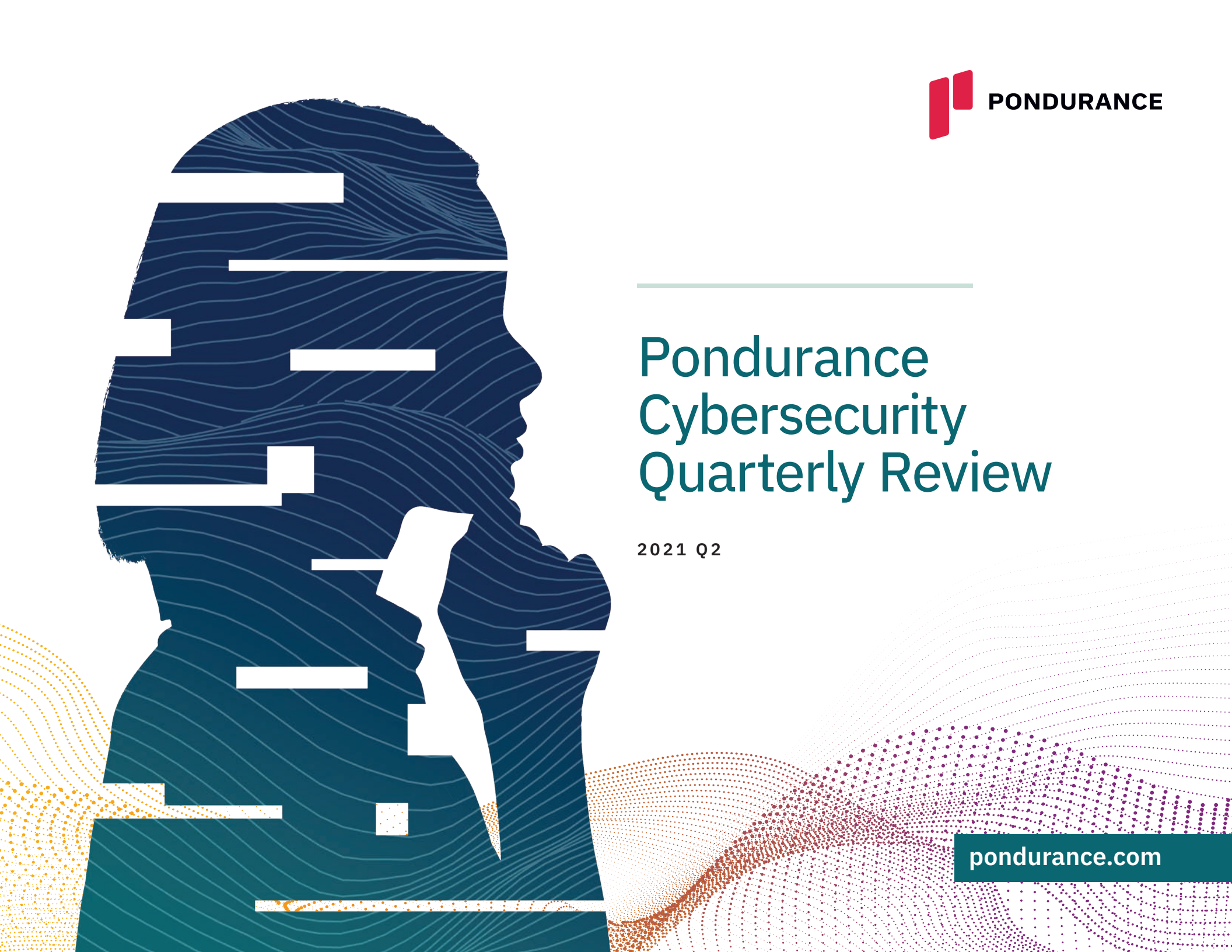


PONDURANCE

Pondurance Cybersecurity Quarterly Review

2021 Q2

pondurance.com

Table of Contents

Attackers Are Increasing Their Focus on the Manufacturing Industry 3

Bad Actors Are Getting Smarter and More Creative 4

RaaS, DarkSide, and the Colonial Pipeline 5

Phishing Attacks Continue To Be the Top Attack Vector Seen by Our Analysts..... 6

Featured Article: Keeping Up With Cyberattacks Against the Manufacturing Industry 7

How Pondurance Can Help 10

About Pondurance 11

The Pondurance Cybersecurity Quarterly Review: 2021 Q2 shares data collected by Pondurance teams, providing a glimpse into the growing attack surface and threats that organizations face in today's threat landscape.

Attackers Are Increasing Focus on the Manufacturing Industry

Manufacturing cyberattacks are on the rise, and while the recent attack on the Colonial Pipeline made headlines, the company wasn't the only one battling attackers. Our Pondurance Managed Detection and Response (MDR) team recorded a **10% increase year over year in cyber alerts being mitigated for manufacturing customers in Q2.** The manufacturing industry is a preferred target, as supply chains continue to be the vulnerable entry point.

"The threat of severe ransomware attacks poses a clear and present danger to your organization, to your company, your customers, your shareholders, and your long-term success. Pay attention now. Invest the resources now." *— Lisa Monaco, U.S. Deputy Attorney General*[1]

"Deterrence is the unique purview of government. Government must do what only the government can do — deter malfeasance in cyberspace, especially by nation-state adversaries, by using our tools of national power against those who are harming us. The private sector cannot defend itself alone against nation-state adversaries and criminals who are agile, persistent, and creative and who operate with no fear of reprisal." *— Niloofar Razi Howe, Chair of the Board, Pondurance*[2]

Read more from Niloo in her blog: Industry Veteran Niloofar Razi Howe Discusses Cybersecurity Trends That Will Shape 2021 and Beyond.

10%

increase year over year in cyber alerts being mitigated for manufacturing customers in Q2

PONDURANCE

Bad Actors Are Getting Smarter and More Creative

Cyberattacks are carried out by humans, and they are getting more innovative and more creative.

Recently, the professional networking site LinkedIn had the data of over 700 million users offered for sale. Although passwords were not stolen, the data did contain email addresses, full names, phone numbers, physical addresses, and details on other social media accounts. This data could be used to craft creative phishing emails and innovative social engineering attacks and these types of attacks can have devastating results.

DarkSide is said to have attacked the Colonial Pipeline via a single compromised password.

While businesses are responsible for developing cybersecurity programs to detect and contain threats launched by ransomware gangs and state-sponsored attackers, it is also the responsibility of individuals to be aware of these types of attacks, attend social engineering awareness training and review basic tips to keep themselves safe.

> “Humans make thousands of decisions a day and read hundreds of emails. Phishing attacks bet on one wrong click. The numbers are on their side.”
>
> - Lyndon Brown
> **Chief Strategy Officer, Pondurance**

PONDURANCE

RaaS, DarkSide, and the Colonial Pipeline

The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI confirmed that DarkSide is responsible for the Colonial Pipeline attack. As of May 12, the cyberattack caused the Colonial Pipeline to shut down, causing gas shortages affecting 45% of the fuel consumed on the East Coast. Governors in North Carolina, Georgia, and Virginia declared states of emergency and took steps to relax fuel transport rules to ease the price increases at gas stations.

DarkSide apologized for this attack, stating on its website that it does not "participate in geopolitics'' and should not be tied "with a defined government and [to] look for other motives." However, the damage from the ransomware-as-a-service (RaaS) organization is already done.

In a positive turn of events, the Department of Justice seized $2.3 million in cryptocurrency (63.7 bitcoins) paid to DarkSide.[3] The U.S. has the tools to make cyberattacks like the attack on the Colonial Pipeline less detrimental and costly by returning the ransoms paid.

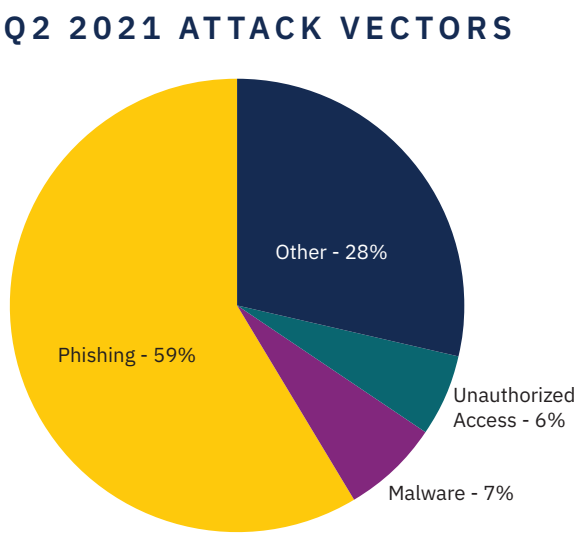
"There is no place beyond the reach of the FBI to conceal illicit funds that will prevent us from imposing risk and consequences upon malicious cyber actors," said FBI Deputy Director Paul Abbate.[1]

If you are in an emergency situation and need help with a cyberattack like ransomware, Gartner points out that "a key value proposition of MDR is performing most of the incident response process. Timely and accurate incident response takes time and skill, which many organizations just don't have, especially when multiple threats need to be addressed simultaneously."

Learn more about this RaaS organization and see screenshots from its webpage before it was taken down by the FBI and the majority of the ransom was seized.

Read More

Phishing attacks continue to be the top attack vector seen by our analysts



Phishing is the main cause of ransomware, accounting for

59%

of Pondurance MDR alerts in the second quarter of 2021.

Fraud attack glossary:

- **Ransomware-as-a-service (RaaS):** A subscription-based model that enables affiliates to use already developed ransomware tools to execute ransomware attacks. Learn more in our blog RaaS, DarkSide, and the Colonial Pipeline.
- **Social engineering:** A term used for a broad range of malicious activities accomplished through human interactions using psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- **Supply chain attack:** Seeks to infiltrate and disrupt the computer systems of a company's supply chain in order to harm that target company. The idea is that key suppliers or vendors of a company may be more vulnerable to attack than the primary target, making them weak links in the target's overall network.

FEATURED ARTICLE

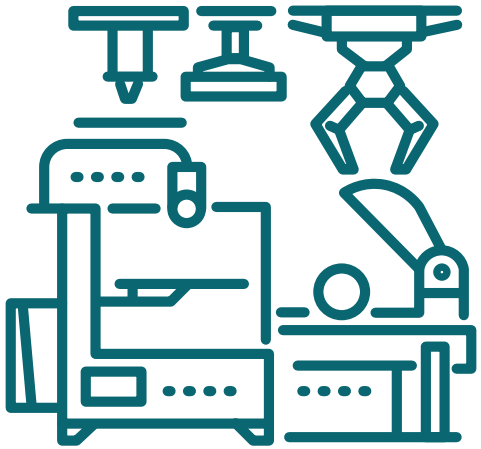
Keeping Up With Cyberattacks Against the Manufacturing Industry

The manufacturing industry leads the world in its adoption of cutting-edge technologies. As more manufacturers join the “Industrial Revolution 4.0,” they drive the demand for artificial intelligence, machine learning, and analytics to operate a myriad of evolving technology in a digital world. The growing demand for a connected environment opens up a variety of new cyber risks for manufacturers, where ransomware gangs and nation-state attackers have identified supply chains as preferred targets for a soft entry point into larger corporations and government networks.

PONDURANCE

Along with the financial and healthcare industries, the private sector has made significant strides to increase investment in cybersecurity tools, security services, and skilled cybersecurity talent. At the same time, manufacturing continues to struggle to keep up with the evolving threat landscape. Managing cyber risks within the manufacturing industry requires collaboration between the operational technology (OT) and information technology (IT) entities.

OT has been around far longer than IT departments within the manufacturing industry, and according to Gartner, OT is "hardware and software that detects or causes change through the direct monitoring and/or control of physical devices, processes and events in the enterprise."[4] OT "manages the shop floor," whereas IT is networking and business operations. The two have operated separately for quite some time. However, as the market expands, more manufacturers are rapidly adopting digital acceleration. OT and IT must work together to detect suspicious activity and protect its technology from bad actors.



The ransomware attacks on the Colonial Pipeline and the JBS meatpacking company demonstrate that attackers can negatively impact critical resources U.S. citizens rely on to survive. These manufacturers cannot afford operational disruption, and disabled manufacturing systems can impact assembly line management due to a cyberattack. In addition, the risk of losing intellectual property and patent records can affect business relationships.

Operational disruptions can significantly impact suppliers and create a chain reaction in supply chain penalties starting with contractual procurement. It can take 302 days to identify and contain a data breach for manufacturers.[5] As downstream clients rely on manufacturers, downtime affects more than financial losses; it negatively impacts the relationships between client and customer. It is critical to have 24/7 visibility and security analysts to detect anomalous activity before attackers disrupt operations.

Different manufacturers handle different types of data. For example, medical manufacturers working on the COVID-19 vaccine must protect patient information, medical trial data, intellectual property, and HIPAA-covered information. Medical manufacturers are considered HIPAA-covered entities

as “business associates” if they handle sensitive protected health information. As a result, these manufacturers must have the recommended security requirements to ensure that data is protected. Otherwise, they can face fines and penalties in the event of a cyberattack or data breach.

Supply chain attacks are rising at an alarming rate. On average, a manufacturing data breach can cost upward of $4.9 million per data breach.[5] The cost of operational disruption, legal, penalties, recovery, and more all contribute to these rising costs. As manufacturers continue to pay ransoms, the costs are going to continue to rise per attack.

The increased attacks on manufacturing and supply chains have caught the attention of the White House. President Joe Biden released a cybersecurity executive order aimed at developing clear and actionable cybersecurity standards to defend business and remediate cyber threats. Under Biden’s leadership, the Federal Government will be working with partners around the globe to disrupt and deter attacks by “disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds,” according to Biden’s memo.

Manufacturers that work in partnership with vendors to improve logistics, technology, and operations need to understand the risks associated with digital acceleration. Understanding your risks is a critical factor in managing vulnerabilities. In addition, implementing a cybersecurity strategy that provides OT and IT with constant visibility into network, endpoint, logs, and cloud infrastructure to detect threats effectively is critical.

People, processes, and technology continue to be vital resources when developing a comprehensive cyberdefense program. Having a 24/7 security operations center (SOC) is critical to detect and mitigate threats in real time. However, cybersecurity talent is expensive to hire and retain. As a result, manufacturers are turning to MDR services to act as an extension of their security teams. This provides them the full range of visibility they need to triage alerts, mitigate threats, and manage vulnerabilities that lead to operational disruptions.

THE ROOT CAUSE OF A MANUFACTURING DATA BREACH:

54%
Malicious Attacks

23%
System Glitch

23%
Human Error[5]

How Pondurance Can Help

Our mission is to ensure that every organization is able to detect and respond to cyberthreats — regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease risk to your mission.

CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based SOC services powered by analysts, threat hunters, and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber-risk reduction. By integrating 360-degree visibility across log, endpoint, and network data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyberthreats.

Pondurance MDR is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyberthreats. Human attackers must be confronted by human defenders.

INCIDENT RESPONSE

When every minute counts, organizations need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response services with an experienced team capable of guiding you and your organization every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and helping to quickly restore your normal operations.

SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from penetration testing to red team exercises, along with compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyberattacks.

Copyright © 2021 Pondurance

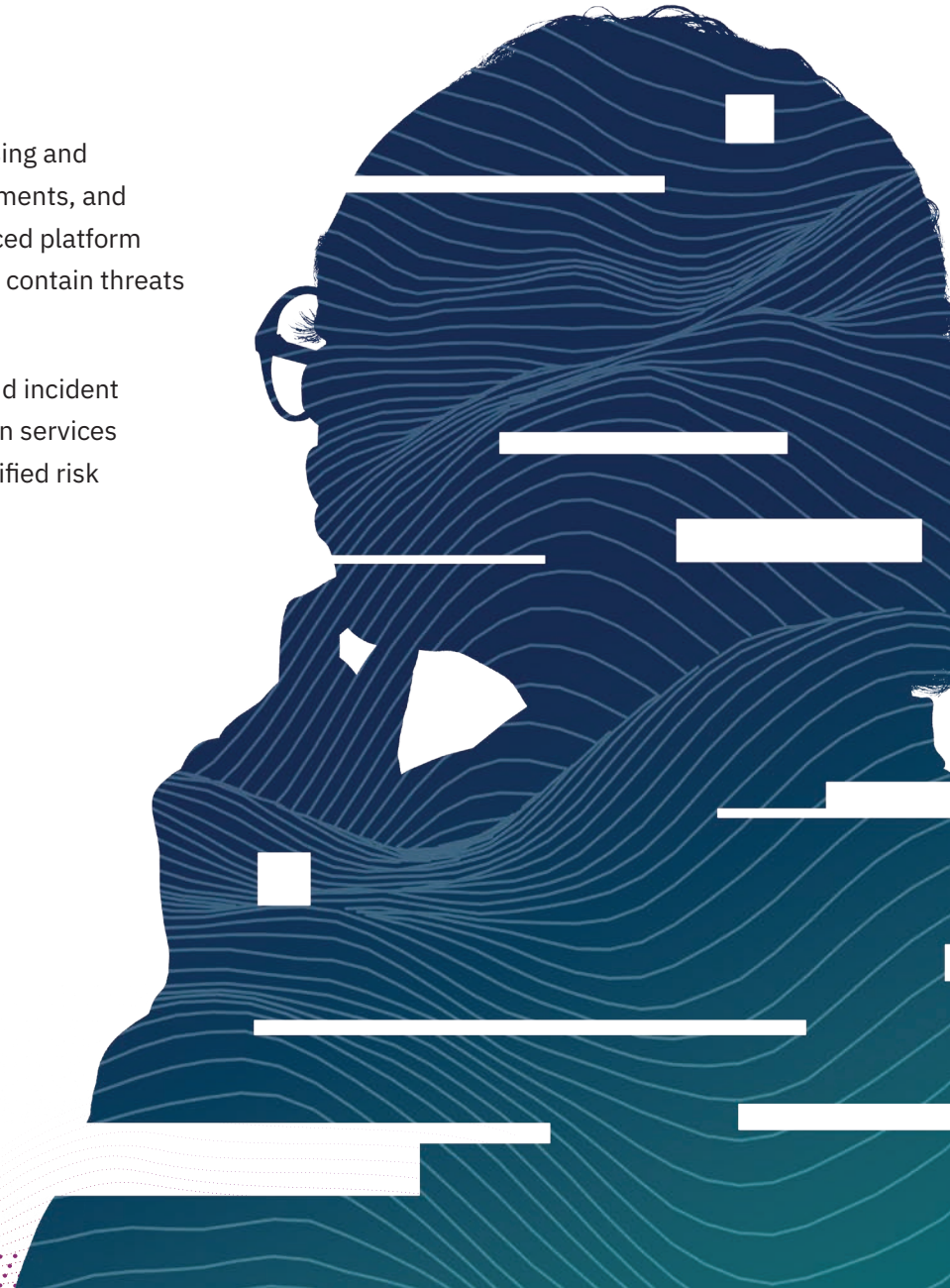
PONDURANCE

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.



Sources:
1. DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline, The United States Department of Justice, June 7, 2021.
2. Testimony to the Defense Subcommittee of the House Appropriations Committee, Pondurance, March 23, 2021.
3. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, The United States Department of Justice, June 7, 2021.
4. Operational Technology (OT), Gartner, 2021.
5. Cost of a Data Breach Report 2020, IBM, 2020.

pondurance.com

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204