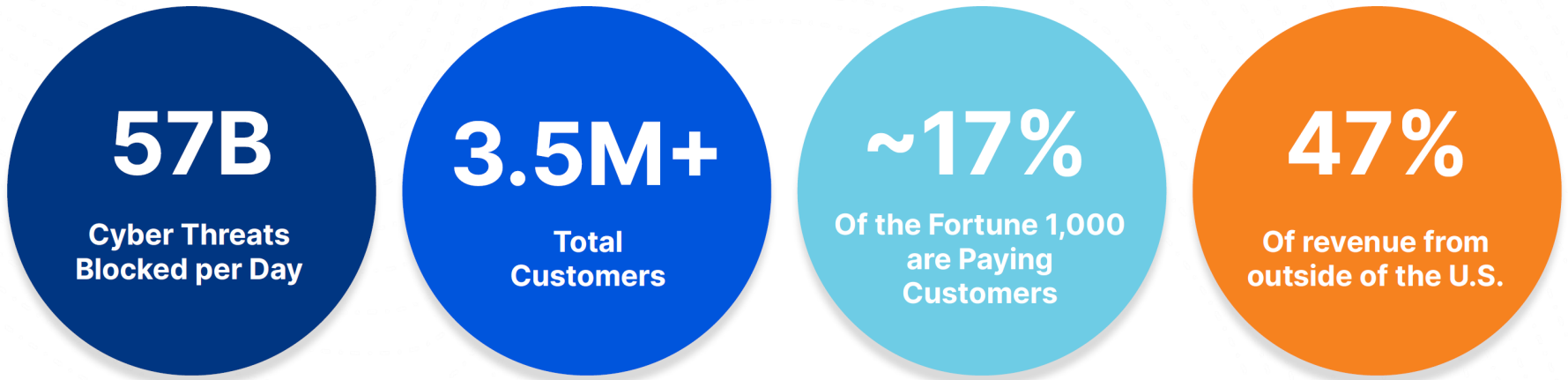
## Impact

- + Attacks are not only still happening, but are being amplified by the pervasiveness, speed, and connectedness of the cloud. Instead of applying legacy solutions to the cloud, organizations need security solutions that are architected for the cloud, combining control and integrity with scalability and agility.



Source: Team8, WisdomTree.

# We Operate at Massive Scale



Source: Cloudflare 4Q 2020 Investor Presentation. Cyber threats blocked per day is an approximate average for the three months ended 31 December 2020.

# Are Customers Spending Enough on Security? CrowdStrike's Perspective...

## CLOUD WORKLOADS ARE UNDER PROTECTED

### CLOUD IT SPEND

2020

2023

IaaS and PaaS Vendor Revenue Estimate, IDC

\$106.4 BILLION

\$217.7 BILLION

### CLOUD SECURITY SPEND

Worldwide Hybrid Cloud Security Revenue Estimate, IDC

\$1.2 BILLION

\$2.0 BILLION

Cloud Security Spend as % of Cloud IT Spend

1.1%

0.9%

Insufficient Cloud  
Security Investment

Source: CrowdStrike Corporate Overview, March 2021.

# Security of Things in Focus



- + Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP)
- + Vulnerability Management
- + IoT Security
- + Deception
- + Managed Detection and Response (MDR)
- + User Behaviour Analytics
- + OT Security
- + Antivirus

## Security of Things

- + Technology advances are fuelling Internet of Things (IoT) device connectivity that is driving the Industrial Economy to digitize and unlock new business value. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and the stakes are raised. Cyber threats move from data to people – disrupting supply chains and infrastructure critical to health and safety.

## Impact

- + Ransomware is increasingly focused on OT environments and is now one of the top threats facing CISOs and CIOs. As 5G proliferates, everything will become "a thing" and the concept of networks will change. IT security controls can't adapt to work in OT environments. To mitigate risk of threats that cross the IT/OT boundary, new models and mindsets are needed.

**RAPID7**

  
CROWDSTRIKE

 FIREEYE™

 paloalto®  
NETWORKS

  
Qualys.

 tenable®

Source: Team8, WisdomTree.  
CISO is Chief Information Security Officer. CIO is Chief Information Officer.

# What Might a Breach Look Like? RAPID7 Example...

The screenshot displays the Rapid7 Insight interface. At the top left, the logo and name 'Rapid7 Insight' are visible. The main heading is 'Investigation'. Below this, there are columns for 'User', 'Asset', and 'Investigation status'. A modal window is open, titled 'Asset "BOS-D-1094" Quarantined'. Inside the modal, under 'Suggested Next Actions', there are three items:

- 6 Assets Directly Accessible**  
Recommended Action: Quarantine 6 assets immediately. Buttons: Details, Quarantine 6 Assets
- 24 Cloud Accounts Accessible**  
Recommended Action: Revoke Access to all accounts immediately. Buttons: Details, Revoke 24 Accounts
- 19 Network Endpoints Show Indicators**  
Recommended Action: Investigate endpoint details in InsightIDR. Buttons: Details, Investigate

A 'Done' button is located at the bottom left of the modal. In the background, a user profile for 'Alice Smith, ENG MGR' is visible, along with a 'Suggested Base' section and a 'Details' button for the asset 'BOS-D-1094'. At the bottom of the interface, there are sections for 'Enriched indicators with Recorded Future' and 'InsightConnect Automation' with a 'View' button.

Source: Rapid7 Investor Day Presentation, 10 March 2021.



# Estimated Consequences of a Breach FireEye's Perspective...

## Side Effects of a Breach



### Stunted Growth

A breach can stall a company's growth for up to 3 years



### Reduced Stock Price

Average stock price decline of 3% – 7.5% after breach disclosure



### Incurred Cost

Average cost of a data breach is ~\$4 million USD or ~\$150 USD per lost record



### Lost Customers

Breaches cause abnormal customer turnover of 3.9% on average

Source: FireEye 2021 Corporate Presentation.

# Perimeterless World in Focus



- + Identity Access Management
- + Zero Trust
- + User Entity Behaviour Analysis
- + Secure Access Server Edge (SASE)
- + Software Defined Perimeter (SDP)
- + Cloud Access Security Brokers (CASB)

## Perimeterless World

- + The enterprise perimeter is nearly extinct and the dramatic shift to remote work during the pandemic is accelerating its demise. Security needs rethinking in a world without perimeters, where identity and zero trust architectures will need to play increasingly important roles governing access management.

## Impact

- + With less and less behind the walls of the enterprise, companies can no longer take a fortress approach to defend against threat actors. Security strategies need to change to support new ways of doing business that drive growth, productivity, and competitive advantage.

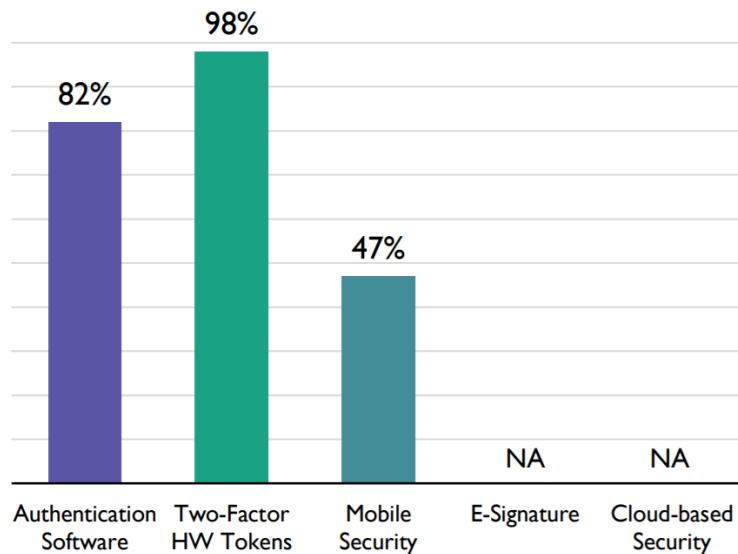


Source: Team8, WisdomTree.

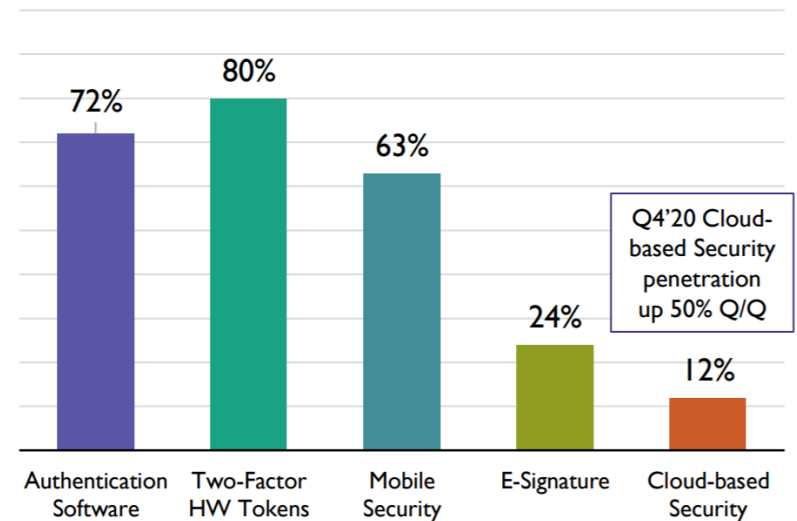
# What Security Services Look Like is Changing The OneSpan Example...

## Significant Growth Opportunity in Existing Customer Base

Product Penetration – December 31, 2015<sup>1</sup>



Product Penetration – December 31, 2020<sup>1</sup>



Source: OneSpan March 2021 Corporate Presentation.

# Conclusion

*Cybersecurity is subject to  
continual Evolution &  
Innovation*

## Conclusion

- + Cybersecurity issues will continue to generate headlines and attract attention
- + Ransomware, Phishing...these are just some of the types of things companies and individuals need to be thinking about and prepared for
- + There is a constant race between the 'bad actors' and those looking to protect networks
- + There is no substitute for expertise when it comes to Cybersecurity, since it's a megatrend that changes quickly.

# Questions

For more information and insight please visit: [wisdomtree.eu](https://wisdomtree.eu)



WISDOMTREE®

A MOMENT IN MARKETS

*Can equity investors look beyond rising yields?*

READ NOW



WISDOMTREE®



**HYDROGEN FUEL CELLS'  
COMING OF AGE?**

READ NOW



WISDOMTREE®



TEAM8 BLOG SERIES

**Smarter Security**

Cybersecurity must Learn and Evolve to Match the Environment

READ NOW



# Disclaimer

**Communications issued in the European Economic Area (“EEA”):** This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

**Communications issued in jurisdictions outside of the EEA:** This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as “WisdomTree” (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

**For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.**

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

This document may contain independent market commentary prepared by WisdomTree based on publicly available information. Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Any third party data providers used to source the information in this document make no warranties or representation of any kind relating to such data. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.

This document may contain forward looking statements including statements regarding current expectations or beliefs with regards to the performance of certain assets classes and/or sectors. Forward looking statements are subject to certain risks, uncertainties and assumptions. There can be no assurance that such statements will be accurate and actual results could differ materially from those anticipated in such statements. WisdomTree strongly recommends that you do not place undue reliance on these forward-looking statements.

Any historical performance included in this document may be based on back testing. Back testing is the process of evaluating an investment strategy by applying it to historical data to simulate what the performance of such strategy would have been. However, back tested performance is purely hypothetical and is provided in this document solely for informational purposes. Back tested data does not represent actual performance and should not be interpreted as an indication of actual or future performance.