proofpoint.

SOLUTION BRIEF

Securing Pharmaceutical and Life Sciences Firms with Proofpoint

Protect patient data, IP and operations from today's biggest threats

Products

- Proofpoint Threat Protection
- Proofpoint Identity Threat Defense
- Proofpoint Information Protection
- Proofpoint Intelligent Compliance

Key Benefits

- Secure IP and PHI against financially motivated attackers, nation-state actors, and insider threats
- Protect the people in your organization—especially those who are most likely to be attacked
- Support compliance in a heavily regulated industry

Pharmaceutical and life sciences firms face many of the same cybersecurity challenges as other healthcare organizations. They must, for example, safeguard employee data and patients' protected health information (PHI). But they also must protect large amounts of intellectual property (IP). This IP can include drug formularies, manufacturing processes, prototypes and clinical trials. And because this data is so valuable, drugmakers are enticing targets for both cyber criminals and nation-state actors. A cyber attack can cost a life sciences firm not only financially, but also reputationally. And in extreme cases, such attacks can put years of research into jeopardy. Proofpoint's people-centric approach helps protect your data, operations and IP from today's biggest threats.

A Treasure Trove of Data

Life sciences firms develop safe, effective medical products that improve health and enhance lives. To do this, they must keep detailed records of drug formularies and production processes. They conduct clinical trials and other research to prove the effectiveness of their products when used as prescribed. This often requires direct interaction with patients. It also involves the maintenance of detailed medical records for each participant.

All of this record-keeping creates large amounts of sensitive information, which can include IP, clinical trial data and PHI. And this makes these firms very attractive targets for cyber criminals. They can cash in on both stolen IP and PHI from a single attack. It also increases the risk that data loss or system downtime can spoil clinical research. In short, maintaining data integrity and business continuity can be a matter of life and death. This is true not only for the patients that a life sciences firm serve, but for its own business as well.

Hurting the Healers

Cyber threats on pharmaceutical companies can have many harmful effects, including:

- Loss of competitive advantage and market position
- Fines for noncompliance with the Health Insurance Portability and Accountability Act (HIPAA) and other regulations
- Fines and other costs from breaches of clinical trial results and patient data
- Damage to critical systems and business disruptions, such halting drug production
- Brand damage, which means consumers lose trust in a company's ability to protect their personal health information or keep drugs safe
- Reduced shareholder value from bad press and fines attributed to a breach
- Financial impact due to lawsuits and lost revenue

But in an era of global digital collaboration, that challenge is more complex than ever. To bring innovations to market today, companies share large amounts of data both internally and with outside partners. Internal users may even access this data over the public internet through software-defined networking and cloud-based applications. When third parties use the data, they view it on devices outside of the company's control. This means the data may be on network infrastructure that they do not directly protect.

Cyber attackers can use this openness to gain access to valuable information. And they act to cash in on it. A successful attack can cause direct financial harm to a pharmaceutical firm. It can cause longer-term damage to their brand. And it can even potentially cause physical harm to customers.

An Industry Under Attack

Cyber attacks have continued apace in recent years. In September 2022, the RansomHouse cyber crime group exfiltrated an estimated 500 GB of employee and IP data in a ransomware attack on IPCA Laboratories, one of India's largest pharmaceutical firms.[1] Another Indian firm, Aarti Drugs, lost business data in a separate incident a day earlier.[2]

Firms in Western countries are not immune to the threat. Novartis, for instance, suffered an attack in February 2022.[3] In that case, the company did not lose any sensitive data. But hackers did leak clinical trial data for the COVID-19 vaccine from Pfizer-BioNTech in December 2020.[4] And other cyber criminals tried but failed to do the same thing with AstraZeneca a month before.[5]

Financially motivated attacks

Most attacks on pharmaceutical firms are financially motivated. And the stakes are very high. Bringing a new product to market is a lengthy and expensive process. The London School of Economics found that the average cost to bring a drug to market is $1.3 billion.[6] This figure may be staggering, but other studies have found costs that are up to twice as high.

Illicit drug companies can steal IP directly to replicate a medicine for their own benefit. And ordinary cyber criminals can command big sums for stolen IP on the black market. PHI from patients is also valuable. It can be used in identity-theft schemes. It can also be sold directly to others. In recent years, ransomware has been a preferred tactic for making a quick buck. But the more recent trend of data exfiltration as a part of a ransomware attack makes this method even more risky.

1 Jagmeet Singh (*TechCrunch*). "Extortion Group Claims Cyberattack on Pharmaceutical Giant IPCA Laboratories." September 2022.

2 Ibid.

3 Lawrence Abrams (*Bleeping Computer*). "Novartis Says No Sensitive Data Was Compromised in Cyberattack." June 2022.

4 Sophie Porter (*Healthcare IT News*). "Pfizer COVID-19 Vaccine Data Leaked by Hackers." January 2021.

5 Jack Stubbs (*Reuters*). "Exclusive: Suspected North Korean Hackers Targeted COVID Vaccine Maker AstraZeneca—Sources." November 2020.

6 *London School of Hygiene & Tropical Medicine*. "Average Cost of Developing A New Drug Could Be Up To $1.5 Billion Less Than Pharmaceutical Industry Claims." March 2020.

PHI is also valuable for stealing identities. Criminals can even use it for obtaining prescription drugs in a patient's name. Scammers often obtain opioids and other highly addictive drugs for their own use or to sell to others. This is the so-called OxyContin threat vector. And the corporate network is not the only place where bad actors can obtain PHI. Social media sites that pharmaceutical firms use can also open other doors for potential PHI theft.

Life sciences firms are especially susceptible to advanced persistent threats from state-sponsored entities, which often have deep pockets and sophisticated technology.

Geopolitically motivated attacks

Hackers are not the only ones who seek to monetize data from pharmaceutical firms. Nation-state actors also target them. These state-owned drug companies are interested in drugs that are under development. The companies are beyond the reach of institutions in the West that enforce patents and require new drugs to undergo a lengthy approval process. A company that steals drug-related trade secrets can use that information to rush to market with a cheaper version. Doing so would undercut the firm that invested in its development.

This means that life sciences firms are especially susceptible to advanced persistent threats (APTs) from state-sponsored entities, which often have deep pockets and sophisticated technology.[7] But the attackers also use more low-tech tactics. They might bribe an insider to hand over key data, for example. Or they might plant a spy, hired as a legitimate employee, to carry out the deed.

Insider threats

Insider attacks are another risk. These can come from both malicious and well-meaning users. After years of extreme stress for workers in the healthcare sector, it is hardly surprising when an overworked employee accidentally clicks on a phishing email. The same job-related stress can also lead to workers who become disgruntled. And they may be tempted to steal confidential data for nefarious purposes. Either way, the growing universe of "insiders" increases risk. These insiders now include partners and other third parties who have access to internal systems.

Malicious outsiders who gain access to an insider's privileged account are another type of threat. Credential theft is still the most common path that cyber criminals use in data breaches.[8] It enables attackers to traverse the network disguised as an insider. This path can bypass detection and monitoring tools. Unmanaged superuser accounts can lead to loss or theft of sensitive data. They can also serve as an entry point for malware.

7 Meg Rivers (*Pharmaceutical Executive*). "Cybersecurity Threats & Pharma." January 2023.

8 Verizon. "Data Breach Investigations Report 2022."

A People-Centric Approach

Like firms in many other industries, drugmakers have invested in traditional security tools. But these tools defend only the traditional network perimeter. And this perimeter is dissolving. Gone are the days when sensitive data is kept within a traditional, firewall-protected, on-premises corporate network. Instead, "borderless" drug research and development networks are now the norm.

Attackers no longer expend much effort to penetrate a firewall. Instead, they target individuals. That's why drugmakers must take a people-centered approach to secure their stakeholders, users and consumers as well as the data they use and share.

Pharmaceutical and life sciences workers are duty-bound to improve lives. This can make the industry especially vulnerable to attacks that exploit human nature. Figure 1 shows an analysis of the top 10 Very Attacked Persons™ (VAPs) at a real multinational pharmaceutical firm.

We assessed attacks and their targets using Proofpoint Targeted Attack Protection (TAP), which includes sandbox analysis. Their email addresses received more malicious attack attempts than any others in the company.

It is not surprising to see the company's CEO in the top 10. This is because cyber criminals often exploit password vulnerabilities to navigate through the personal email accounts and social media. Beyond this, the top 10 VAPs tend to be public-facing email addresses and aliases, specifically those in the public affairs office. This team is highly visible. And it addresses policy issues related to funding, regulations and IP. Their emails are also among the easiest to obtain.

Also interesting is the large number of credential phishing, imposter, keylogger and malware attacks identified in the top 10 alias VAPs. Impostor attacks are sophisticated because they do not have malicious payloads to detect. Attackers often pose as someone who their victims trust. They then trick them into making fraudulent financial payments. Keyloggers are a form of spyware that tracks the keys pressed on a keyboard without the user knowing. This can result in the theft of credentials and PHI.

How Proofpoint Can Help

Our people-centric approach is uniquely equipped to help you manage today's threats in all the digital channels that matter. These channels include email, cloud, web and social media. Our cloud-based suite protects you against a wide range of attacks. We can help make users more resilient, stop attacks where they start and block unsanctioned access to sensitive data and systems.

Proofpoint solutions are built on four platforms:

- Threat Protection
- Identity Threat Defense
- Information Protection
- Intelligent Compliance

Each of these platforms is described in more detail below.

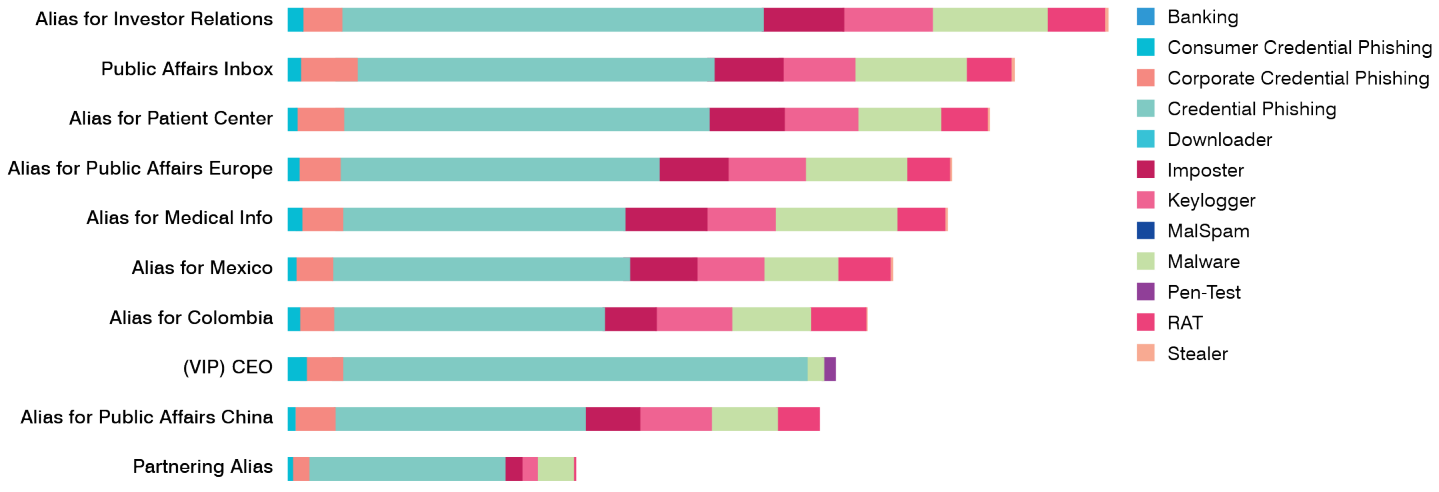

Figure 1: Top 10 Very Attacked Persons (VAP) for a multinational pharmaceutical company.

Threat Protection platform

Proofpoint Threat Protection is an artificial intelligence (AI) and machine learning (ML) platform that disarms today's advanced attacks. These attacks can include business email compromise (BEC), phishing, ransomware, supply-chain threats and more. Threat Protection solutions focus on email security and threat protection, advanced threat protection and security awareness training.

Email security and threat protection

The platform's email security and protection solutions protect people, data and brands from common and new threats and help to reduce inbox clutter. They include solutions like:

- **Proofpoint Email Protection**—Protects users against unwanted and malicious email such as impostor email or BEC
- **Proofpoint Email Fraud Defense**—Helps you protect your firm's reputation in email fraud attacks
- **Proofpoint Threat Response Auto-Pull**—Automatically recalls malicious emails that have already reached a user's inbox

For more information on these and other Proofpoint email security and protection solutions, see **proofpoint.com/us/products/email-security-and-protection**.

Advanced threat protection

The platform's advanced threat protection solutions help you stop threats before they reach your people. They also allow you to respond quickly when things go wrong. They include solutions like:

- **Proofpoint Targeted Attack Protection**—Detects, analyzes and blocks advanced threats
- **Proofpoint Email Isolation**—Allows users to freely access personal webmail and corporate email from corporate devices without security concerns
- **Proofpoint Threat Response**—Helps your security teams respond more efficiently to threats
- **Proofpoint Emerging Threats Intelligence**—Gives your security teams the intelligence and context they need to stop malicious attacks

For more information on Proofpoint advanced threat protection solutions, see **www.proofpoint.com/us/products/advanced-threat-protection**.

Security awareness training

The Threat Protection platform also has Proofpoint Security Awareness training packages. These packages can turn even your most attacked people into a strong line of defense. They provide up-to-date and relevant real-world phishing simulations to help assess which users are vulnerable, and how. Education modules help people become better informed about emerging threats. You can track user progress over time to help them improve.

For more information on Proofpoint Security Awareness training solutions, see **www.proofpoint.com/us/products/security-awareness-training**.

Identity Threat Defense platform

Solutions in the Proofpoint Identity Threat Defense platform detect and prevent identity risk to stop lateral movement and privilege escalation.

- **Proofpoint Shadow**—Detects attackers trying to move laterally within your organization. It consistently identifies attacks that often bypass signature and behavioral approaches to detection.
- **Proofpoint Spotlight**—Automatically discovers and remediates identity vulnerabilities before attackers can exploit them for unauthorized lateral movement and privilege escalation.

For more information on Proofpoint Identity Threat Defense solutions, see **www.proofpoint.com/us/products/identity-threat-detection-response**.

Information Protection platform

The Proofpoint Information Protection platform merges content classification, threat telemetry and user behavior across channels in a unified interface. Its solutions focus on information protection and cloud security.

Information protection

The platform's information protection family of solutions protects data against both accidental and malicious insider threats. These solutions extend protection across your cloud services, email, endpoints, cloud apps, web and on-premises and shared cloud repositories. They give you a people-centric approach to data loss prevention (DLP). And they bring together content, threat and behavior insights.

For more information on the Proofpoint information protection family of solutions, see **www.proofpoint.com/us/products/information-protection**.

Cloud security

The platform's cloud security solutions help you deliver secure access to web and cloud services. These solutions include:

- **Proofpoint Cloud Account Defense**—Protects users from Microsoft Office 365 account compromise
- **Proofpoint Cloud App Security Broker**—Provides risk-aware data protection for cloud apps
- **Proofpoint Browser Isolation and Proofpoint Web Security**—Allow your users to freely access websites, personal email and cloud apps

For more information on the Proofpoint cloud security family of products, see **www.proofpoint.com/us/products/cloud-security.**

Intelligent Compliance platform

Proofpoint Intelligent Compliance is a platform of solutions for compliance and archiving. They help you execute a strategy to enable compliance with regulatory requirements or other standards. The platform includes solutions like:

- **Proofpoint Capture**—Helps you capture and retain content efficiently from all the tools your employees use to communicate
- **Proofpoint Patrol**—Simplifies compliance for social media communications by giving you full visibility into the social activity of your employees and customers
- **Proofpoint Track**—Gives you control and visibility into your capture stream
- **Proofpoint Archive**—Helps you address all your basic e-discovery requirements
- **Proofpoint Discover**—Enhances Proofpoint Archive to empower your legal teams with self-service control over e-discovery

For more information on the Proofpoint Intelligent Compliance platform, see **www.proofpoint.com/us/products/archiving-and-compliance**.

Conclusion

Proofpoint gives life sciences firms protection and visibility for their greatest cybersecurity risk: their people. We provide the most effective cybersecurity for researchers, production managers, executives, clinical trial patients and others. We protect them whether they are targeted through email, web, social media or cloud apps. And we help stop threats and protect your data, operations and IP from today's biggest cyber attacks. Leading pharmaceutical and life sciences firms of all sizes, including more than 75% of the Fortune 500 healthcare organizations, rely on Proofpoint for people-centric security and compliance solutions to mitigate their most critical security risks before they can cause lasting harm.

LEARN MORE

For more information, visit **proofpoint.com**.