WHITE PAPER

Cybersecurity for Pharmaceutical Enterprises:

Understanding and Solving for Evolving Threats

Introduction

Pharmaceutical companies have long been targets of cyberattacks for their valuable intellectual property (IP) and the high – and growing – costs associated with disruption or downtime. From financial to reputational, most pharmaceutical companies agree that the losses from a cyber attack are staggering. Consequences can range from litigation to stolen IP, repeating clinical trials, and lost revenue. Many of the largest pharmaceutical companies have been the targets of attackers seeking vaccine-related IP since 2020, but it's not only the big players that are under attack.

Life sciences and pharmaceutical companies large and small are being targeted, as work-from-home endpoints, migration from on-premises and legacy systems to cloud and hybrid cloud solutions, and the increased exchange of data through patient and healthcare provider portals have all vastly increased their attack surface.

Now the question is not *if* there will be an attack, but *when* — and how soon it can be detected to prevent further damage to your organization's value chain, from research, prototyping, and approval to manufacturing, distribution, and patient treatment. Trust in your brand and operational efficiency is on the line, and attackers are relentless, attempting to breach pharmaceutical systems billions of times a day.

To help ensure that your cybersecurity strategy is prepared to protect your critical IP and protected health information (PHI), this paper lays out:

- Where most pharmaceutical enterprises are vulnerable and why
- What happens if there is a breach
- How to prioritize cybersecurity investments to protect vital assets

Where are your cybersecurity vulnerabilities?

Digital footprint

The larger your digital footprint — and the faster it's growing — the greater your likelihood of a cyberattack. All the following data create targets, especially as they are available across a larger number of assets, devices, and vendors:

- IP, including drug patents and technologies, trademarks, copyright, and trade secrets
- Research data, including testing and clinical trial data
- PHI
- Drug cost and pricing information
- Manufacturing contract terms
- Executive/employee salaries and personal information
- Internal correspondence

Operations

The digitization of operational practices also puts life sciences and healthcare companies at risk. Relationships with third parties and suppliers expand opportunities to breach your enterprise network and systems.

Internet of Things (IoT) devices, like auto-injectors or smart pills, open up more potential attack vectors. In addition, legacy manufacturing systems, such as older dryers or granulators, that require an outdated control system or an operating system that is no longer supported, are not built to handle the modern scale of data or security threats.

Additionally, as in all industries, remote work has created additional threats, such as employees sending sensitive patient data across insecure connections or working on unmanaged personal devices.

> **"While there is no disputing the many benefits of remote working, it does add a layer of complexity that creates security challenges."**
>
> *— National Library of Medicine, National Center for Biotechnology Information remote access report*

Take, for example, what happened to one of the world's largest pharmaceutical companies. It was reported that nation-state hackers used a spear-phishing campaign to target employees working on the COVID-19 vaccine. Posing as job recruiters, the hackers approached staff with fake job offers to gain access to victims' computers and IP.

Network landscape

The IT profile in a pharmaceutical enterprise is complex. The way data and applications are architected creates potential for security risks. On-premises solutions, both modern applications and legacy systems (such as pharmaceutical management information systems or enterprise resource management); cloud and hybrid cloud environments; and the use of multiple IT service vendors expand the potential attack surface, and increase the complexity of effectively securing your organization's network.

Despite its security pitfalls, distributing storage and applications across vendors and platforms has its benefits. The strategy of using multiple cloud providers reduces potential downtime and service disruptions, compared with using a single provider. But with more providers and systems to manage, monitor, and defend, maintaining visibility into IT infrastructure becomes increasingly difficult.

Cloud platforms offer security capabilities, including continuous infrastructure and application security. But protecting your network and all its applications should go beyond the native tools offered by service providers and, sometimes, even beyond what the internal security team can manage. Security across systems requires continuously configuring rules to cover on-premises systems and cloud-hosted solutions, which is resource-intensive work in terms of the time, expertise, and talent required, and opens up opportunities for errors.

It's important to find flexible distributed denial-of-service (DDoS) attack protection across hybrid architectures — especially since responsibility for security within public cloud environments can be inconsistent from provider to provider. Making a false assumption about who's responsible can leave you exposed to huge risk.

In general, the customer is ultimately responsible for application security in the public cloud. That responsibility includes DDoS protection, but also extends to higher-level security controls like protecting against data exfiltration, hacking, and bots.

Results of a breach

Breaches threaten the significant investments pharmaceutical companies make in developing, testing, and marketing their products.

- IP theft — losses up to $363 million
- Regulatory fines — up to 4% global turnover
- Reputational damage — 20% loss of valuation, 5% drop in share price
- Operational disruption — losses of approximately $5 million per breach
- Compromised clinical trial data — drugs can be worth more than $1 billion a year and any delays can have huge revenue impact
- Supply chain issues — leading to less favorable logistics contracts due to threat of disruption or potential product shortages

Understanding the nature of an attack

There are people, processes, and technologies at each stage of the drug development and pharmaceutical value chain that create vulnerabilities for pharmaceutical organizations and require protection.

1. R&D: Early discovery

Industrial robots used in the high-throughput screening of compounds at the discovery phase are vulnerable because of outdated or proprietary programming languages. A breach or attack on the database or network hosting one of these robots could disrupt drug development, or enable the bad actor to steal proprietary information.

2. R&D: Clinical trials/FDA approval

Cyberattacks can delay urgent research. In October 2020, a company supporting a biopharmaceutical partner suffered a ransomware attack that locked researchers out of COVID-19 vaccine trials.

3. Manufacturing and distribution

Hacking can threaten the manufacturing of lifesaving drugs. The NotPetya attack on a major pharmaceutical company halted manufacturing for a vaccine and delayed distribution of their potentially lifesaving drug.

4. Sales and marketing

Hackers can disrupt operations, such as when malware took the public website and patient portal offline at a nonprofit health system in early 2021.

What's there to lose?

Unidentified patient information — This can stop or delay research, potentially lose business and revenue, and damage reputation

PHI — PHI has a longer shelf life than information like credit card numbers, and sells for a much higher price on the black market

IP, including early-stage drug combinations and patents, and proprietary processes and machinery — IP can represent up to 80% of a company's value and its can result in losing customers, market advantage, revenue, or reputation

Operations — Stopping or slowing down operations (such as through a DDoS attack or ransomware) is costly in terms of mitigation costs and potential lost business and revenue

FDA filing documentation — Stopping or delaying the development and release of drugs may result in the loss of business and revenue

Patient or provider lists — Selling of personal information can damage reputation or business

Corporate and information website content — Selling of proprietary information can disrupt business and damage reputation

What does this mean for pharmaceutical organizations?

The pharmaceutical industry has the third-highest average total cost of a breach, $4.8 million in 2022, behind only non-pharmaceutical healthcare and financial services.

Bad actors generally target specific companies with a particular objective in mind. But crimes of opportunity are not out of the question: criminals take a broader approach, and look for any available information to use to their advantage. The goals of the criminals vary; sometimes the desired result is to wreak havoc, disrupt operations, or damage reputations, and sometimes the intention is to steal valuable assets.

Notable life sciences and pharmaceutical company cyberattacks

	MOTIVATION	METHOD	DAMAGE	HOW TO PROTECT AGAINST
UNNAMED CYBERATTACK ON EUROPEAN MEDICINES AGENCY (EMA) 2020	Steal documents related to the regulatory submission of a COVID-19 vaccine	Credential stealing of a single IT application	Word documents, PDFs, email screenshots, PowerPoint presentations, and EMA peer-review comments were leaked in an edited format one month later	Multi-factor authentication, which is an additional layer of verification beyond log-in and password credentials
NOTPETYA 2017	Attack on Ukraine, with hundreds of companies as collateral damage, to wreak havoc, disrupt operations, or damage reputations	Malware in a tax application	30,000 computers down for two weeks across a large pharmaceutical company, including sales, manufacturing, and research — $410 million of potential sales lost	Microsegmentation, which allows the setup and enforcement of process-level rules to control flow between application components
DRAGONFLY (AKA ENERGETIC BEAR) 2014	Theft of IP, including proprietary recipes and production sequence steps, including pharmaceutical IP for the purpose of manufacturing counterfeit drugs	Trojan to download code to compromise the industrial control software	Minor, though the attack did wake up the industry to supply chain threats	Secure web gateway that prevents unauthorized traffic from entering the network by filtering DNS queries

Prioritizing security

Whether you are protecting the thousands of potential access points in internal systems and data, cloud-hosted solutions, or hybrid solutions, it is paramount to prioritize security. There are two layers to think about: bad actors getting into your system (north–south) and what they do once they are inside (east–west; think: lateral movement).

Who are the bad actors?

The bad actors may be any criminal, from big and well-funded groups sponsored by nation-states to smaller actors looking to cause mayhem; they can even be insiders.

Cybercriminal groups targeting pharmaceutical companies

Industrial Spy — The online extortion ring hijacked the data of one of Switzerland's largest pharmaceutical companies, attempting to sell the data on their Dark Web marketplace for $500,000 in crypto-currency.

ALPHV — The ransomware group took responsibility for accessing more than 17TB of data from the world's fourth-largest generic drugs manufacturer. The stolen data included sensitive information on customers and vendors and employment documentation for more than 1,500 employees.

Insider threats are difficult to detect because the actor doesn't need to break into the network they already have access. These threats can be accidental, like an untrained employee or one who skips a security step to save time; or they can be malicious, to sell secrets or disrupt operations.

> **Forrester predicted that insider incidents, both accidental and malicious, would factor into a third of all data breaches in 2023.**

Bad actors in the system

At some point, bad actors might succeed in breaching your system. To gain entry they may use tools to manipulate people to share confidential information through social engineering, like phishing; through brute force to repeatedly test a system, such as with stolen usernames and passwords; or via botnets or human farms that try combinations of usernames and passwords until they find a way in.

Once inside, they may exploit a zero-day vulnerability — code that the network owner doesn't know is there or for which there isn't yet a fix. These criminals can then take advantage of the vulnerability to launch a big attack — whether it's stealing valuable assets like PHI or taking over the enterprise system to cripple operations and demand ransom.

How to protect your organization

Zero Trust

In today's complex IT environments, the risk of exposure is from both outside and inside the network. And the most effective security model for protecting all aspects of the network is Zero Trust. This principle is based on a strict identity verification process — only authenticated and authorized users and devices can access specific data and applications, protecting the applications and the users from threats on the internet.

North–south security

Traffic into and out of the network is referred to as north–south traffic. Protecting your system from an outside attack includes:

- Access security — gives users precise access to only the apps they need
- Secure web gateways — safely connects users and devices to the internet
- Authentication — allows only trusted users inside the system

East–west security

Inside-the-network activity is referred to as lateral, or east–west, traffic. Protecting traffic between internal hosts and servers is trickier — you cannot know that all traffic is from trusted users. With the average cybercriminal being inside a system for 322 days, it is important to be able to stop bad actors from moving around your system and figuring out what to steal or how to disrupt your whole enterprise.

East–west security is about limiting bad actors' ability to move once they are identified inside the network and includes:

Microsegmentation — controls access and segments users by identity

Scenario

A pharmaceutical company with cross-functional teams and projects, with many owners of different IT applications within the network, across both on-premises and cloud environments, detected a malicious IP address connected to the network.

The core security rules were customized and set by a third-party contractor and the cloud service provider security was on-demand, so there was confusion about which team was responsible for the attack vector and what they could do to stop the breach.

The lack of insight into the system, and the misunderstanding about who should take responsibility for fixing the problem, added hours to response time, meaning the hacker had extra time inside the system for malicious behavior.

With visibility into the system and microsegmentation, the company could have identified the bad actor sooner and limited the hacker's movement (and disruption) within the network.

Conclusion

Robust security tools are both proactive and reactive in addressing cyberthreats by mitigating risk in the ever-evolving IT landscape and by limiting the effects of a breach. Look for tools that have the capability to evaluate breaches and attempts after the fact to learn what went wrong so you can strengthen protocols for the future.

Remember, no single technology or product can protect every aspect of your infrastructure, either internal or cloud systems. Effective security requires layers of protection, both inside your enterprise and with service providers.

Choosing a technology partner that can cover your system from every angle, and provide a single pane of glass — visibility into all your security in one platform — provides significant benefits. As you think about how to optimize your organization's enterprise cybersecurity posture, ask yourself these questions:

- Do I have visibility into the entire system?
- What does it cost me to do it myself, including hiring the right people to keep the system up to date?
- What is the potential cost of an attack to our business — downtime, lost IP, data breach fines, etc?
- How am I protecting both on-premises and cloud solutions?
- How complex is my security response? Do I know who to contact in the event of an attack, or do I have to work with teams across business units, as well as internally and externally?

As the complexity of the healthcare and life sciences ecosystem grows, and your organization scales to evolve in tandem, it's imperative to consider a third-party provider with extensive experience in your industry.

Akamai powers and protects life online for nine of the world's largest pharmaceutical companies, along with the largest banks, retailers, governments, and streaming platforms. More than two decades of experience has given Akamai the perspective to precipitate and evaluate cutting-edge trends and innovations among threat actors, and work across on-premises and cloud services providers to build solutions based on cybersecurity best practices.

Akamai has the tools to protect your enterprise from a variety of threats

- Microsegmentation to limit the spread of ransomware inside the system
- Web application firewall to protect web pages and APIs
- Secure web gateways to prevent users from visiting malicious sites
- Multi-factor authentication to admit only authorized users to the system
- Layered protection against DDoS attacks

Learn more about Akamai's comprehensive solutions for pharmaceutical enterprises by contacting us today.

Contact us here, or give us a ring at +1-877-425-2624.