WHITE PAPER

Cyber Threat Predictions for 2023

An Annual Perspective by FortiGuard Labs

While "less is more" is the critical strategy behind consolidating networks and security, "more is more" seems to be the mantra cybercriminals continue to live by.

The most troubling trend we've observed across the cyber landscape is one we see continuing into the future—that threats of all kinds are becoming increasingly ubiquitous. From Ransomware-as-a-Service (RaaS) to new attacks on nontraditional targets like edge devices to the emerging use of wipers, the volume and variety of cyberthreats will keep security teams on their toes in 2023 and beyond.

A Look Back at Our 2022 Predictions

Last year, we made several predictions about how the threat landscape would evolve, ranging from attackers spending more effort on pre-attack activities to an increasing number of attack attempts impacting operational technology (OT). Let's look at how some of our predictions fared and how we expect these threats to evolve as we plan for 2023.

The Rise of Advanced Persistent Cybercrime

We predicted a rise in new vulnerabilities and more "left hand" activity, or pre-attack reconnaissance and weaponization, among attackers that would pave the way to further escalate the growth of Crime-as-a-Service (CaaS). And in just the first half of 2022, the number of new ransomware variants we identified increased by nearly 100% compared to the previous six-month period, with our FortiGuard Labs team documenting 10,666 new ransomware variants in 1H 2022 compared to just 5,400 in 2H 2021. This explosive growth in new ransomware variants can be primarily attributed to the growing popularity of RaaS on the dark web. That's right: Like streaming media or food delivery apps, we anticipate that cybercriminal organizations will use subscription-model services and purchase plug-and-play ransomware to achieve a quick payday. To add more pressure on victims, RaaS operators often threaten to leak stolen data on the dark web if their demands aren't met.

While the number of ransomware variants being introduced is skyrocketing mainly due to RaaS, ransomware payments are also climbing. The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) reported that organizations paid out almost $600 million in ransomware in the first half of 2021, which puts the U.S. on track to surpass the combined payouts of the previous decade in a single year.[1] According to a recent survey, 72% of respondents claim they have a ransom policy in place, and the procedure for 49% of them is to pay the ransom outright.[2]

We now predict that the CaaS market will expand significantly into 2023 and beyond, with new exploits, services, and structured programs soon being offered to threat actors through subscription models.

How to Protect Your Environment

We're already seeing the growth of CaaS contribute to an increased volume of attacks. For organizations, it's no longer a matter of "if" but "when" they're breached. Standard security tools—EDR technology, sandbox solutions augmented with MITRE ATT&CK mappings, anti-malware engines using AI detection signatures, advanced intrusion prevention system (IPS) detection, and NGFWs—must be able to scale to address the proliferation of cyber threats. New reconnaissance tools and services that monitor dark web activity, such as locating compromised credentials for sale, are essential in helping organizations stop attacks before they can happen. Ideally, these technologies should be deployed everywhere an organization operates, from data centers to branch offices, using an integrated security platform that can see, share, correlate, and respond to threats as a unified solution. Finally, using deception technology such as honeypots is essential in developing a secure infrastructure and detecting attacker activity early in the kill chain.

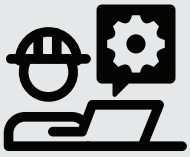
Edge Attacks Go Mainstream

Edge devices such as OT systems and satellite-based internet networks were once considered nontraditional (and less popular) targets for crafty attackers. Yet over the past decade, we've observed a rise in the sophistication and volume of attempted cyberattacks against these targets. The near-universal convergence of IT and OT networks has made it easier for attackers to access OT systems through compromised home networks and remote worker devices. And now, according to the Fortinet 2022 State of Operational Technology and Cybersecurity Report, 93% of organizations experienced an intrusion targeting their OT infrastructure in the past 12 months, with 83% experiencing more than three.[3]

Last year, we predicted that threat actors would increasingly use Edge-Access Trojans (EATs) to target edge environments, and we saw several examples of this play out. One such example observed by FortiGuard Labs in March 2022 was a generic Trojan named StartPage that changes a browser's homepage to display advertising, promote misleading or malicious applications, or exploit the browser to run threats. It drove a global uptick in malware delivery to OT devices.

We also predicted that satellite-based internet networks would become a new target for cybercriminals. As the size and scale of these networks continue to grow, so do the number of compromise attempts. Earlier this year, hackers used AcidRain, a new destructive strain of wiper malware, to attack a satellite communications company's infrastructure in Ukraine, impacting satellite-based internet connections across Europe. The attack also knocked nearly 6,000 German wind turbines offline, where turbine controls became unavailable because of their compromised satellite connection. We expect these types of satellite-based attacks to continue, with the biggest targets being organizations that rely on satellite-based connectivity to support low-latency activities, such as cruise and cargo ships, airlines, oil and gas rigs and pipelines, and remote field offices.

The motivation for cybercriminals looking to exploit edge devices is simple: Targets like OT systems and satellite-based networks offer attackers new entry points into an organization's environment. The increase in network edges also means there are more places for living-off-the-land-type threats to hide, allowing attackers to make their malicious operations appear as normal network activity and go undetected.



How to Protect Your Environment

OT and edge systems are, and will continue to be, highly desirable targets for attackers. While many attacks use purpose-built tools to target these systems, other breach attempts target IT platforms but end up doing damage to OT as well. Then these attacks impact the IT systems now being used to monitor and control OT platforms. To protect OT successfully, we must also protect IT. Security must be part any IT/OT convergence strategy from day zero.

There are foundational steps security leaders can take to ensure their OT/IT environments are secured. Best practices include conducting network mapping and connectivity analysis, detecting suspicious activities, implementing a zero-trust framework, aligning the right remote access tools, and implementing a strong identity and access management (IAM) strategy.

Ransomware and Wipers Run Rampant

Ransomware is getting nastier and more expensive all the time. In a global ransomware survey conducted by Fortinet, 67% of organizations report suffering a ransomware attack.[4] Even worse, almost half said they had been targeted more than once, and nearly one in six said they were attacked three or more times.[5]

In 2021, we began to see early indications that attackers were upping the ante by adding wiper malware to their ransomware attacks. Wiper malware, which was initially discovered a decade ago, gives cybercriminals the ability to delete data and cripple critical system availability, such as OT or manufacturing equipment and servers, unless a ransom demand is met. Given the level of convergence we've seen between various attack methods and advanced persistent threats (APTs), we anticipated that an increasing number of ransomware attacks would be combined with more destructive capabilities like wiper malware.

This year, the war in Ukraine fueled a substantial increase in disk wiping malware among threat actors primarily targeting critical infrastructure. FortiGuard Labs identified at least seven major new wiper variants in the first six months of 2022 that were used in various campaigns against government, military, and private organizations. This number is significant because it's close to the total number of wiper variants that have been publicly detected in the decade since 2012. Additionally, these wipers didn't stay in one geographical location—they were detected in 24 countries in addition to Ukraine.

Wiper malware trends reveal a disturbing evolution of more destructive and sophisticated attack techniques. The rising prevalence of wiper malware is an indicator that these weaponized payloads aren't limited to one target or region and will likely be used in combination with other cybercrime playbooks in the future. Combining wiper malware with ransomware represents a vicious new combination that ups the ante for criminals looking to extort payments from their victims.

How to Protect Your Environment

There are several best practices organizations should implement to minimize the impact of wiper malware. Using inline sandboxing is an excellent starting point to protect against ransomware and wiper malware. As a result, only benign files will be delivered to your endpoints. Another important countermeasure is to have backups available. However, malware often actively searches for backups on the machine (such as Windows Shadow Copy) or the network to destroy. Therefore, backups must be stored off-site and offline to survive sophisticated attacks. Proper network segmentation is also helpful—if an attack occurs, segmentation can help contain an incident to just one part of the network. Have disaster recovery and incident response plans in place, as those preparedness efforts often make the difference between successfully averting data loss and complete data destruction.

And as always, patch your systems. Most successful attacks target vulnerabilities for which a patch is readily available. Good cyber-hygiene practices can be worth their weight in gold when a malicious attack targets known vulnerabilities.

Weaponizing Artificial Intelligence

AI is already used defensively to detect unusual Internet-of-Things (IoT) behavior that may indicate an attack, usually by botnets. And as we predicted, cybercriminals have begun to increasingly take advantage of AI to support a multitude of malicious activities, ranging from thwarting the algorithms that detect abnormal network activity to mimicking human behavior.

One such example of attackers weaponizing AI is the development of deepfakes. The term "deepfake" was first used five years ago. This attack vector presents a growing cause for concern. There are several methods for creating deepfakes, and the technologies are rapidly improving. One of the most popular is using the generative adversarial network (GAN), which trains itself to recognize patterns using algorithms that can also be used to create fake images. Another method is through AI algorithms called encoders, which are used in face-replacement and face-swapping technology. The decoder retrieves and swaps images of faces, enabling one face to be superimposed onto a completely different body.

Many of the deepfake examples that have captured headlines in the past year—like NVIDIA using a computer-generated video to make it appear that CEO Jensen Huang was giving a press conference from his kitchen—weren't created by cybercriminals looking to steal sensitive information. But deepfakes certainly represent another potential threat vector that security teams and their organizations need to consider. We're already seeing some instances of hackers using these tactics to support criminal activities.

How to Protect Your Environment

Web filtering, antivirus software, and EDR technology all have a role to play in protecting an organization against the weaponization of AI. However, one of the most effective defense methods for preventing AI-related attacks is cybersecurity awareness education. While many organizations offer basic security training programs for employees, enterprises should consider adding new modules that provide education on spotting AI-focused threats. For example, a session on deepfakes might offer tips for identifying deepfake videos, such as unnatural eye movement, a lack of blinking, inconsistent facial positions, and more.

Hello, Crypto Wallet Heists

Bank transactions and wire transfers used to be prime targets for cybercriminals. Yet as banks increasingly enhance their security measures—encrypting transactions and requiring multi-factor authentication (MFA)—it's now more difficult for hackers to intercept these transactions. But as the saying goes, "When one door closes, another opens." As predicted, we observed more instances of malware designed to target stored crypto credentials and drain digital wallets. Digital wallets are easy targets for hackers, as they tend to be less secure.

We can point to numerous examples of major non-fungible token (NFT) hacks that occurred in 2022. In February, attackers launched a phishing attack on OpenSea users, stealing $1.7M in NFTs. Then hackers successfully stole $400K in NFTs from Premint users just a few months later. Several NFT hacks that occurred on the popular social platform Discord also made headlines. That said, the vulnerabilities and further exploitation in these blockchains are still yet to be widely exploited, which may fuel further skepticism regarding cryptocurrency markets.

How to Protect Your Environment

Keeping crypto wallets safe starts with the wallet owner. Using a non-custodial wallet is preferred, as it gives the crypto user full ownership of their cryptocurrency holdings and control over their private keys. A custodial wallet—or one owned by a third party—is riskier, as the user doesn't have total control over their wallet.

New Attack Trends to Watch for in 2023

It's no secret that hackers will continue to rely on certain tried-and-true attack tactics, particularly those that are easy to execute and help them achieve a quick payday. However, our FortiGuard Labs team predicts that several distinct new attack trends will emerge in 2023. Here are some of the unique security attack developments we'll be watching for in the next year.

New Crime-as-a-Service Offerings

Given cybercriminals' success with RaaS, we predict that a growing number of additional attack vectors will be made available as a service through the dark web. In addition to the sale of ransomware and other Malware-as-a-Service (MaaS) offerings, we'll also start to see new criminal solutions and an increase in the sale of access to pre-compromised targets.

CaaS could be an attractive business model for threat actors. We expect to see more turnkey, subscription-based offerings being made available to threat actors. This emerging model would allow cybercriminals of all skill levels to deploy more sophisticated attacks without investing the time and resources up front to craft their own unique plan. And for seasoned cybercriminals, creating and selling "as a service" attack portfolios offer a simple, quick, and repeatable payday.

As a result, get ready for an expanded CaaS portfolio to emerge in 2023 and beyond. We also anticipate that threat actors will begin to leverage emerging attack vectors such as deepfakes, offering these videos and audio recordings and related algorithms more broadly for purchase. Beyond targeting high-profile celebrities and public officials, we expect threat actors to expand their purview to include influencers, particularly those with a strong digital presence. Casting a wider net like this offers cybercriminals more opportunities to impersonate others and lure unsuspecting fans into taking an action, such as "purchasing" a product that doesn't actually exist.

In addition to deepfakes, we predict that Reconnaissance-as-a-Service will increase in popularity. As attacks become more targeted, threat actors will likely hire "detectives" on the dark web to gather intelligence on a particular target before launching the attack. Like the insights one might gain from hiring a private investigator, Reconnaissance-as-a-Service offerings may serve up attack blueprints—to include an organization's security schema, key security personnel, the number of servers they have, known external vulnerabilities, and even compromised credentials for sale, and more—to help a cybercriminal carry out a highly targeted and effective attack.

Money Laundering Gets a Boost from Automation

To help grow a criminal organization, leaders and affiliate programs usually employ money mules—people who are knowingly or unknowingly used to help launder money on behalf of a crime syndicate. Money mules are often recruited through advertisements and are used to anonymously move money from one country or bank account to another. This money shuffling is typically done through anonymous wire transfer services or through crypto exchanges to avoid detection. Using unknowing mules for transactions and the physical relocation of money helps to avoid leaving a digital trace and is still common. Funds are often fragmented into smaller batches and then transferred through multiple channels to avoid triggering alerts mandated by anti-money laundering laws.

Setting up money mule recruitment campaigns has historically been a time-consuming process, as cybercrime leaders go to great lengths to create websites for fake organizations and subsequent job listings—typically for accounts receivable-type positions—to make their businesses seem legitimate, successfully recruit mules, and evade law enforcement. We anticipate that cybercriminals will start using machine learning (ML) for recruitment targeting, helping them to better identify potential mules while reducing the time it takes to find these recruits.

We also expect to see manual mule campaigns replaced with automated services that move money through layers of crypto exchanges, making the process faster and more challenging to trace. Like adding coins to a machine at a laundromat, cybercriminals will be able to pay a fee to kick off an automated campaign, reducing manual recruitment needs or even cutting it entirely out of the process.

Money Laundering-as-a-Service is clearly on the horizon. This could quickly become part of the growing CaaS portfolio. And for the organizations and individuals that fall victim to this type of cybercrime, the move to automation means that money laundering will be harder to trace, decreasing the chances of recovering stolen funds.

Virtual Cities Welcome a New Wave of Cybercrime

The metaverse is giving rise to new, fully immersive experiences in the online world, and cities are some of the first to foray into this new version of the internet driven by augmented reality (AR), virtual reality (VR), and mixed reality (MR) technologies. These virtual cities—Dubai being the first—promise to replicate real-life experiences and places: Individuals can create avatars that can then work, play, shop, and more in a virtual space. Retailers are even launching digital goods available for purchase in these virtual worlds. Late last year, designer Ralph Lauren launched an exclusive digital clothing collection on the online gaming platform Roblox.

However, while these new online destinations open a world of possibilities, they also open the door to an unprecedented increase in cybercrime. Consider that an individual's avatar is essentially a gateway to their personally identifiable information (PII), making them prime targets for attackers. Because individuals can purchase goods and services in virtual cities, digital wallets, crypto exchanges, NFTs, and any currencies used to transact offer threat actors yet another attack surface. These virtual goods and assets can also be stolen and resold. Biometric hacking could also become a real possibility because of the AR- and VR-driven components of virtual cities, making it easier for a cybercriminal to steal fingerprint mapping, facial recognition data, and retina scans and then use those for malicious purposes.

Playing the (Attack) Long Game

We can predict that certain new technologies will offer cybercriminals new opportunities for compromise. Based on what we know today about emerging technologies, such as Web3, as well as those that seem to be more rampant and destructive than ever, here are several longer-term predictions about how we can expect the threat landscape to evolve, not just in the next 12 months but over the coming years.

Wipeout

Wiper malware has made a dramatic comeback this year, with attackers introducing new variants of this decade-old attack method. While the growth in the prevalence of wiper malware itself is alarming, we anticipate that threat actors will increasingly combine various threats to maximize the level of ongoing destruction they can cause. For example, a cybercriminal could easily combine a computer worm with wiper malware, making it easier for the malware to replicate quickly and spread more widely. Given the right vulnerability, such an exploit could cause massive destruction in a short period of time. This makes time to detection, and the speed at which security teams can remediate, paramount.

Looking ahead, the use of wipers in combination with other attack vectors is one of the biggest emerging threats we're facing as a security community. Wipers can potentially take cyberspace by storm, impacting IT networks across public and private sectors worldwide. Because of the commoditization of wipers, these have the potential to impact networks at exponential scale.

The Wild West of Web3

Web3, a new, blockchain-based iteration of the internet that aims to decentralize ownership of the digital economy, is quickly becoming mainstream, with an increasing number of corporations beginning to experiment with Web3 tools. And it's easy to see why: Web3 offers organizations many potential benefits, such as making it easier for development teams to deploy applications without managing and maintaining new infrastructure to support that process.

But just like any new technology, Web3 isn't without security risks. Web3 is about the user controlling their own data. And if there's anything we've learned from past security incidents, it's that users are often the weakest link. And although the irreversible aspect of blockchain offers some benefits, it introduces challenges as well. For example, Web3 wallets today don't use MFA, rely only on passwords, and they're difficult to recover if lost.

We anticipate that before Web3 goes mainstream, we'll see some regulations introduced on how network nodes—the nodes that are responsible for maintaining the state of the network—address fraudulent activities and stolen data. Protocols should be in place so that when a fraud is committed, the activity can be traced and contained in the same way banks do when an unauthorized individual uses a credit card.

Cue the Q-Day Preparations

Quantum computing began more than four decades ago, but in recent years, both public and private sector organizations have increased their investments in this technology. A recent McKinsey and Company report asserts, "While quantum computing promises to help businesses solve problems that are beyond the reach and speed of conventional high-performance computers, use cases are largely experimental and hypothetical at this early stage."[6] Quantum computing is already providing a breakthrough in things like breaking previously unbreakable cryptographic algorithms.

Although certain quantum computing capabilities might not be widely applicable or available today, some experts warn that quantum day (also called Q-Day)—the point at which quantum computers become powerful enough to break current-day encryption mechanisms—is quickly approaching. And while the security community is working to create new encryption algorithms designed to stand up to quantum computers, this effort is still a work in progress.

For example, just a few months ago, NIST announced the winners of a multi-year contest in which entrants were asked to design new encryption standards that could potentially defend against quantum computers. One of these post-quantum encryption algorithms—Supersingular Isogeny Key Encapsulation, or "SIKE" for short—quickly suffered a cyberattack from a single-core computer that successfully broke the encryption. Months later, the National Security Agency (NSA) released its Commercial National Security Algorithm Suite (CNSA) 2.0—a collection of cryptographic algorithms designed to replace the encryption algorithms used today. All of these were analyzed and deemed secure against quantum computers. While NSA issued guidance and a suggested timeline for implementing these algorithms, it's too early to understand the implementation rate and success of these new encryption standards.

Quantum computing will undoubtedly evolve and become more powerful in the future, even beyond its eventual ability to crack encryption algorithm. Because quantum computing elevates processing capabilities by an unfathomable amount, it's possible that they'll eventually be used by cybercriminals for additional activities. One potential example is bad actors using quantum computing to weaponize AI and then apply it to application fuzzing in the quest for new zero-day vulnerabilities.

Defending Against the Evolving Threat Landscape

Threat actors may be expanding their respective bags of tricks, but the good news is that numerous efforts are underway to push back against the cybercrime ecosystem. The Department of Justice (DOJ) saw key victories against ransomware operators this year. In January, 14 members of the notorious REvil cybersecurity gang were arrested in Russia at the request of U.S. authorities. REvil was responsible for the Kaseya attack, and one of the hackers was also involved in the Colonial Pipeline incident. A month later, two individuals were arrested in New York City for conspiring to launder the proceeds of 119,754 bitcoin that were stolen from a virtual currency exchange and initiated more than 2,000 unauthorized transactions. Law enforcement has seized over $3.6 billion in cryptocurrency linked to that hack so far.

Partnerships that span across countries and vendors are helping to identify cybercrime syndicates as well. As one of the founding members of the World Economic Forum's (WEF) Partnership Against Cybercrime (PAC), Fortinet strives to do this with the Cybercrime ATLAS project, a mission dedicated to mapping cybercriminal ecosystems to better understand their blueprint, then disrupt. FortiGuard Labs shares intelligence and works with a number of additional organizations, including: Microsoft Active Protections Program (MAPP), Forum of Incident Response and Security Teams (FIRST), Cyber Threat Alliance (CTA), INTERPOL Global Crime Expert Group (GCEG) and Gateway Project, NATO Industry Cyber Partnership (NICP), World Economic Forum's Centre for Cybersecurity, and MITRE Engenuity Center for Threat Informed Defense.

Tracking down attackers and tactics makes it easier to know what to do about an attack. Attributing where funds are moving also helps, including crypto wallets and currency flows. And instead of focusing solely on operators, more investigations are going after affiliates, which sends the message that they are not immune from prosecution.

While this progress is promising, the reality is that cybercriminals aren't ever entirely going away. But many of the threats we're observing are simply an evolution of the typical tactics we've seen threat actors rely on for years. Even with zero-day attacks, cybercriminals all have the same goal: to infiltrate networks and steal sensitive information. While keeping up with the volume and velocity of threats can often feel like an uphill battle, the good news is that most of the tactics they're using to execute these attacks are familiar, which better positions security teams to protect against them.

Here's our best advice for protecting your environment and staying one step ahead of the bad actors.

Understand the Lifecycle of a Cyberattack

To effectively defend your organization, you need to better understand cybercriminals, their motivations, their tactics, and how they act. The MITRE ATT&CK framework can help with this, as it documents common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against enterprise networks. ATT&CK can be used in several ways to support security operations, threat intelligence, and security architecture.

Adopt a Cybersecurity Mesh Platform

A broad, integrated, and automated cybersecurity mesh platform is essential for reducing complexity and increasing security effectiveness, especially as networks expand and bad actors increasingly find new ways to carry out their exploits. Cybersecurity defenses have traditionally been deployed one solution at a time, usually in response to an emerging challenge. But a collection of point solutions isn't effective in today's landscape. Consolidation and convergence into a single cybersecurity platform is crucial, allowing for much tighter integration, increased automation, and a more rapid, coordinated, and effective protection of and response to threats across the network. To enable a quick and coordinated response, security solutions should be enhanced with AI so they can detect attack patterns and stop threats in real time. Solutions also should be able to scale to address the increase in attacks. Organizations should ideally have these solutions in place:

- Digital risk protection service (DRPS) and deception technology designed to counter attacks at the reconnaissance phase
- Web, DNS, and C2 protection
- Anti-malware tools that include AI detection signatures
- Advanced intrusion prevention system (IPS) detection
- Endpoint detection and response (EDR)
- AI-powered inline sandboxing technology with MITRE ATT&CK mappings

Ideally, the solutions should be deployed consistently across the distributed network, including the data center, campus, branch, multi-cloud, home office, and endpoint.

Implement Network Segmentation and Microsegmentation

Network segmentation offers many benefits for businesses. Segmentation improves security by preventing attacks from spreading across a network and infiltrating unprotected devices. In the event of an attack, segmentation also ensures that malware can't spread into other enterprise systems.

Microsegmentation is a network security technique that enables security architects to further segment an environment for lateral visibility of all assets in the same broadcast domain. Granularity is achieved by logically dividing the network environment into distinct security segments down to the individual workload level. Because policies are applied to individual workloads, microsegmentation offers enhanced resistance to attacks. And if a breach does occur, it limits a hacker's ability to move among compromised applications.

About FortiGuard Labs

FortiGuard Labs is the threat intelligence and research organization at Fortinet. Its mission is to provide Fortinet customers with the industry's best threat intelligence designed to protect them from malicious activity and sophisticated cyberattacks. It is composed of some of the industry's most knowledgeable threat hunters, researchers, analysts, engineers, and data scientists in the industry, working in dedicated threat research labs all around the world. FortiGuard Labs continuously monitors the worldwide attack surface using millions of network sensors and hundreds of intelligence-sharing partners. It analyzes and processes this information using AI and other innovative technology to mine that data for new threats. These efforts result in timely, actionable threat intelligence in the form of Fortinet security product updates, proactive threat research to help our customers better understand the threats and actors they face, and threat intelligence to help our customers better understand and defend their threat landscape. Learn more about Fortinet, the Fortinet Blog, and FortiGuard Labs.

[1] "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," U.S. Treasury Financial Crimes Enforcement Network, October 15, 2021.

[2] "Fortinet Ransomware Survey Shows Many Organizations Unprepared," Fortinet, September 29, 2021.

[3] "2022 State of Operational Technology and Cybersecurity Report," Fortinet, June 21, 2022.

[4] "Fortinet Ransomware Survey Shows Many Organizations Unprepared," Fortinet, September 29, 2021.

[5] "Fortinet Ransomware Survey Shows Many Organizations Unprepared," Fortinet, September 29, 2021.

[6] "Quantum Computing: An Emerging Ecosystem and Industry Use Cases," McKinsey and Company, December 2021.

November 4, 2022 3:29 PM

1346406-0-0-EN