Akamai

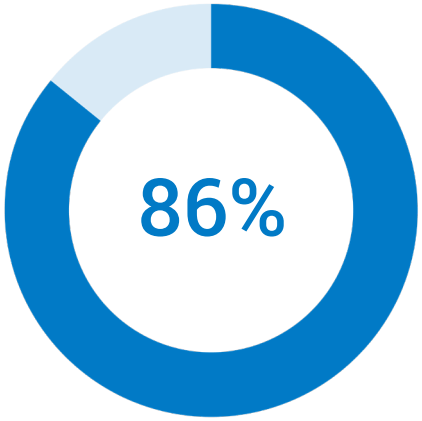
WHITE PAPER

6 Themes Driving Life Sciences IT Investment in EMEA

Innovation promises to accelerate R&D and testing — but requires complementary focus on cybersecurity and data protection

Executive summary

- This white paper highlights six key thematic areas that drive life sciences companies' investment in IT across Europe, the Middle East, and Africa (EMEA).
- Digital advances offer significant opportunities for life sciences companies, but the increased digital risk surface came at a cost: 86% of the Layer 7 distributed denial-of-service (DDoS) attacks seen on Akamai's platform from January 1, 2023, to March 31, 2024, were targeting pharmaceutical companies in EMEA.
- Life sciences companies are investing more in IT, making digital transformation a leading priority globally — yet, many companies are slow to adopt practices to prevent potential cyberthreats.
- The six themes driving life sciences IT investment are:
  1. Cloud hosting, big data, and analytics
  2. Artificial intelligence and machine learning
  3. Virtual care
  4. Mergers and acquisitions
  5. Blockchain and distributed databases
  6. Cybersecurity: Safety, compliance, and reputation
- Each of the six themes requires secure implementation, quality testing, and customer acceptance testing, in addition to following certain regulations to promote diligent protection.



86% of Layer 7 DDoS attacks on Akamai's platform targeted EMEA pharmaceutical companies

Addressing underinvestment in a high-risk environment

IT investment within the life sciences and the pharmaceutical industries is climbing. In 2024, 72% of pharmaceutical companies increased their IT budgets, driving an approximately 58% increase in revenue opportunity for the life sciences information and communications technology sector by 2028. These investments are driven by both trends and regulations, including precision medicine and legislation categorising life sciences companies as critical infrastructure. Although these factors are diverse, one pivotal priority unites them: the importance of investing in preventive cybersecurity measures. According to KPMG research, 75% of life sciences CEOs anticipate that cybercrime and cyber insecurity will likely have a negative impact on their organisation over the next three years.

However, despite this looming concern, cybersecurity needs are often overlooked or identified too late. Digital transformation strategies that don't incorporate cybersecurity investments often result in an increased budget strain down the line as companies contend with increased risk and costly cyberattacks.

Quantifying the threat, EMEA pharmaceutical companies made up 86% of Layer 7 DDoS attacks on Akamai's platform between January 1, 2023, and March 31, 2024. DDoS attacks, or other methods that result in downtime or operational standstill, are incredibly costly for pharmaceutical companies, as they may result in trial delays and damaged or spoiled medications, in addition to revenue loss.

The potential economic impacts of cyberattacks

Although a cybersecurity investment might not seem like an immediate concern, it can save organisations millions in cyber incident cleanup, downtime, and brand repair (Table 1).

Consequences of cyberattacks	Economic impact
Operational standstills	• Revenue loss • Trial/research delays
Data breaches	• Damaged brand reputation • Loss of patient and trial participant trust • Loss of intellectual property
Ransomware	• Ransom cost • Operational downtime
Defaced information	• Tainted or unreliable clinical trial data, which could cause incorrect care and delay European Medicines Agency (EMA) approval • Lost revenue from reduced patent protection • Loss of provider and patient trust for commercial products
Rebuilding systems after the attack	• Rebuilding costs and lost revenue due to operational standstill during rebuilds (if necessary)

Table 1: The potential economic impacts of the consequences of cyberattacks

Prioritising cybersecurity requirements alongside technical investment decisions is the best way to protect patient populations from cyberattacks.

The six themes driving life sciences IT investment

These are the six themes driving IT investment within life sciences and pharmaceuticals, along with best practices for pharmaceutical companies to optimise protection against cyberattacks.

Theme #1

Cloud hosting, big data, and analytics

Big data and analytics involves the deployment of scalable cloud computing with powerful analytic software to identify patterns in data and extract insights. It involves migrating core technologies and infrastructure from on-premises to the cloud, and using advanced tools and algorithms to run models to analyse the datasets and derive insights.

The benefits of cloud hosting, big data, and analytics for life science companies include:

- Shifting lumpy capital expenses to more predictable and dynamically scalable operating expenses by taking advantage of consumption-based pricing
- Shifting workloads closer to end users via distributed edge networks, which improves performance by reducing latency while also reducing cloud spend
- Increasing flexibility with multicloud and hybrid cloud infrastructures, enabling organisations to maintain benefits of legacy configurations while gaining new features and functionality
- Increasing log observability by using more performant and cost-effective tools that keep data warm while also reducing storage costs
- Automating and improving system scalability by using tools to automatically provision resources based on traffic spikes
- Shortening exploration cycles, leading to quicker discovery and distribution of new and more effective drugs
- Enhancing data management capabilities, especially when sharing data with third parties and collaborators
- Developing and distributing personalised (precision) medicine (e.g., genomics)

Theme #2

Artificial intelligence and machine learning

Artificial intelligence (AI) is the general ability of computers to emulate human thought and perform tasks in real-world environments, while machine learning (ML) refers to the technologies and algorithms that enable systems to identify patterns, make decisions, and improve themselves through experience and data.

These tools empower computers to develop intelligence to think and perform tasks like a human without human intervention. However, both AI and ML depend heavily on datasets, often sensitive (clinical, financial) or proprietary. As companies invest in AI/ML capabilities, they should conduct a parallel security review to ensure ongoing resilience. Finally, these implementations require a secure edge to ensure the investment is not stolen or abused.

The benefits of artificial intelligence and machine learning for pharmaceutical companies include:

- The ability to simulate drug and intervention interactions with synthetic patients, reducing research and development waste
- Improved participant profiling, discovery, and matching, expediting recruitment for clinical trials
- End-to-end evaluation of data related to supply chain and manufacturing, establishing baseline performance and identifying opportunities to streamline both manufacturing operations and shipping and delivery
- Enhanced conversational experiences via AI agents and chat models, reducing admin overhead while also providing patients or trial participants with 24/7 access

> **Investments in AI, cloud, and virtual care must go hand in hand with robust cybersecurity frameworks to be truly transformative.**

Theme #3

Virtual care

This theme includes decentralised clinical trials that are designed to be executed wherever the patients are physically located through a combination of remote patient monitoring and telehealth. It also includes wearables and remote patient-monitoring devices, which are tools worn by patients that collect and transmit key information. As with other key areas of investment, decentralising care comes with potential risks due to reduced "physical" visibility of patients, users, and data submitters. Life sciences companies taking advantage of the benefits of virtual and distributed care should also consider implementing elements of Zero Trust, such as multi-factor authentication, to secure their systems for access or engagement by authenticated and authorised users.

The benefits of virtual care for pharmaceutical companies include:

- Reduced costs to recruit and retain participants for clinical trials, and decreased clinical trial delays due to recruitment issues
- More diverse trial population due to easier trial access
- Decreased costs to execute clinical trials through telehealth
- More real-time communication and data collection from patients using commercial products, reducing time to clinician action, empowering patients to take control of their healthcare journey, and increasing potential medication efficacy

Theme #4

Mergers and acquisitions

This theme affects organisations that are merging with or acquiring other organisations to expand their market reach, increase the scope of offerings, and/or achieve economies of scale. These organisations must consolidate and reconcile technologies, users, and processes to successfully integrate. These efforts are highly prone to unintended risks and exposures due to the complex technical footprints created after the acquisition or merger.

Key areas of focus should be comprehensive visibility through a solution like microsegmentation (to achieve dynamic, software-based comprehensive visibility and resilience) in addition to continuous API monitoring and security. In the digital age, merging two companies often results in deprecating or sunsetting products and services, but the related APIs and microservices still must be monitored and secured, or be deprecated as well. With mixed teams and mixed systems, internal documentation consolidation may not be enough, and automated solutions for segmentation and API security reduce the potential for human error.

The benefits of mergers and acquisitions (M&A) for pharmaceutical companies include:

- The ability to realign or expand portfolios in response to strategic shifts (including pipeline replenishment of drugs that reach patent cliffs)
- The ability to acquire innovative technologies that complement an existing product portfolio or core competency
- Access to new and/or different markets
- Cost reduction synergies, including expertise in digital solutions

Theme #5

Blockchain and distributed databases

A blockchain is a digitally distributed, decentralised, public ledger that exists across a business network. In healthcare, it is used to preserve and exchange patient data through various systems and stakeholders. Blockchain has also been used to provide supply chain visibility into raw materials and APIs, as well as to verify authenticity and track pharmaceutical shipments.

While blockchain is one method of implementing distributed databases, other cloud- and edge-deployed alternatives exist that can achieve similar benefits. Healthcare is distributed, and technical implementations should be able to handle distributed performance and functionality at scale. Additionally, it is important to make sure the implementation is done with infrastructure that provides speed for performance and security for trust.

The benefits of blockchain for pharmaceutical companies include:

- Securing supply chains through increased transparency, reducing substandard, and/or outdated drugs
- Reducing counterfeit medicine through supply chain traceability
- Enhancing patient privacy and data protection during clinical trials
- Predicting and preventing drug shortages through visibility into APIs and raw materials

Theme #6

Cybersecurity: Safety, compliance, and reputation

Life sciences companies face a highly regulated environment in which noncompliance or poor investment across technical infrastructure, security, and organisational resilience can be costly in many ways. Service or supply chain disruption from cyber incidents can impact patient safety by delaying access to prescribed medicines or access to information. Additionally, Europe's regulatory environment emphasises data protection and critical infrastructure cybersecurity, so the life sciences industry is subject to some of the strictest regulations of any industry. Beyond safety and compliance, cyber incidents can cause damage to brands and to a company's reputation.

The benefits of investing in cybersecurity compliance include:

- Avoiding noncompliance fines of up to €15,000,000 or 2.5% of the global yearly revenue in the most severe cases for EU companies
- Reducing the risk of delays, which cost life sciences companies US$600,000 to US$8 million per day, and preventing impacts to clinical trial recruitment
- Preventing data breaches, which average a cost of US$5.1 million per incident in the life sciences industry

Cybersecurity is more than a theme, it is a foundational baseline for resilience in life sciences.

The importance of microsegmentation and API security

In traditional network security models, networks are usually divided into broad segments using network-based firewalls. While this approach provides a certain level of security, it lacks the granularity required to fully protect modern, distributed environments. In federal environments, network-based segmentation typically results in overprovisioning; that is, users and applications have access to more resources than they really need. This creates unintended opportunities for lateral movement. As attackers compromise one part of the network, they can move across to more sensitive areas with little resistance.

The concept of microsegmentation addresses this challenge by introducing fine-grained control over east-west traffic within the network. In a microsegmented environment, each application, workload, or service is isolated from others, and access is restricted based on specific policies. This ensures that users, devices, and applications can only communicate with the resources they are explicitly authorised to access. By implementing identity-based, application-aware segmentation, microsegmentation limits the potential damage from cyberattacks, reduces the attack surface, and enforces the principle of Zero Trust.

When it comes to north-south network traffic, federal networks increasingly rely on APIs to facilitate communication among systems. As a result, protecting API endpoints becomes a top priority. API attacks — including injection attacks, credential stuffing, and unauthorized data access — have increased sharply in recent years. Federal agencies and departments need comprehensive API security solutions that provide full lifecycle protection for APIs, enabling security personnel to discover, monitor, and secure their API traffic in real time. API discovery is especially important — it is not uncommon to have APIs that no one knows about.

A deeper dive into cybersecurity and compliance

Each cybersecurity-related regulation affects pharmaceutical investment across infrastructure, security, and resilience.

For most of Europe, EU regulations, such as the General Data Protection Regulation (GDPR) and the Cyber Resilience Act, set out specific and uniform standards for data infrastructure, security, and resilience. Another regulation, the EU AI Act, includes additional data infrastructure and security measures for companies that are exploring the use of AI applications. Every company doing business in the European Union must be in compliance with these regulations, and penalties are enforced by regulators in each member country in the same manner.

Beyond these regulations, the Network and Information Security Directive (NIS2) means that life sciences companies must check — and comply with — additional nation-by-nation standards for cybersecurity and resilience. Even countries not in the European Union — like the United Kingdom and Switzerland — have adopted similar policies for data protection and cybersecurity standardisation to sync business continuity and cross-border operations with the rest of the bloc.

Life sciences–specific cybersecurity regulations in Europe

Finally, many countries in Europe also have additional cybersecurity regulations for companies operating in the critical infrastructure or healthcare & life sciences sectors. These standards vary country to country, but are nonetheless crucial for compliance. Life sciences companies must determine whether these regulations apply to each country they operate in.

Table 2 shows the levels of cybersecurity laws and regulations that life sciences companies that do business in Europe must navigate.

EU cyber regulations (EU-wide standards)		
GDPR	EU AI Act	Cyber Resilience Act
EU cyber directives (Passed country by country in the European Union)		
NIS2		
Country laws (Passed by a single country)		
Cybersecurity laws (e.g., Denmark, United Kingdom)	Critical infrastructure laws (e.g., Germany)	Healthcare & life sciences laws (e.g., France, Switzerland)

Table 2: The cybersecurity laws and regulations that apply to life sciences companies in Europe

At each level, these policies require life sciences companies to meet standards for data infrastructure, security and privacy, and resilience and recovery. Each individual business must identify the right tools to protect strategic investments while staying in compliance.

Mapping cybersecurity measures and methods to areas of investment

Life sciences investments that result in technical advancements and modernisation, either to drive growth or in response to inorganic growth and M&A, have security implications that require proactive attention. Table 3 shows the cybersecurity capabilities that are most important for protecting the six pharmaceutical investment themes. Using proactivity as a guiding imperative, the table organises methods and measures into securing infrastructure, securing access, securing applications and APIs, and facilitating appropriate resourcing.

How to enhance protection	Areas of concentration
Securing infrastructure • Harden the outside of your infrastructure with a DDoS mitigation tool and a best-in-class web application firewall • Harden the inside of your infrastructure with a microsegmentation solution	• Cloud hosting, big data, and analytics • M&A • Virtual care
Securing access • Zero Trust Network Access • Multi-factor authentication to avoid account takeover • Secure web gateway	• Cloud hosting, big data, and analytics • Artificial intelligence and machine learning • Virtual care • M&A • Blockchain and distributed databases
Securing applications and APIs • Secure web applications and APIs to harden data and analytics outcome integrity • Analyse API traffic to identify behavioural anomalies and threat actors	• Cloud hosting, big data, and analytics • Artificial intelligence and machine learning • Virtual care • Cybersecurity: Safety, compliance, and reputation
Facilitating appropriate resourcing • Conduct scheduled threat hunts and red teaming • Prioritise partners with support models that match your organisation's capabilities; if your team is small, opt for full-service partners, as needed	• Cloud hosting, big data, and analytics • Artificial intelligence and machine learning • Virtual care • M&A • Blockchain and distributed databases

Table 3: The most important cybersecurity capabilities to enhance protection

Stay protected

Although this is a dynamic and innovative time for the pharmaceutical industry, many challenges still must be addressed. Healthcare is a prime target for cyberattacks, with pharmaceutical companies being no exception because of the high value of supply chain information, protected health information, and intellectual property (such as patents) that they hold.

The best way to stay on top of risks while investing in transformation is to work with a trusted leader in the healthcare cybersecurity space — from product, expertise, and resource perspectives — to adequately protect against potential cyberthreats amid technology advancements. Akamai is the cybersecurity and cloud computing company that powers and protects business online. Today, Akamai secures 8 of the top 10 pharmaceutical companies. Our market-leading security solutions, superior threat intelligence, and global operations team provide defence in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global pharmaceutical and life sciences enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence.

Contact Akamai for a deeper dive into the solutions that will protect the applications that drive your business at every point of interaction, without compromising performance or customer experience.