Security-as-a-Service for Life Science Companies

For the life sciences world, security and compliance concerns have become amplified by the shift toward a more distributed and home-based workforce. Threat sophistication is increasing rapidly, and use of cloud-based services spreads valuable intellectual property across multiple places. The front-line of protection has moved from the perimeter of your network to the devices and identity of each user, wherever they may be.

With security and compliance moving to the forefront, compliance requirements such as HIPAA and HITRUST and industry frameworks such as CIS and NIST are increasingly important for customers, partners, investors, and regulators. Industry best practices for security are no longer optional; they're requirements for doing business in the modern world. Failing to measure up can cost you customers, partners and credibility in the market.

The Best Approach for Life Science Companies

To meet the security challenges of today and tomorrow, life science IT managers are shifting to centrally-managed tools and skills. Identity and access management, endpoint management, and AI-powered endpoint protection are becoming a vital part of the security landscape, in addition to all the traditional network protections. There are hundreds of different solutions for companies of different sizes and levels of sophistication, the best of which are cloud-based to maintain high availability for distributed workforces. For the foreseeable future, most solutions will be constantly updated to meet the ever-evolving threats.

In addition to tools and services, the life sciences world needs leaders with detailed knowledge of security and compliance requirements, credible industry certifications, and experience working in life science industries specifically. All of these qualities must also be intertwined with basic IT solutions such as firewalls, wireless networks, back-ups and disaster recovery. It's not enough to simply audit and identify problems. Life science IT security leadership needs to understand how to specify and implement solutions and manage an ongoing security plan, all while managing the fabric of interrelated requirements and solutions.

KalioTek's virtual team provides all the combined capabilities needed to build and maintain secure, compliant, and operationally sound IT environments for emerging and midsize life science companies. Every team is led by a Security Manager who has the appropriate security certifications (e.g. CISSP, CISA, CISM, CCSP, SSCP) and many years' experience working with similar life science companies. Your organization can benefit from their experience and knowledge at a fraction of the cost of hiring this role full time. If your company already has a Chief Information Security Officer (CISO), either as a full-time employee or consultant, KalioTek can provide the technical team and toolset to execute their plans. We've served hundreds of companies over the last 20 years, many all the way from startup to IPO or acquisition by major industry titans. The team scales with you for each phase of growth, providing the necessary capabilities at an affordable price.

Security Manager as a Consultant

Every company's security program is completely unique to them. The Security Manager works directly with the client to establish priorities, report progress against plan and resolve issues. To track progress, the team establishes a customized dashboard or reporting format. These duties tend to grow over time as the company grows and the environment becomes more complex, but the cost remains significantly lower than a full-time Security Director. We leverage our full team's expertise, and our work with many similar clients allows us to perform these duties efficiently.

Initially, time must be spent developing security policies (Information Security, Acceptable Use, IT policies, etc.), so we provide templates and recommendations to accelerate development. Policies are necessary to maintain any kind of compliance and make scaling and employee implementation much easier. In the event of a breach or compliance review, the first thing auditors or investigators will ask for is your security policies. Your policies are much more than simple exercises. They involve controversial decisions such as whether or not to give users admin access to their devices, acceptable hardware and software, use of cloud services, accessing corporate systems from home computers, telecommuting policies, and much more. Security threats and computing environments are constantly changing. Policies must evolve to continually be effective.

Next, we jointly select a security framework (CIS, NIST, ISO 27001, etc.) for our baseline. KalioTek uses the Center for Internet Security (CIS) framework for our default baseline. Sometimes companies prefer other frameworks based on their compliance path, and we are happy to work with them to achieve their goals on their chosen framework.

KalioTek's Security Operations in Action

After policies are set, we begin to monitor and enforce good Cyber Hygiene. Cyber Hygiene practices typically require minimal effort at first, but the effort increases over time as more users and systems are added. Centrally-managed tools are an efficient way to enforce and track compliance, but their results require analysis and action to mitigate risks. Some of the questions addressed in Cyber Hygiene are:

- Are there new unauthorized hardware and software on the network (CIS #1 and #2 sources of data breaches)?
- Are user machines and servers being backed up as intended?
- Do the firewall, networking equipment, servers, and user machines all have the necessary security patches?
- Are anti-virus/endpoint protection tools enabled and updated on user machines?
- Is encryption enabled on machines?
- Are users receiving the "least privilege" required for their roles?
- Evolution of privileges for security groups is managed here.
- Periodic security scans produce reports with issues with different levels of urgency.
- These need to be evaluated and acted upon.
- Do cloud environments being used to share data with employees, partners and customers have the proper permission settings?
- These require constant maintenance to ensure that users have the proper access.
- Do users have inappropriate access to admin rights on their machines?
- Do all employees receive annual security awareness training?
- Are anti-phishing exercises conducted to identify users that need more training?
- Is the output from all security tools analyzed methodically?
- Do you block IPs or even countries being used to attack assets?

Over time new security tools will appear and become relevant. The Security Manager can assist with assessing the company's needs, make recommendations, and evaluate providers and manage implementation projects.

Frequently, customers and partners now ask providers to fill out security questionnaires and sign agreements, such as Business Associate Agreements required for HIPAA compliance. In the event of an audit or formal compliance assessment, a project may need to be declared to demonstrate compliance, answer questions, write responses, etc. The KalioTek team will be responsible for completing these duties and interacting with the 3rd party on any questions and concerns. In our experience it is often major customers or sales opportunities that drive the urgency. It can be very difficult to meet required timelines if substantive work has not already been completed.

KalioTek's Security-as-a-Service offering scales with the company, providing appropriate guidance and capacity for each phase of growth. If and when the company requires a full time Security Manager, KalioTek will transition responsibilities and provide support on an as-needed basis.

About KalioTek

KalioTek's mission is to provide emerging and midsize life sciences companies with a wide range of IT and security expertise in a flexible, affordable model. Since 2002 our team has provided consulting and managed services to hundreds of ambitious companies. Our technically-savvy client base requires that we stay on top of IT and security technologies as they evolve and understand the solutions appropriate for growing life sciences organizations.

For more information or to inquire about how KalioTek can help your company with some of the solutions described above, contact us at 408.550.8007 or sales@kaliotek.com.