WHITE PAPER

Securing the Pharmaceutical Industry With Secure SD-WAN

Executive Summary

The pharmaceutical industry is unique among enterprise organizations due to its need to maintain a complex set of connections across and between multiple sub-industries, all with varying business models, technology requirements, manufacturing, and supply chain needs. This includes universities and research centers, labs, manufacturing facilities, and even hospitals, pharmacies, healthcare centers, and clinics, especially during development phases such as clinical trials. Adding to this complexity is the need to maintain a high degree of security across these connections to protect highly coveted intellectual property and maintain the privacy of patients.

The numerous and vast touchpoints of the industry impose a constant state of vulnerability with the number of potential attack vectors constantly growing and changing. What all of the players in the pharma industry have in common is that they are a valuable target for cyber criminals to gain access to sensitive, extremely valuable information, such as secret formulas, patient and customer information, and scientific research. And unlike many other industries, cyber criminals in this space are often well-funded by competitors and nation-states looking to bypass the expense of research and development.

In addition to the complexities resulting from a sprawling infrastructure, there are three other characteristics that complicate the information security posture of leading pharma organizations: heterogeneity, agility, and culture.

Heterogeneity

Heterogeneity refers to the IT complexity caused mainly by mergers and acquisitions. Often, legacy IT assets remain operationally functional, even though they do not seamlessly interoperate with other segments of the network. A single merger between labs, for example, can double the number of security devices that need to be managed. And such complexity is a breeding ground for security gaps as users look for ways to navigate between the various systems to access the resources and build the workflows they need to do their jobs. This need to balance security with access can quickly overburden cybersecurity staff, and individual point security devices operating in a silo simply make it more difficult to secure the environment against quickly evolving threats. Pharmaceutical companies need security tools designed to communicate with one another so threats can be detected quickly, response times are shortened, and a reactive environment becomes proactive in hunting for and stopping threats in progress, or before they even begin.

Agility

Agility and flexibility are essential aspects of pharma organizations as they, for example, race to develop vaccines. With research, development, and commercialization happening at critical speeds, these organizations need to be able to function freely without boundaries or obstacles. Pharmaceutical companies need a unified security fabric built around common standards and open application programming interfaces (APIs) to extend visibility and control, and enable a common set of protocols spanning the entire distributed ecosystem.

Culture

The pharma culture relies on the sharing of data and resources, but it also needs to ensure that only the right people have the right access—it is both open access and stringently locked down. Pharma organizations need a security solution that has the agility and ability to handle both.

Spotlight on the Vaccine

Pharmaceutical companies continue to be in the spotlight since the onset of the COVID-19 pandemic, as all eyes have been looking to the most ingenious research organizations have undertaken to create and distribute a vaccine for the masses—as quickly as possible. The highly sensitive, extremely valuable information that is embedded in the process of developing a vaccine was a dangerous vulnerability for cyberattacks. In addition to securing this valuable information, pharma companies also had to contend with the full capabilities of nation-states or other pharmaceutical companies with state sponsorship looking to gain access to their research.

In fact, as the race to bring a coronavirus vaccine to market accelerated, threats increased in step. In July 2020, cybersecurity agencies and authorities in the United States, United Kingdom, and Canada released a joint warning of attacks targeting COVID-19 research and vaccine development facilities.[1] And any breaches or attacks could have caused delays in delivering vaccines, which could put millions of lives at risk.

In the United States, several government agencies joined forces early on to safeguard pharmaceutical companies that were developing a vaccine or that were integral to manufacturing and distribution once the vaccine was approved. Contaminated drugs, stolen intellectual property (IP), the need to repeat clinical trials, damaged reputation, downtime, litigation, and lost revenue were all important security concerns.

Today, vaccines have been successfully developed and are being administered globally. But in order to continue to defeat attacks aimed at the pharmaceutical industry, it is important to understand some of the top threats they face aside from those related to the pandemic.

In the race to create a COVID-19 vaccine by collaborating across the industry, pharmaceutical companies have exposed more threat surfaces than existed before the pandemic.[2]

Top Threats Pharmaceutical Organizations Face

1. **Too many endpoints**

   Pharma companies have many attack vectors because of digital innovation efforts as well as the rapid growth in Internet-of-Things (IoT) and Industrial-Internet-of-Things (IIoT) device integration into the network (via OT/IT convergence). This has caused the attack surface to grow exponentially. Cloud migrations, connected medicine and telehealth, remote workers, and clinics have all contributed to the proliferation of endpoints and have led to an increase in the number of ransomware and phishing attacks aimed at vulnerable pharma networks.

2. **Increasingly complex networks**

   Many pharma organizations have rapidly bolted on point security products to their networks to meet specific security or compliance requirements. However, these solutions are often not part of a cohesive security strategy. Consequently, a majority of these companies are now overtaxed with maintaining complex, disjointed security systems comprised of scores of isolated security tools. These fragmented, complex security systems cause a number of issues, such as:

   - **Lack of visibility:** Networks need transparency in order to detect and understand security events.
   - **No automation of threat response:** Attacks can occur in milliseconds, far faster than a human can detect and respond. Automated responses are immeasurably faster than manual fixes.
   - **Complicated compliance demonstration:** Maintaining compliance requirements can be prohibitively resource-intensive (including those of the World Health Organization, U.S. Food and Drug Administration, U.K. Medicines and Healthcare Products Regulatory Agency).
   - **Wasted IT resources:** Separately and manually managing all of the different security controls in place wastes valuable time and IT skills.

   Due to lack of connectivity and communication between these security solutions, threat response cannot be automated nor can it be timely. IT security teams need integrated solutions that are woven into the network infrastructure so the organization can be agile and flexible, enabling it to scale and keep up with digital innovation efforts. An integrated solution not only takes less precious IT resource time but also can be automated to a degree impossible to achieve using a traditional model.

3. **Distributed networks and acquisitions**

   Intellectual property, electronic protected health information (ePHI), and other sensitive medical and operational data is routinely accessed and transferred across pharma networks. Because their systems are disconnected, pharma enterprises struggle with visibility, data control, access auditing, and compliance reporting. Along with disconnected networks, mergers and acquisitions can cause additional security problems. Often the acquisition target does not possess adequate or easily integrated security infrastructures, further fragmenting the heterogeneous security architecture.

4. Threats from within

Damage from insider sources can be hard to detect and deter because they represent a wide range of behaviors and motives. It could be a disgruntled employee wanting to disrupt operations, a staff member trying to sell customer data, or a well-intentioned co-worker who accidentally sidesteps a company policy—or an overly complex security infrastructure—to save time.

Rather than try to solve each issue separately, pharma organizations should assess their current security systems and strive toward a comprehensive, integrated architectural approach to network security. Such an approach provides the visibility, automation, and responsiveness to threats that can also demonstrate compliance while defeating attackers.

53% of pharmaceutical IP thefts and related breaches are carried out by bad actors with insider access, according to the United Kingdom Office of Cyber Security and Information Assurance.[3]

Pharma Needs

More and more pharmaceutical organizations are moving a growing portion of their operations to the cloud to provide access to and collaboration with critical assets. They are also looking to be able to quickly scale, offer seamless connectivity, and expand compute and storage capabilities. They need to have unfettered access to critical trials data from participants using mobile devices to communicate, for example. The expansion of phones, tablets, wearables, and other IoT devices challenges pharma organizations to ensure the integrity and security of data arriving from these devices and endpoints. Pharma organizations need a unified security posture to protect this data.

The Ideal Security Model for the Pharmaceutical Industry

Connectivity, reliability, and resiliency

To secure the expanding network attack surfaces and simplify the vastly distributed network infrastructures of the pharma industry, pharmaceutical organizations need to unify and consolidate their security solutions. A secure software-defined wide-area networking (SD-WAN) solution addresses the issues of IoT sprawl and disconnectivity by integrating networking and security capabilities across the WAN edge, access layer, and endpoints. While most SD-WAN solutions leverage the corporate WAN as well as multi-cloud connectivity to deliver high-speed application performance at the WAN edge, few provide the security infrastructure needed to secure data in motion. A Secure SD-WAN model builds enterprise-grade security directly into the connection with firewalls and virtual private network (VPN) functions (and they can also include encryption, intrusion prevention system [IPS], antivirus [AV], and sandboxing). It offers intuitive orchestration and zero-touch deployments, saving precious pharma IT resource time. And single-source orchestration enables overlay (VPN) automation for the most complex network, with intuitive workflows to prioritize critical applications, and advanced networking capabilities to enable a self-healing WAN.

A true Secure SD-WAN solution tightly integrates networking, connectivity, and security functions into a unified platform to meet the full range of secure connectivity needs. This enables pharma IT security teams to consolidate essential functions into a unified location to respond more rapidly to any incidents.

Keeping Pharma Secure

The pharmaceutical industry faces a number of cybersecurity challenges and vulnerabilities, from network complexity and compliance to fortifying against and responding to ransomware and phishing attacks. A cohesive, unified architectural approach to network security provides the visibility, automation, and responsiveness required to thwart attacks and remain compliant.

A Secure SD-WAN solution can provide advanced visibility, security, and protection for today's vulnerable pharmaceutical networks. It allows pharma organizations to concentrate on lifesaving and life-enhancing pursuits, knowing that their networks and users are secure. Secure SD-WAN solutions are the prescription for fast, scalable, and flexible connectivity among all network environments, which is essential for all of the players in the pharma game.

[1] Derek B. Johnson, "U.S., U.K., Canada warn that Russian intelligence targeting COVID vaccine data," FCW, July 16, 2020.

[2] Louis Columbus, "10 Ways Covid-19 Vaccine Supply Chains Need To Be Protected By Cybersecurity," Forbes, January 24, 2021.

[3] Ibid.

March 23, 2021 5:48 AM

D:\Fortinet\2021 Rebranded templates\White paper\March\SD-WAN for Pharma\wp-securing-the-pharmaceutical-industry-V1-3232021\wp-securing-the-pharmaceutical-industry-V1-3232021

932508-0-0-EN