

Cybersecurity Predictions for 2021:

INSIGHTS & TRENDS



Introduction

2021 is sure to see more bad actors executing more cyberattacks than ever before. Gartner estimates the global impact of such incidents to reach a staggering \$6 trillion. An effective cyberdefense is critical now more than ever. Protocols and technologies that worked five years ago will not cover the range and sophistication of threats facing all industries today. In this eBook, we outline our top five cybersecurity predictions for 2021, including steps you can take to prepare for the year to come.

1 PREDICTION

The MDR industry will continue to grow as organizations are challenged to keep up with the growing number of cyberattacks executed in 2021.

By 2025,
50%
of organizations will be using
MDR services.

— Gartner Market Guide

THE DETAILS

With the increase in cyberthreats, we see more organizations enlisting managed detection and response (MDR) service providers as their primary security team or an extension of their internal security operations. MDRs provide a broad range of monitoring over endpoints, networks, cloud services, operational technology, and traditional log data.

MDRs often include human analysts to power a 24/7 security operations center (SOC). Organizations will look for a partner that can truly detect an incident, contain the incident, eliminate the source, and help them return to operations. They will want the full closed-loop service in order to reduce risk, accelerate response, and manage costs. With more cyberattacks occurring year over year, we see the need for increased partnership in security operations as a must for organizations in 2021.

HOW TO PREPARE

If you are lacking a security team or could use an extension to your security team, an MDR could be the answer for your organization.

Start by assessing your organization's needs. Do you have technology but need more specialized personnel? Do you need 24/7 coverage? Would your team be able to resolve a bump in the night?

Research MDR providers and ask your potential MDR partners for a total cost of ownership evaluation to see how they might fit into your budget. The marketplace is evolving, so look for a partner that has innovation and evolution as part of their culture to be sure they can provide the flexibility you need.

If you already have an MDR provider, review the agreed scope and make sure that the support you are receiving is what you need for 2021.

2 PREDICTION

Robust cyberattacks will increase due to insufficient protection of the domain controller (DC), regardless of other security controls implemented.

THE DETAILS

The domain controller (DC) can be a substantial point of weakness if not protected. Historically, the majority of enterprise-impacting breaches (such as ransomware) occurred where an attacker gained unauthorized access with administration rights to the DC. We predict that attacks against the DC will continue to facilitate large-scale incidents among bad actors in 2021, and they will more often seek out cloud-based domain controller equivalents.

When the DC is compromised, attackers use it as a catalyst to systematically detonate attacks like a ransomware payload to each connecting system. A common habit that we see from attackers is the quick impact they can have when accessing Microsoft Windows Active Directory. Once they have domain administrative access, they can often gain access to everything in the organization's environment and consequently can get access to whatever they please.

HOW TO PREPARE

We recommend having a defense-in-depth strategy and plan in place. The most common techniques for accessing the domain controller and basic hygiene best practices for prevention can be found in our [The Domain Controller...an Achilles Heel](#) whitepaper.



Compromised domain controllers are the common denominator in

99%

of ransomware attacks.

3 PREDICTION

Cyberattacks will become a greater risk for healthcare organizations.



THE DETAILS

Over the past year, we have seen both direct and indirect cyberattacks pose an even greater risk to healthcare organizations. With the rapid pace of digital transformation in the healthcare industry, opportunities are increasing for cyberattacks. We predict we will continue to see attempts to cause operational issues at hospitals and to impact the safety and effectiveness of medical devices.

Recently, the [Wall Street Journal](#) reported that the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Interpol, and cybersecurity researchers have all warned of actors targeting the supply chain for coronavirus vaccine shots. “Covid-19 vaccines are ‘Liquid Gold’ to organized crime,” Interpol says. The CISA warned that actors are targeting specific organizations working on the vaccine such as Pfizer and Moderna.

There have already been attacks on the suppliers, and we expect to see more attacks on the supply chain for the vaccine, especially involving cold storage, as many facilities are controlled by Internet of Things (IoT) or smart devices that could be hacked.

HOW TO PREPARE

As healthcare organizations seek to reduce their cyber-risks, we predict that many will expand their operations to include incident response (IR) specialists. Some will partner with cybersecurity experts that have specific experience supporting healthcare organizations and strong [digital forensics incident response \(DFIR\)](#) capabilities. Threats and vulnerabilities cannot be completely eliminated in any industry, and in the healthcare industry, the speed and accuracy of the DFIR team is critical as timing could affect patient care. Having an extended security team with [MDR services](#) and proven DFIR experience allows healthcare organizations to focus on what matters most: patient care.

4 PREDICTION

Data regulation penalties are tightening, which means protocol adjustments will be needed to achieve compliance.

THE DETAILS

Regulatory requirements and penalties around data privacy and security will continue to evolve and tighten over the next year. The value of data is increasing, which is leading lawmakers to tighten regulations including the California Consumer Protection Act effective Jan. 1, 2021, and the IoT Cybersecurity Improvement Act.

The updates to the [California Consumer Protection Act](#) effective Jan. 1, 2021, expand the department's authority to regulate financial products and services that were not previously regulated. Organizations will need to adjust protocols to stay compliant with these new updates.

The newly instated IoT Cybersecurity Improvement Act tightens security standards and guidance for federal procurement of IoT devices. These devices could range from heating and cooling systems to elevators, medical devices, and even vehicles. While these standards only apply to the federal government, we expect them to influence state and private sector practices as well.

HOW TO PREPARE

Compliance risk can result in significant fines if not addressed; however, protocols should not be instituted to simply check a compliance box. We recommend speaking to a compliance consultant to see how the consultant can help ensure that your cybersecurity program is compliant given recent updates. The consultant can help you prove and improve your security.

In the interim, be sure that your security program is established on one of the many available frameworks and that the control techniques are supported by your risk assessment. By developing your program to ensure true security risk is addressed, compliance with any addressable or prescriptive mandates becomes a simple alignment exercise.

General data protection regulation
fines in 2019 reached
\$43 million.



5 PREDICTION

Implementing more cyber hygiene basics will be required to help manage cyber insurance premiums.



The FBI cites
\$3.5 billion
 in cybercrime losses
 reported in 2019.

THE DETAILS

We do not see the market for cyber liability insurance going away. It is important for organizations to understand the details of what their policies cover and do not cover.

The NotPetya malware attack in the summer of 2017 began in Ukraine and caused a total of more than \$10 billion in damages. The pharmaceutical company Merck was hit badly, and most of its insurers and reinsurers denied coverage under the company's policy. Even though NotPetya caused \$1.75 billion worth of damage and Merck was covered for that amount and for risks including destruction to computer data as well as coding and software, Merck's policies specifically excluded acts of war. Since NotPetya was an organized attack from a nation-state, the insurance companies considered the attacks an act of war. The lesson learned from that is to fully understand your coverage and ensure that it covers events such as these.

Bad actors are getting smarter with ransomware demands because they know cyber insurance will pay. We have even seen efforts of reconnaissance to see the amount of insurance a business holds. This may provide them with knowledge in terms of deductibles and maximum coverages that lend more precision in their demand and an increased likelihood that demand will be met and paid. Bad actors are also catching on that organizations are better positioned to recover their data from backups and avoid paying a ransom. As a result, there are more acts of extortion where the attackers will exfiltrate data and threaten to expose it if they are not paid.

HOW TO PREPARE

We think the underwriting process will become more stringent in 2021 to ensure that organizations are duly considering their true risk including protection of their domain controllers. To get an affordable premium, we recommend that companies add cyber hygiene basics like multifactor authentication, dynamic defensive measures (such as MDR), endpoint detection and response across all assets, and encryption of all mobile laptop hard drives. It is equally prudent to establish a vulnerability management program to assure systems are updated and configured appropriately over time. Learn more about recommended foundational hygiene to protect your environment in our whitepaper [The Domain Controller...an Achilles Heel](#).

Overall, cyber insurance is one of the most important decisions an organization can make. If you want to learn more, read our whitepaper [To Cover or Not to Cover: How Digital Forensics Answers the Question and Shapes the Future of Cyber Insurance](#).

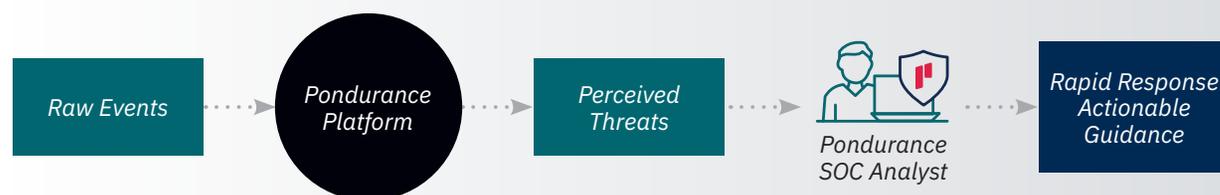
How Pondurance Can Help

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.

MDR

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 DFIR 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 IR and business continuity planning to put you in the best position to defend against and respond to cyberattacks.

Conclusion

Cybersecurity technology has improved, but bad actors continue to evolve. The requirements for effective cyberdefense have grown beyond traditional data and system security solutions.

While a SIEM or endpoint security product may recognize the first sign of trouble, systems alone can't anticipate the actions of highly motivated human opponents.

At Pondurance, our MDR services provide the most complete solution in the market. We pair the latest technology with expert analysts and threat hunters to provide the broadest detection and threat hunting capabilities to detect and deter bad actors. Should your organization experience a cyber incident, we provide a complete closed-loop rapid response team of experts to contain the incident, determine exposures, and quickly restore normal operations.

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, DFIR 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.

AUTHOR

Ron Pelletier

Founder and Chief Customer Officer
Pondurance

Ron Pelletier is the original Founder of Pondurance, having started the company from his basement in 2008. Ron has over 25 years of cybersecurity advisory experience. He started his career as an officer in the U.S. Army, followed by nine years with Big Four firm EY. As a strong consensus builder and customer advocate, Ron is focused on evangelizing the Pondurance brand as well as customer success.

pondurance.com

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

