illusive

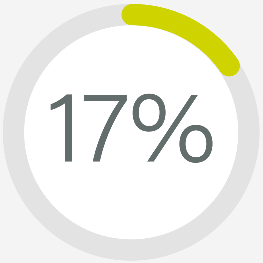
WHITE PAPER

Cyber Risk on the Front Lines of Pharma

To Combat Attacks, Drug Companies Must Combat Lateral Threat Movement on Their Networks

Pharmaceutical and biotechnology companies have always faced a unique mix of challenges. Their work is highly regulated, and their continued profitability depends on a robust pipeline of new products under development. They are at the cutting edge of health research, and such research is expensive. One analysis found that the industry spends 17% of revenues on research and development—more than every other sector except for the semiconductor industry.[1] With the average cost of bringing a new drug to market topping $300 million,[2] companies take on an extraordinary financial risk with every research project. This is especially true for companies taking part in the current race to develop an effective and widely distributed vaccine against SARS-CoV-2, the virus that causes COVID-19—as well as therapeutics that might improve patients' prognosis. Every new drug represents millions of dollars in investment and intellectual property requiring proper protection and security.

One analysis found that the industry spends 17% of revenues on research and development



Cybersecurity Compounds the Hazards

On top of these risks, pharmaceutical firms and other healthcare organizations remain top targets for cyber criminals. In fact, some evidence suggests that the industry is even more targeted in the wake of the COVID-19 pandemic. The Verizon Data Breach Investigations Report for 2020 identified 521 confirmed instances of data exposure in the healthcare industry, which for the purposes of the report included pharmaceutical and life sciences firms—up from 304 in the prior year's report.[3]

The way such attacks are publicized, they often seem to have occurred quite quickly. But the fact is that 70% of successful attacks involve lateral movement within the network by adversaries[4] —often for weeks or months. Research by the Ponemon Institute found that the average time to identify and contain an attack was 280 days in 2020—up slightly from 279 days in 2019.[5] And once adversaries are inside an organization's network undetected, perimeter defenses are useless.

70% of successful attacks involve lateral movement in the network by adversaries

Average time to identify and contain an attack is 280 days

Data Protection:

Another Big Risk in a Risky Business

Working at the intersection of cutting-edge medical research and precision manufacturing, pharmaceutical and life sciences firms must protect critical data to protect throughout the lifecycle of each research project, and of every drug that is ultimately brought to market. Two types of information are vulnerable to theft through data breaches—intellectual property and personal health information (PHI).

Intellectual Property

Protecting intellectual property has always been a priority for the pharmaceutical industry, and the security of this data may be even more important as companies compete to develop therapeutics and vaccines for COVID-19.[6] The scientific data related to development and clinical trials for these drugs could bring great financial benefit for a cyber criminal, and nation-state actors have built extensive infrastructure for industrial espionage.[7]

Likewise, data about manufacturing processes, details about procurement and the supply chain, and financial data can be attractive targets for attackers. Pharmaceutical products are typically only protected by patent for seven years in the United States, and this data could help foreign generic drug manufacturers to be more ready for the expiration of the patent.

© 2020 Illusive Networks. All rights reserved.

Personal Health Information (PHI)

Another risk during clinical trials is the disclosure of patient data. Pharmaceutical and biotechnology companies compile extremely detailed health records when they assess potential participants and monitor the research subjects who are selected.[8]

Most trials require a detailed medical history, regular laboratory tests, and frequent visits with doctors involved in the research. What is more, many pharmaceutical companies find that patient data is all over the network—from medical Internet-of-Medical-Things (IoMT) devices at the network edge to databases at the heart of the data center or in the cloud.

The Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union both place strict controls on the use of personal health information (PHI)—and impose substantial penalties when data is breached. In addition to those costs, organizations face the all-too-real costs of remediating systems, compensating victims, and degradation of brand value when a breach actually occurs.

Industry giant Pfizer recently experienced a close call when it learned that PHI of hundreds of prescription drug users had been exposed for months—or even years—in an incident blamed on misconfiguration of a cloud storage system.[9] The unprotected Google Cloud storage bucket also contained financial and personally-identifiable information (PII) for some patients, along with transcripts from calls to a customer service line.

Data Integrity:

Lives Are on the Line

While the theft of business-critical data would be devastating to a pharmaceutical or life sciences company's bottom line, cybersecurity threats to the integrity of data can be a matter of life or death for patients and research subjects.

Medical Research and Formulary Data

Data from clinical trials is not only subject to theft, but also to being corrupted. For example, databases that track which subjects are taking the placebo rather than the drug being studied are extremely sensitive. Neither patients nor most of the healthcare workers involved in the study may know this information. If this data is disclosed, this could spoil an expensive trial. If the integrity of the information is attacked, subjects could potentially experience devastating medical consequences.

Precision Manufacturing Data

Data integrity also poses a risk in the manufacturing process. For example, if the formulary for this year's influenza vaccine is maliciously changed in an electronic system, thousands or millions of patients could lose immunity. The same is true for vaccines and therapeutics for COVID-19, with even more risky results.

Security Challenges:

Threats from All Directions

Those who manage cybersecurity at pharmaceutical companies likely feel bombarded from every side in today's threat landscape. Attackers can come from the outside or the inside, they can attack anywhere across a broad attack surface on an increasingly distributed network, and they routinely use attack methodologies that can be devastating to operations.

Ransomware: Disabling Systems for Profit

While different attack types tend to go in and out of fashion with cyber criminals on a fairly rapid basis, ransomware has been one of the most popular for several years.[10] As their work has become more sophisticated, they have gotten better at locking down systems, which has made their ransom demands more effective. While many victims can restore their systems without paying the ransom, enough see no alternative but to pay—and this success results in even more ransomware attacks being launched.

The pharmaceutical industry saw the damage that ransomware can cause when Merck was attacked by the NotPetya encrypting malware in 2017. Digital systems were down for two weeks, and the company ultimately reported that the attack caused $1.3 billion in damages.[11] While damage at that scale is less common, ransomware attacks are becoming almost routine in the healthcare industry. In recent months, ruthless attackers caused days and weeks of downtime at several hospital systems in the middle of a pandemic,[12] and executed a combination of ransomware and data theft at a pharmaceutical staffing firm.[13]

Unfortunately, ransomware is currently seeing an unprecedented spike in volume, with one study estimating that it will ultimately grow sevenfold in 2020 over 2019.[14] This astounding increase suggests that ransomware has evolved so that it behaves more like an advanced persistent threat, in which adversaries penetrate a network, moving about undetected for weeks or months until they are in the perfect position for a successful attack.

Insider Threats:

Malicious Actors and Human Error

While nation-states and common cyber criminals often pose a significant risk to organizations, a substantial percentage of attacks come from the inside, rather than from external hackers. In fact, one study found that the average organization sees $11.45 million in annual costs from insider threats—both malicious and inadvertently through negligence.[15] A related phenomenon is third-party risk, as most companies today routinely grant access to sensitive systems and applications to partner organizations.

The value of the data housed at pharmaceutical companies can create temptation for longtime employees who are perhaps less happy at the organization than in the past. At the same time, many employees and family members have felt significant economic pain since the beginning of the pandemic. Insider threats come from employees who are already trusted users in the system and know where critical data is located. Third-party access adds a further complication, as the company that owns a particular IT asset may not even have an employer–employee relationship with many users that have access to it.

© 2020 Illusive Networks. All rights reserved.

OT Systems:

Not Designed for Security

While pharmaceutical companies must manufacture their products with great precision, the operational technology (OT) infrastructure that runs the factory floor is, more often than not, based on very old technology. Historically isolated by "air gapping," OT systems are now increasingly connected to IT systems—and to the internet.[16] According to one recent study, nearly two thirds of OT devices are connected—32% directly to the internet, and another 32% through a gateway into the enterprise.[17]

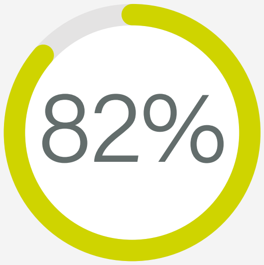
While connected OT systems bring great benefits in efficiency, the elimination of the air gap exposes OT systems to IT-based security risks—and to intrusion by adversaries who have infiltrated the IT network. Since these systems typically were not built with security in mind, this can be a real problem. A lack of visibility is another problem. One survey found that 82% of respondents said they are unable to identify all the devices connected to their OT and IT networks.[18] As OT systems are added to the IT attack surface, their lack of security protection can be the "weak link" through which cyber criminals can enter.

IoT and IoMT Devices:

A Ballooning Attack Surface

Internet-of-Things (IoT) devices are proliferating across all industries. IDC estimates that there will be 41.6 million connected IoT devices in 2025, generating 79.4 zettabytes of data.[19] In the pharmaceutical industry, firms depend on IoT devices on the manufacturing floor to ensure smooth operations. In the R&D function, IoMT devices are increasingly critical to both research and patient care.

While the benefits of IoT and IoMT devices are clear, they increase the attack surface dramatically, providing more openings for cyber criminals to penetrate the network from the edge. Devices often have poor security protection built in, and the vast number of device types increases complexity. Attackers can enter a network through such devices and move laterally to systems with valuable data, threatening data integrity while they move about.



of respondents said they are unable to identify all the devices connected to their OT and IT networks.[18]

© 2020 Illusive Networks. All rights reserved.

Eroding Effectiveness of Behavioral Detection:

What Is Really Normal?

While many pharmaceutical and life sciences organizations have deployed behavior-based approaches like user and entity behavioral analysis (UEBA) to spot anomalous behavior on the network, today's changing workplace and the rapidly evolving marketplace mean that it is difficult for such solutions' algorithms to keep up with what is "normal" behavior. A massive shift toward working from home in the first half of 2020 has been followed at some companies with a gradual return to the workplace or "hybrid" arrangements. At other organizations, remote work may be the new standard.[20] Either way, organizations are evolving their practices at warp speed to respond to the rapid change in business conditions and customer preferences.

The result of this turmoil is an increase in false positives for behavior-based tools—and less ongoing clarity about how benign activity can be distinguished behaviorally from malicious activity.[21] These complications compound longstanding stresses caused by the cybersecurity skills shortage, which has resulted in understaffed and overwhelmed security operations teams that simply cannot keep up with the alert noise from a variety of security tools.[22]

© 2020 Illusive Networks. All rights reserved.

Conclusion:

Fighting Back to Protect Pharma

Clearly, pharmaceutical and biotechnology companies face a complex threat landscape, with several types of complex and sensitive data to protect, an expanded attack surface, and a variety of threat vectors. Detecting intruders early is critical, but the average organization takes more than nine months to do so. It is clear that a new paradigm is needed, with which organizations can "shift left" with their intrusion detection while minimizing noise. Specifically, organizations would do well to take the following steps:

Shrinking the Attack Surface to Prevent Malicious Lateral Movement

An expanded attack surface creates more opportunities for adversaries to penetrate a network—and move laterally within it. Because of this, it is critical to be proactive about limiting the pathways that attackers can use to hop from endpoint to endpoint on a network without being detected.

Organizations create these pathways in the course of normal business: failing to close access to specific systems for users who no longer need it, adding new services without adequate network segmentation, failing to change passwords regularly—or even using default passwords—just to name a few. The key is to develop an automated, policy-driven way to find these pathways and remove them as they are created.

Detecting Early Malicious Lateral Movement Through Deception

In addition to reducing the actual attack surface, it is helpful for pharmaceutical and biotechnology companies to expand the apparent attack surface using deception technology. This involves the placement of imaginary paths and devices that look and feel like what attackers would normally use to infiltrate and move laterally within a network. These deceptions surround legitimate paths and devices in great numbers—including hard-to-protect OT, IoT, and IoMT devices.[23]

The result is that attackers cannot tell the real paths from the fake ones, and must second-guess every movement they try to make. The moment attackers interact with deceptive data, they are detected—whether they are attempting to deploy a targeted ransomware attack, steal critical data, or any other intrusion. This is because deceptions are not accessible to legitimate users, but are hidden where only malicious actors would see them. This eliminates the guesswork—and the false positives—inherent in behavior-based detection tools.

Leveraging Source-Based Forensics on Demand

Another critical step for pharmaceutical and life sciences organizations is to achieve the ability to conduct forensics so that the security operations team can glean actionable information about attack trends and the effectiveness of current security practices. A deception technology solution should have the ability to collect forensics about each attack including a chronological timeline, screenshots of what happened at an endpoint, and the pathways taken by attackers.

Armed with this information, security operations can take strategic containment steps using other security tools like security information and event management (SIEM), security orchestration, automation, and response (SOAR), and endpoint detection and response (EDR). With the forensics reporting automated and false positives virtually eliminated, lower-tier analysts can handle more incidents themselves while escalating the most risky alerts.

Eliminating highly manual data collection and correlation efforts not only makes the security operations center (SOC) more efficient, but also can improve morale on the team. No longer will they need to do manual compilation and correlation of attack data—often on an urgent timeline—only to respond after it is too late.

A Holistic Approach to Preventing Lateral Movement

Shrinking the real attack surface, expanding the imaginary attack surface, and automating forensics can help pharmaceutical companies protect the security and integrity of their critical data. This enables them to focus on what they are really good at—developing and producing products that preserve human life and improve its quality.

© 2020 Illusive Networks. All rights reserved.

Sources

[1] “Average Research & Development Costs for Pharmaceutical Companies,” Investopedia, August 8, 2019.

[2] “New Estimate Puts Cost to Develop a New Drug at $1B, Adding to Long-Running Debate,” Biopharma Dive, March 3rd, 2020

[3] “2020 Data Breach Investigations Report,” Verizon, April 2020.

[4] “Global Incident Response Threat Report,” Carbon Black, April 2019.

[5] “Cost of a Data Breach Report, 2020,” Ponemon Institute and IBM, April 2020.

[6] Saheli Roy Choudhary, “In Race to Bring Vaccine to Market, Big Pharma Struggles to Protect its Intellectual Property Rights,” CNBC, July 9, 2020.

[7] Steve Grobman, “When Nation-states Hack the Private Sector for Intellectual Property,” The Hill, March 31, 2018.

[8] Marjorie A. Bowman, “A Beginner’s Guide to Avoiding Protected Health Information (PHI) Issues in Clinical Research,” ScienceDirect, September 2018.

[9] Tara Seals, “Pharma Giant Pfizer Leaks Customer Prescription Info, Call Transcripts,” ThreatPost, October 20, 2020.

[10] Juliana De Groot, “A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time,” Digital Guardian, October 6, 2020.

[11] David Voreacos et. al, “Merck Cyberattack’s $1.3 Billion Question: Was It an Act of War?” Bloomberg, December 3, 2019.

[12] Laura Dyrda, “4-day Nebraska Medicine Computer System Outage Wreaking Havoc at 2 Health Systems,” Becker Hospital Review, September 24, 2020.

[13] Phil Muncaster, “Pharma Giant ExecuPharm Suffers Data Breach/Ransomware Combo,” InfoSecurity, April 29, 2020.

[14] Danny Palmer, “Ransomware: Huge Rise in Attacks This Year as Cyber Criminals Hunt Bigger Pay Days,” ZDNet, September 9, 2020.

[15] “Global Cybersecurity Study: Insider Threats Cost Organizations $11.45 Million Annually, up 31 Percent from 2018,” Proofpoint, February 3, 2020.

[16] Baral Perelman, “Digital Transformation in Pharma Introduces New OT Security Threats,” SecurityWeek, October 29, 2019.

[17] Barbara Filkins, “The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns,” SANS Analyst Program, July 2018.

[18] Jeff Goldman, “IoT Security Fail: 82 Percent of Companies Can’t Identify All Network-Connected Devices,” eSecurity Planet, November 8, 2017.

[19] “The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast,” IDC, June 18, 2019.

[20] “When Everyone Can Work from Home, What’s the Office For?” PwC, June 25, 2020.

[21] Kirby Wadsworth, “4 Ways Coronavirus Will Affect Cybersecurity, and 4 Defense Methods,” Illusive Networks, March 24, 2020.

[22] Silviu Stahie, “SOC Employees Continue to Battle Stress and Skill Shortages, Study Finds ,” Security Boulevard, July 15, 2020.

[23] Nicole Bucala, “Healthcare Under Cyberattack—Advanced Ransomware, IoMT Devices, and Data Breaches,” Illusive Networks, October 8, 2020. See also “Reduce Detection Blind Spots with Deceptive Emulations of IoT, OT, and Network Devices,” Illusive Networks, October 15, 2020.

About Illusive

At Illusive, we know that defenders want to be in command of their security. In order to do that, they need to stop attackers from getting to important assets. Despite significant investments, it’s still difficult to see and stop attackers moving inside the perimeter. We understand how frustrating it is to invest so much and still feel like attackers have the upper hand when defenders deserve to win.

Illusive Networks is the first company spun out of the Israel-based, company-building venture group Team8, which was co-founded by veterans of the country’s military intelligence division, Unit 8200. Illusive Networks offers a proven platform that stops Advanced Ransomware Threats and Advanced Persistent Threats in ways that supplement other defensive technologies, allowing security teams to beat both attackers and red teams alike. Illusive’s multinational clients include top five organizations in the legal, pharmaceutical, and retailer sectors; and top ten global organizations in the financial sector.

Illusive Networks Inc
488 Madison Avenue
11th Floor
New York, NY 10022

Visit us: www.illusivenetworks.com
Email us: info@illusivenetworks.com
Call us:: US: +1 844.455.8748
EMEA / AsiaPac: +972 73.272.4006
Find us: in f

© 2020 Illusive Networks. All rights reserved.