Solution Brief

Security
Pharmaceuticals/
Biotechnology

Pharmaceutical and Biotechnology Organizations Reduce Cybersecurity Risk with Fortinet and Intel

Security-driven networking powered by Fortinet Security Processing Units (SPUs) and Intel® technologies offers a multilayered security approach to increase peace of mind.

Threat actors are becoming more sophisticated as they move against pharma and biotech organizations.

- Nearly 92 percent of pharma organizations surveyed had at least one database exposed, and 46 percent had experienced exposure of data due to unprotected Windows file sharing resources utilizing Server Block Message (SMB) protocol.[1]
- The average cost of a breach for a pharma organization is more than $5 million, which is 1.3x more than the average for other industries.[2]
- On average, it can take up to 257 days for a pharmaceutical company to identify a breach.[3]
- Companies face liabilities if electronic protected health information (ePHI) is exposed.

Introduction

Breakthroughs in the pharmaceutical and biotechnology industries make the world a better place by helping to prevent disease, extend life expectancies, and improve global health. New gene therapies, personalized medicine, and biologics are some of the most sophisticated accomplishments in modern science.

But the complexity of the pharma and biotech development and manufacturing processes can put organizations at high risk for cybersecurity threats. The broad ecosystems of suppliers and partners raise the risk that a supplier or partner might have a weaker security posture. The need to run clinical trials means that sensitive intellectual property (IP) and personally identifiable information (PII) might be exposed. As pharma and biotech companies have invested in digital transformation, their operations and infrastructures have become a mix of digital and legacy technologies. The task of managing both old and new technologies increases the risk that a vulnerability might be overlooked.

Fortinet and Intel understand these risks, and both tech leaders have the expertise and experience to help. Fortinet has achieved nine "recommended" ratings from NSS Labs, and it has achieved the best score in the NSS Labs Next-Generation Firewall (NGFW) Security Value Map.[4] Intel has made security a differentiator in hardware-based computing platforms, and it has invested aggressively in vulnerability management, in addition to offensive security research to make its microprocessors more resilient.[5]

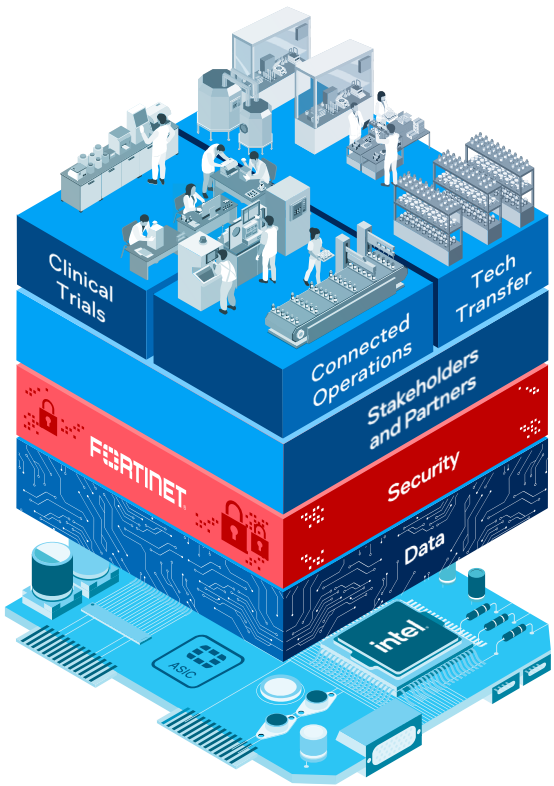

Figure 1. Secure networking powered by Fortinet Security Processing Units (SPUs) and Intel® technologies delivers a multi-layered security approach for pharma and biotech organizations

The Fortinet Security Fabric, powered by Fortinet Security Processing Units (SPUs) and Intel technologies, brings together physical and digital security technologies from each company to scale security enforcement as a single fabric.

The core of the Fortinet Security Fabric consists of FortiGate Next Generation Firewall (FortiGate NGFW), which secures networks from cyberattacks. As the world's most deployed network firewall, FortiGate NGFW can provide deep visibility and security in a variety of form factors, including virtual firewalls and appliances.[6] Some FortiGate NGFW models include Intel® Xeon® processors with Intel® Advanced Vector Extensions 512 (Intel® AVX-512), a set of instructions that can help accelerate performance for vector processing–intensive workloads.[7] Other FortiGate NGFW models use the Data Plane Development Kit (DPDK), a set of libraries that can improve packet processing performance.

The following sections discuss three use cases that illustrate the benefits of the Fortinet Security Fabric.

Technology transfer

Whether developing a transdermal patch, a topical ointment, or an injectable, the transformation of a pharma or biotech candidate into a commercialized product requires a high degree of collaboration.[8] Figure 2 illustrates the high-level steps required to transfer technology from one organization to another. Cybercrime could occur at any stage if a threat actor gains access to a vulnerable endpoint or system. Step 4, digital documentation transfer, is especially prone to risk.

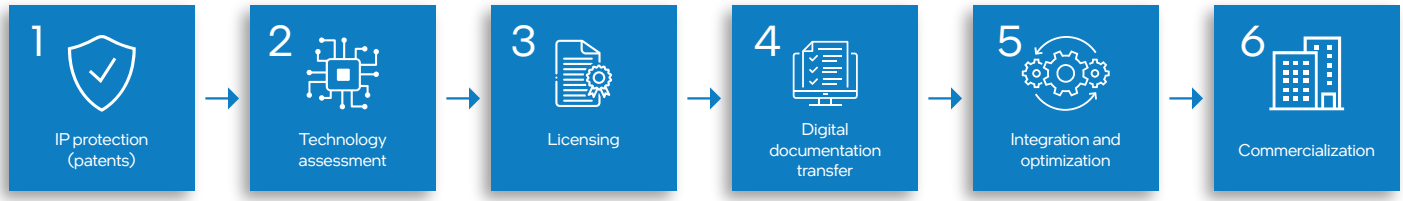

Figure 2. Process flow illustrating joint drug development and manufacturing technology transfer

Scenario: A French university has developed a novel gene-editing technology. The technology has shown promising results in preclinical studies, and the researchers believe that it has the potential to be a game-changer in the field of gene therapy. The research institution wants to transfer the technology to a biotech company for further development and commercialization.

Security challenges:

- Insiders or third parties could steal technology through network access.
- Ransomware actors could extort leaks about research methods or data.
- Outsourced partners might not have the same level of cybersecurity awareness or expertise.

Solution: The university employs FortiGate NGFWs with SD-WAN solutions to help protect network infrastructure, applications, and data from a wide range of threats including intrusions or unauthorized access from insiders or third parties or access by ransomware actors.

Fortinet's portfolio of cybersecurity solutions also includes FortiInsight, the Fortinet user and entity behavior analytics (UEBA) solution. FortiInsight can continuously monitor the behavior of users and endpoints to identify threats from insiders or third parties and respond automatically in real time.

FortiNAC, Fortinet's network-access-control (NAC) solution, which runs on Intel Xeon processors, can help maintain security when research teams work with outsourced partners. FortiNAC helps research teams control devices—a critical step in protecting sensitive IP and documentation.[9] FortiNAC can use Intel® Secure Device Onboard (Intel® SDO), an automated cloud-independent service that allows a device to be provisioned onto a network in a matter of seconds.

Figure 3. A pharma organization has received regulatory approval to start a clinical trial

Clinical trials

Pharma and biotech organizations run clinical trials to evaluate the safety, efficacy, and pharmacokinetics of new drugs or medical devices. Clinical trials are required by regulatory agencies before new drugs or medical devices can be approved for use by patients.

Scenario: An American pharmaceutical company has developed a new drug candidate for the treatment of rheumatoid arthritis, a chronic autoimmune disorder that affects millions of people worldwide. The company has conducted preclinical studies and obtained promising results, and it is now ready to move forward with a clinical trial to evaluate the safety and efficacy of the drug in humans.

The Phase I trial will be conducted with 20 rheumatoid arthritis patients in the United States and Europe. The pharma company is scheduled to start the trial next week.

Security challenges:

- Trial data is subject to cyberattacks, such as phishing, hacking, and malware, especially when trials are carried out at disparate geographic locations.
- Insiders might intentionally or unintentionally disclose sensitive data, or they could introduce malware.
- Organizations open themselves to liability for infringement of the General Data Protection Regulation (GDPR) and other government privacy regulations.[11]

Solution: The Fortinet Security Fabric, with Fortinet SPUs and Intel technologies, can help protect clinical trial sponsors from losing sensitive IP or becoming liable for exposure of patient data. Again, FortiGate NGFW with Intel Xeon processors and SD-WAN solutions plays a pivotal role within the Fortinet Security Fabric. Pharma and biotech organizations can use FortiGate NGFWs to:

- Detect and prevent phishing, hacking, and malware as quickly as possible
- Implement access control to protect sensitive data and comply with regulations
- Deliver automated security at any location

Trial sponsors can also benefit from FortiDeceptor run on Intel Xeon processors. FortiDeceptor poses as legitimate endpoints, such as desktops, servers, printers, or medical devices. When attackers disturb these decoys, FortiDeceptor alerts security operation centers of malicious activity.

The pharma company can also use analysis tools like FortiSIEM. This tool helps bring together logging and information related to data access to help correlate patterns that might be indicative of a security concern. FortiSIEM also runs on Intel Xeon processors, and it helps identify insider and incoming threats that might pass traditional defenses.[12]

Fortinet and Intel ecosystems strengthen security

Both Fortinet and Intel offer broad ecosystems to help customers strengthen their security postures and gain a competitive edge. Fortinet's Open Fabric Ecosystem features more than 500 partner integrations.[10]

Connected operations

Pharma and biotech manufacturers are integrating new technologies, including the Internet of Things (IoT), cloud computing, and artificial intelligence (AI), into their production facilities and throughout their operations.

Scenario: A pharmaceutical manufacturer is investing in smart, connected operations by introducing digital technologies across its manufacturing facility. It has installed sensors on its bioreactors, plate readers, and dispensing systems, which collect data on parameters like temperature or oxygen concentration. Most data is analyzed on-premises, but some is transferred to the cloud for storage or additional analysis. This digital feedback loop improves batch yields, reduces non-compliant deviations in the process, and improves operational efficiency. However, the connected operations have expanded the attack surface.

Figure 4. A pharma manufacturer has invested in connected operations

Security challenges:

- Connecting legacy equipment to the cloud potentially increases exposure to attacks.
- Keeping legacy equipment updated with security patches is an ongoing activity.
- Educating staff on new security processes to avoid inadvertent breaches takes time.

Solution: The Fortinet Security Fabric, with Fortinet SPUs and Intel technologies, provides this pharma manufacturer with a broad, integrated, and automated security architecture that can cover all aspects of its manufacturing business—from the back office to the manufacturing floor. The fabric reaches across the entire manufacturing organization as a single platform, offering a simple approach to addressing vulnerable patchwork security. Fortinet Security Fabric builds on the foundation of FortiGate NGFWs.

FortiGate NGFWs also make use of AI-powered threat intelligence from FortiGuard Labs. Using Fortinet's large global footprint, experts continually monitor the threat landscape and feed information back to strengthen the security of firewalls and appliances.

FortiNAC simplifies onboarding and management of sensors on manufacturing or HVAC equipment. FortiNAC with Intel Xeon processors includes Intel SDO service, so that devices can be provisioned onto networks in seconds.[13]

FortiAnalyzer, a powerful log-management, analytics, and reporting platform that runs on high-speed Intel Xeon processors with the Intel DPDK to boost packet processing, is another tool within Fortinet Security Fabric that can help secure operational technology (OT) networks.

ISVs enhance security solutions for pharma and biotech

ISVs that build software solutions for pharma and biotech on top of Fortinet Security Fabric solutions can enhance protection even further by using additional Intel technologies. Intel's diverse portfolio of hardware-enabled security and accelerator technologies enables the ecosystem to protect against today's most sophisticated cyberattacks.

- **Intel® Software Guard Extensions (Intel® SGX):** Helps protect data in use via unique application-isolation technology. Intel SGX powers confidential computing and allows AI models and data to be shared without exposing IP and sensitive data.
- **Intel® Advanced Matrix Extensions (Intel® AMX) and Intel® Deep Learning Boost (Intel® DL Boost):** Built-in accelerators that improve the performance of deep learning (DL) training and inference on the CPU. Intel AMX and Intel DL Boost take AI performance to the next level to identify patterns and trends.
- **Intel® QuickAssist Technology (Intel® QAT):** Platform-based hardware-acceleration for cryptography and data compression.
- **Intel Advanced Vector Extensions 512 (Intel AVX-512) Vector Neural Network Instructions (VNNI):** Boosts DL performance for intrusion detection and analysis.

Increase peace of mind

Pharma and biotech organizations hold data worth billions of dollars, including IP, research and development (R&D) data, proprietary information, and patient and clinical trial data. This valuable and highly sensitive information makes these industries extremely attractive to cybercriminals.

To help secure connections with suppliers and partners, protect IP and patient data, and secure OT networks, pharma and biotech organizations turn to Fortinet and Intel. The Fortinet Security Fabric, powered by Fortinet SPUs and Intel technologies, brings together physical and digital security technologies from each company to allow centralized visibility and control over disparate security elements to increase peace of mind.

Get started with Fortinet today: fortinet.com/solutions/industries/pharma

Resources

View the Intel security technologies infographic to learn more about Intel security technologies: intel.com/content/www/us/en/security/intel-security-technologies-infographic.html

Read more about the Intel value for security in lab and life sciences: intel.com/content/www/us/en/content-details/767654/content-details.html

Learn more about Fortinet Security Fabric and request a demo: fortinet.com/solutions/enterprise-midsize-business/security-fabric

[1] Cision PR Newswire. "Over 92% of Leading Pharmaceutical Companies Have Exposed Databases." Reposify. July 2021. prnewswire.com/news-releases/over-92-of-leading-pharmaceutical-companies-have-exposed-databases-301342820.html.
[2] Pharmaceutical Technology. "New report highlights pharma companies' vulnerability to cyberattacks." July 2021. pharmaceutical-technology.com/news/new-report-pharma-companies-cybersecurity/.
[3] Fortinet. "Top 5 Cybersecurity Threats and Challenges to Pharmaceutical Businesses for 2022." 2021. fortinet.com/content/dam/fortinet/assets/white-papers/wp-top-5-cybersecurity-threats-and-challenges-to-pharmaceutical.pdf.
[4] Fortinet. "Pharmaceutical Cybersecurity." Accessed May 2023. fortinet.com/solutions/industries/pharma.
[5] IDC. "The Business Value of Intel Security for PCs." Sponsored by Intel. March 2023. intel.com/content/www/us/en/architecture-and-technology/vpro/hardware-shield/business-value-security-for-pcs-whitepaper.html.
[6] Fortinet. "Next-Generation Firewall (NGFW)" web page. Accessed May 2023. fortinet.com/products/next-generation-firewall.
[7] Intel. "Get Outstanding Computational Performance without a Specialized Accelerator." July 2022. intel.com/content/www/us/en/architecture-and-technology/avx-512-solution-brief.html.
[8] Popat B. Mohite and Sachin V. Sangle. "Technology transfer in pharmaceutical industry – A Review." *International Journal of Advances in Pharmaceutics*. January 2017. https://core.ac.uk/download/pdf/335078031.pdf.
[9] Fortinet. FortiNAC Datasheet. April 2023. fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf.
[10] Fortinet. "Fortinet Fabric-Ready Technology Alliance Partner Program Hits New Milestone, Surpassing 500 Integrations." May 2022. fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortinet-fabric-ready-technology-alliance-partner-program-hits-new-milestone-surpassing-integrations.
[11] JDSupra. "European Court of Justice Clarifies Rules on Damages Compensation for GDPR Breaches." May 2023. jdsupra.com/legalnews/european-court-of-justice-clarifies-7120375/.
[12] Fortinet. FortiSIEM Datasheet. April 2023. fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf.
[13] Intel. "Intel® Secure Device Onboard." September 2017. intel.com/content/dam/www/public/us/en/documents/product-briefs/intel-secure-device-onboard-product-brief.pdf.

Printed in USA 0823/SD/PRW/PDF Please Recycle 355890-001US