The 2021 State of Pharmaceuticals and Cybersecurity Report
# TABLE OF CONTENTS

Executive Summary ................................................. 3

An Industry in Flux Creates an Easy Target for Cyber Criminals .... 4

Study Methodology .................................................. 5


Business Concerns: Access to Training and the Pace of Change Are the Biggest Barriers ............................. 8

Conclusion: Growing Threats Must Be Met With a Modern Approach to Cybersecurity ..................... 10

References .......................................................... 10
Executive Summary

The 2021 State of Pharmaceuticals and Cybersecurity Report from Fortinet finds an industry rapidly losing the race to secure and protect intellectual property, business continuity, and mission-critical data. 98% of pharmaceutical firms surveyed experienced at least one intrusion. And around half of the businesses surveyed experienced between three and five intrusions in the last year.

The most common types of intrusions were:

- **40%** Mobile security breaches
- **37%** Phishing
- **36%** Hacked removable storage device/media
- **35%** Hackers including SQL, zero-day, man-in-the-middle

40% of businesses experienced outages that affected productivity, safety, compliance, revenue, or brand image.

28% of businesses lost business-critical data or IP.

When asked what’s having the greatest impact on cybersecurity posture, pharmaceutical leaders say it is:

- **45%** IT/OT convergence
- **43%** Network complexity
- **38%** Supply chain complexity
- **36%** Mergers and acquisitions
- **35%** Aging OT environments
- **35%** Growing number of IoT devices
- **34%** Insider threats
- **34%** Digital transformation

Some organizations are looking to a trusted partner to improve their cybersecurity strategies. These are the four most important performance capabilities respondents look for in a security provider:

- **30%** Scalability
- **25%** Innovation
- **24%** Product performance
- **21%** Availability/uptime
An Industry in Flux Creates an Easy Target for Cyber Criminals

The pharmaceutical industry is flanked on all sides by change.

On one hand, pharmaceutical organizations are becoming increasingly customer-focused and data-driven to stay ahead of the competition. And many companies are investing in new or improved solutions to boost efficiency, such as:

- Using digital twins to reduce risks supporting asset performance management (APM)
- Increasing overall equipment effectiveness (OEE) to drive increased manufacturing yield
- Shifting from calendar-based to condition-based maintenance to minimize lost production associated with service outages
- Increasing asset availability and reliability

On the other hand, cyber criminals are becoming increasingly sophisticated, well-armed, and ready to take advantage of any gaps they find in enterprise IT estates.

It doesn’t help that, when compared to other industries, pharmaceutical organizations operate in a complex partner ecosystem of universities and research centers, labs, manufacturing facilities, and hospitals. This demands a high degree of security across all connections to protect highly coveted intellectual property and maintain the privacy of patients.

Connected technologies expand the cyber-threat surface

We’re also seeing transformative changes in pharmaceutical organizations and their use of connected digital technologies: Many are now integrating information technology (IT) and operational technology (OT) systems, and using cloud solutions for data processing and global ecosystem collaboration.

But in many cases, these changes are creating an expanded cyberattack surface. As OT systems that were previously siloed from wider networks are now using the same networks as traditional IT systems, these OT systems are now vulnerable to typical IT system attacks. Worse still, the attack surface for an OT system can include Industrial-Internet-of-Things (IIoT) devices, which control critical systems that can have potentially dire health and safety consequences if they’re breached.

At the same time, some organizations are focusing on operational transformations at the expense of cybersecurity, leaving many without the end-to-end, scalable security measures they need to protect their systems and data.

At most pharmaceutical manufacturing organizations, siloed systems for IT, OT, and physical security are the default—and this does not help matters. Integrating just the IT security architecture between the data center, multiple clouds, and the edge is hard enough. But in an age when adversaries can coordinate cyber and physical attacks simultaneously, integrating all elements of security with centralized visibility may be the only viable means of protection.

It all adds up to create an industry where OT systems are increasingly barraged with both recycled IT-based attacks and purpose-built OT exploits, as attacks on the pharmaceutical manufacturing sector’s critical infrastructure can lead to financial loss, compromised trials, contaminated drugs, delivery delays, a risk to brand reputation, and sometimes even loss of life or threats to national security.

To truly understand the state of the industry and the cybersecurity challenges facing pharmaceutical firms, Fortinet surveyed VPs and directors of manufacturing at pharmaceutical companies as part of “The 2021 State of Pharmaceuticals and Cybersecurity Report.” The report explores the most common cyberattacks pharmaceutical manufacturers are experiencing and what features organizations look for in cybersecurity solutions.
Study Methodology

This 2021 State of Pharmaceuticals and Cybersecurity Report is based on a survey conducted April 15–19, 2021. The objectives were to help OT professionals in the pharmaceutical industry better understand:

- How the position fits in the organization
- How security features are utilized
- How information is tracked and reported
- Influences and success factors

The approach was a panel sample used to obtain 100 completes with the following respondent type:

- Come from a business in pharmaceuticals, medical devices, or life sciences with 501 or more employees
- Supports or manages OT security and networking as primary responsibility
- Involved in cybersecurity and networking purchase decisions
- Based in the United States


As noted, IT/OT convergence and network complexity have the biggest impact on enhancing or changing cybersecurity postures. With internal security training and education, security operations centers, network operations centers, and technical operations centers as the most common security features in place, the goals of pharmaceutical security are to reduce risk (23% say it’s the most important strategic capability), expand reach (29%), achieve flexibility (25%), and enhance aggregate quality (23%).

Insight 1: All operational functions are rated fairly similarly.

When asked to rank the following operational functions in order of importance when evaluating and selecting a security solution, effectiveness/efficacy was most important, while agility and flexibility was least important. However, among the options, there was little difference in rank of importance.

Takeaway: Survey respondents show a desire for all operational functions to be present in their ideal cybersecurity tools. Often, a patchwork, point solution approach will leave gaps that undermine this desire to have it all, so pharmaceutical organizations would be best off looking for an end-to-end platform—one that offers cross-vendor interoperability and open architecture to deliver a futureproof security response.

Figure 1: Operational function importance ranking when considering security solutions.
Insight 2: Productivity capabilities have roughly equal importance, but those with “fewer challenges/roadblocks” slightly edge out the others.

Saving time and having fewer challenges and roadblocks were both ranked at 21%, while having transparency across the security solution was a strong second choice. The other options of productivity capabilities were tightly close behind.

**Takeaway:** Efficiency is a must-have for a security solution. Pharmaceutical firms would do well to look for solutions that include automated operations and artificial intelligence. These features can save time and resources across the business, while protecting the application layer with in-line, artificial intelligence (AI)-powered threat intelligence.

![Figure 2: Productivity capability importance ranking when considering security solutions.](image)

Insight 3: More than half of respondents consider reputation and stability a top 3 priority for solution vendors.

When it comes to solutions that keep their enterprise safe, respondents show a clear preference for vendors with a strong reputation and a stable business—with these two elements topping the list when we asked respondents about how they evaluate vendor relationships.

**Takeaway:** Cultural fit and responsiveness are equally important when selecting a security vendor, but a reputable, stable, committed company will be the most trusted to provide a comprehensive solution. Pharmaceutical manufacturers assessing the market would do well to carefully assess security providers and understand how many deployments they’ve made, patents they hold, integrations they have with other solutions, and similar measures that demonstrate a stable product and a strong market reputation.

![Figure 3: Vendor relationship factor importance ranking when considering security solutions.](image)
Insight 4: Aggregate quality and flexibility are less important than risk reduction and reach when it comes to strategic capabilities.

29% of respondents consider reach in strategic capabilities to be their top priority when selecting a vendor. And 25% feel the same about flexibility in their solution of choice.

Takeaway: To find the reach and flexibility pharmaceutical organizations are looking for, it's vital to find a provider that offers integration with core systems and provides comprehensive security across all systems in the business, from research, prototyping, and approval to manufacturing, distribution, and treatment of patients. To satisfy the need for risk reduction, it's also important to find a security partner with proven experience supporting pharmaceutical manufacturers, and organizations in other highly regulated industries.

![Figure 4: Strategic capability importance ranking when considering security solutions.](image)

Insight 5: Monitoring, compliance, and control system protocol protection top the list of important security solution features.

Managing and monitoring security compliance was the most important security solution feature for 19% of respondents. After that, security analysis, monitoring, and assessment tools was the next feature most commonly ranked as important by survey respondents, which shows that pharmaceutical leaders are invested in proactive management and thinking strategically about future solutions.

Takeaway: While some features are more important to respondents than others, the spread of answers shows that organizations in the pharmaceutical industry should consider choosing a single security platform that can unite data across the enterprise to increase speed of response, reduce the burden on IT, and enable effective C-suite reporting. If security tools are spread across multiple platforms, it could fragment the data needed to ensure proper monitoring and reporting, while also adding additional IT complexity and administrative burden.

![Figure 5: Most important security solutions features (ranking).](image)
Business Concerns: Access to Training and the Pace of Change Are the Biggest Barriers

Summary

Respondents agree that the most common challenges to being a successful cybersecurity professional are:

- Ability to keep pace with industry changes
- Regulatory changes
- Availability and access to training

Respondents were asked to list the top three ways cybersecurity solutions negatively impact OT professional success. Creating business concerns and complexity are seen as having the greatest impact.

43% of respondents stated that implementing security solutions create business concerns, they create more complexity (42%), and they require challenging adoption of security standards (37%). This shows how important it is for those involved in cybersecurity to reframe the conversation within their organizations, and help security be seen as a growth enabler instead of a cost center.

What intrusions are organizations seeing—and what are the impacts of a cyber breach?

From drug and device manufacturers to biotech companies, all parts of the pharmaceutical industry retain valuable proprietary data. Secret formulas for patented drugs, protected patient health and customer information, and scientific research and advancements are all prime fodder for cyberattacks if unsecured.
But it’s not just external attacks that pose a threat to organizations. 53% of pharmaceutical IP thefts and related breaches are carried out by bad actors with inside access, according to the United Kingdom Office of Cyber Security and Information Assurance. And according to Health IT Media, 25% of those insider attacks between 2018 and 2020 were deemed malicious, as opposed to being caused by human error or carelessness. Research also shows that these insider threats cost the healthcare and pharmaceutical industries $10.81 million per year.

Damage from insider sources can be hard to detect and deter because the attacks represent a wide range of behaviors and motives. It could be a disgruntled employee wanting to disrupt operations, a staff member hoping to sell valuable data, or even a well-intentioned co-worker accidentally sidestepping a security policy.

Results of the survey showed that most organizations have experienced at least one intrusion in the past year, with around half experiencing three to five. And mobile security breaches are the most common type of intrusion.

**Takeaway:** There has to be complete visibility and coordination across the network to continuously monitor third-party vendors’ cybersecurity. A secure software-defined wide-area networking (SD-WAN) solution addresses these issues by integrating networking and security capabilities across the WAN edge, access layer, and endpoints. In this way, Secure SD-WAN and SD-Branch solutions can provide advanced visibility, security, and protection for today’s rapidly scaling and evolving pharmaceutical networks.

Intrusions have an equal impact on all areas, but business-critical data/IP is the least impacted.

The pharmaceutical leaders who participated in the survey report that their organizations have been largely unsuccessful at preventing cyber criminals from intruding in their systems. The most egregious impact on the organization were breaches that caused operational outages that affected productivity (45%), followed closely by operational outages that put physical safety at risk (43%). These alarming impacts were then followed by brand reputation damage (41%) and outages that impacted revenue.

**Takeaway:** Cyberattacks targeting pharmaceutical organizations can endanger lives. This alone is reason enough to proactively prevent these attacks from happening in the first place.
Companies reacted in different ways to accommodate work from home, but adapting existing technology was the most common change.

Historically, digital innovation efforts and the fast growth of the Internet of Medical Things (IoMT) have opened up vulnerabilities in pharmaceutical companies. Over the years, cloud migrations, connected medicine and telehealth, remote employees, and pop-up vaccination clinics have only increased the number of attack vectors across pharmaceutical manufacturing, leading to a spike in ransomware and phishing attempts.

**Takeaway:** Only 30% of organizations say they needed to adapt their existing technology to support remote work. Interestingly, only about one in ten will continue what they have implemented. Most companies will go back to former processes and/or continue to seek new ways to streamline processes and reduce cost after the pandemic. While this shows a steady return to "normal" operating conditions for the industry, the idea of rolling back systems is concerning, as cyberattacks are far more frequent—and more damaging—than they’ve ever been before. Pharmaceutical manufacturers would be wise to also look forward and consider what their IT and security teams can learn from operations throughout the pandemic.

**Conclusion:** Growing Threats Must Be Met With a Modern Approach to Cybersecurity

The pharmaceutical industry continues to face many cybersecurity challenges and vulnerabilities, from network complexity and compliance to fortifying against and responding to ransomware and phishing attacks. As pharmaceutical networks increasingly depend on digital innovations to continue the important work of enhancing and saving human lives, cybersecurity issues will unfortunately also increase.

To combat the rising complexity of the pharmaceutical ecosystem and the increasing scale of cyberattacks, pharmaceutical companies need a cybersecurity solution that can protect data across connected IT and OT environments—without slowing down the flow of vital information.

Fortinet is the ideal security partner to provide this type of end-to-end security platform. Fortinet supports pharmaceutical organizations of all sizes, allowing them to grow by securing the flow of data across connected IT and OT environments and within complex, evolving pharmaceutical ecosystems. At the same time, pharmaceutical businesses can remain secure throughout their increasingly digital, customer-led and data-driven journeys.

With a broad, integrated security platform, you can enable greater protection and deliver actionable security across IT and OT environments. With our adaptive and business-wide Security Fabric, Fortinet can support requirements for an ecosystem-wide approach to security, compliance, and continuous validation with a broad, integrated, and automated security platform.

To learn more about Fortinet, and how it can help you better protect your growing manufacturing ecosystem, visit https://www.fortinet.com/solutions/industries/pharma.

**References**
