Top 7 Security Recommendations

Follow the 80/20 rule and a practical, prioritized approach to security and regulatory compliance.

If there's one constant from the world of IT security, it's this: the threats of widespread security breaches have never been higher than they are right now. Remote workers are increasing in number, increasing the potential cyberattack surface, and simultaneously, cyberattacks are growing more advanced by the day. All organizations face increasingly stringent requirements in order to protect IP and meet compliance standards such as HIPAA, GDPR and CCPA. Additionally, customers and partners need assurance that your security practices are ready to meet the challenges of global cyber security threats. The only way to remain protected is by continually reviewing and updating your security tools and practices, but for emerging companies, that's a tall order.

There are thousands of security solutions targeting different market tiers, complexity and price points. So which solutions are right for your company? AND, what's the most important now? What's the right implementation order? Industry frameworks such as NIST and COBIT give a comprehensive set of requirements that can be overwhelming to midsize organizations with limited resources.

A practical, prioritized roadmap with right-sized solutions has become a necessity.

With 20 years of experience assisting emerging and midsize life science organizations with security and IT, KalioTek has a deep understanding of right-sized security solutions and prioritization. We've found that with the right guidance, it's possible to cover the top 80% of risks at 20% of the cost and effort. Every year, we reevaluate solutions available in the market to update our recommendations.

Unlike productivity or business process applications which can be "good enough", we recommend that companies buy market-leading security products when possible. Last year's protection doesn't help when you are facing this year's threats, which have the potential to derail your entire business. Great capabilities, formerly available only to large enterprises, are now available at reasonable costs, and we can help you implement them.

Here are some of the most important technologies we recommend.

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 4340 Stevens Creek Blvd #250 • San Jose, CA 95129

KalioTek™

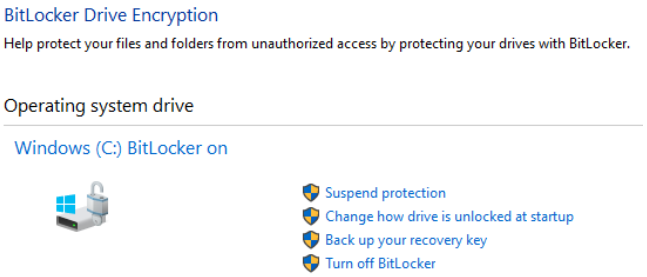
Here are some of our highest priorities for addressing cybersecurity threats

1 Encrypt your data!

It's your easiest get-out-of-jail-free card in the event of a breach: showing that you have taken the first and most obvious step to protect sensitive data. While data encryption tools are readily available from Microsoft, Apple and others, you'll need to be able to verify that everything is encrypted. If sensitive data is scattered across remote employee laptops and cloud services, this would be a good time to organize it and manage permissions centrally. More later on verifying encryption.

Key Benefits

- Protect against breach from accidental loss of equipment containing sensitive data
- Prevent attackers from reading your sensitive data in transit or on the network
- Required for HIPAA compliance
- Protect your enterprise value by protecting your intellectual property

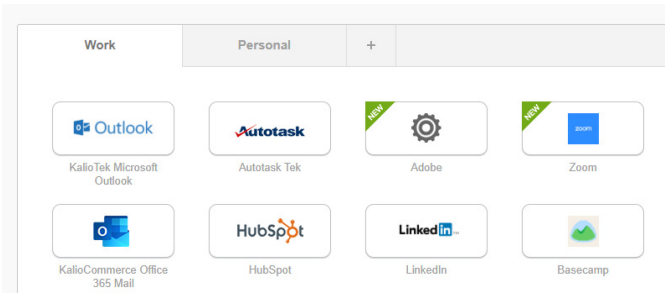


2 Single Sign-On (with Multi-Factor Authentication)

Your next most critical threat is compromise of your employees' login credentials to the dozens of systems most people now have access to. It is by far the hacker's most common point of entry into company networks. Managing individual logins and passwords to numerous systems is almost certain to lead to compromises, given the rise of sophisticated phishing schemes to steal them. Integrating these into a single, secure system allows employees to access authorized applications with a single login, protected by multi-factor authentication. SSO also speeds onboarding and terminations and provides a handy audit trail of access rights. The leading SSO solutions have hundreds of secure, pre-built integrations with other applications to help speed your implementation. We highly recommend taking this step as early as possible, as implementation just gets harder as your headcount and number of applications grows.

Key Benefits

- Protect employee credentials from being compromised
- Eliminate headache of managing many logins
- Streamline onboarding and termination processes
- Provides an audit trail of system permissions



Single Click login to all authorized applications

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 4340 Stevens Creek Blvd #250 • San Jose, CA 95129

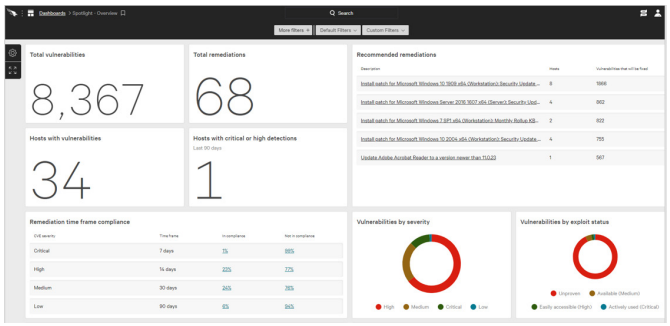
KalioTek™

3 Endpoint Detection and Response (the new antivirus)

Last decade's antivirus solutions that only operate on individual devices don't cut it anymore. Integrating real-time intelligence from endpoint, network, and application threats allows the solution to identify and respond to complex threat behaviors instead of just individual events. Analytics help identify root causes and understand the actions needed to remediate them. This technology is relatively new, but choosing a leading provider will put you on the right path to counter evolving threats for years to come.

Key Benefits

- Real-time protection from Viruses, Malware, Ransomware and Phishing attacks
- Recognizes patterns of attack across multiple devices
- Provides remote and on-premise workers with a single integrated layer of protection
- Backed by 24x7 security operations center (SOC) to rapidly counter emerging threats



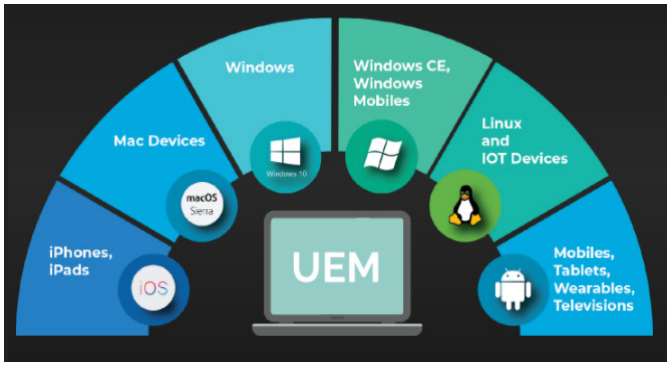
Centralized threat visibility and protection for all network and end user devices, remote & local

4 Unified Endpoint Management

Remote work is here to stay, leaving employees outside the company firewall and the visibility and control of company IT. Remote computers and phones with company data are more vulnerable than onsite devices. UEM gives you visibility into the state of all user devices and allows you to centrally manage them to an extent not possible in the past, granting conditional access at a granular level and enabling remote lock remote wipe, separation of personal data vs. corporate data, the prevention of sensitive data from leaving the device/network, security patches, etc. You can also validate that the device's data is encrypted and backed up. All this is great for demonstrating compliance as well as peace of mind. In our world of distributed, mobile employees, strong endpoint management is now a must for any well-managed IT environment.

Key Benefits

- Real-time inventory of all hardware and software assets, remote or local
- Monitor and enforce patching, encryption, backup and required security setup
- Remotely install new applications
- Remote lock and wipe when equipment is lost or stolen
- Granular, device-level permissions to systems and data
- Data Loss Protection



(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 4340 Stevens Creek Blvd #250 • San Jose, CA 95129

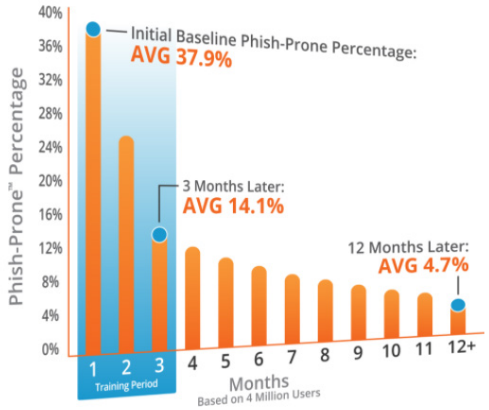
KalioTek™

5 Security Awareness Training and Automation

All of our security technologies notwithstanding, human error is still the weakest link. Compliance regimes require that we train employees on security awareness at least yearly. Now new, inexpensive automated systems are streamlining the process. They train employees on the latest techniques hackers use to fool them and track their completion for review. Then, they send simulated phishing attacks (the most common form) to test users' skills and identify those in need of additional attention. Just knowing that tests will be coming commands users' attention and brings security awareness to the forefront.

Key Benefits

- Updated, professional security awareness training
- Required for compliance
- Automated tests probe user behavior and identify weak spots



Train, then test your employees' comprehension of security best practices

6 SIEM (Security Information and Event Management)

Security is shifting from "incident response" to "continuous response". SIEM systems consolidate, analyze, and store the logs from all network devices. You'll need these for forensics in case of any breach. As the logs are collected, they are analyzed for threat signatures and suspicious behaviors, creating alerts for threats and recommending actions to plug vulnerabilities. Automated technology certainly plays an important role, but constant monitoring by security professionals is still necessary. SIEM solutions are often backed by security operations centers (SOC) staffed 24x7 with qualified security engineers. The service provider model has recently evolved to make these enterprise-grade capabilities available to midsize companies at reasonable costs.

Key Benefits

- 24 X 7 comprehensive threat monitoring from all devices
- Alerting and escalation for high priority events
- Ongoing vulnerability reports and recommendations
- Log storage and management, as required for compliance

Continuous monitoring and alerting for system-wide security events

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 4340 Stevens Creek Blvd #250 • San Jose, CA 95129

KalioTek™

7 Verify Security of Vendors and Partners

Today's enterprises are comprised of tightly-connected supply chains of data, software, and services. HIPAA and other compliance regimes require that affiliated entities with access to your data or systems have robust security practices and are aligned with your compliance obligations. They are required to verify their security policies and practices, the systems and data used to support your business, cyber insurance coverage, compliance assessments they have performed, and any security breaches they have experienced.

Key Benefits

- Fulfills compliance requirements for HIPPA and other regulatory regimens
- Communicates to vendors and partners that you take security seriously
- Gives you recourse in the event of security breaches caused by affiliated parties

HIPAA Business Associate Agreement between Covered Entity and Business Associate
(Compliance with Privacy and Security Rules)

This HIPAA Business Associate Agreement (*Agreement*) is between _____ _____ ***(Name of Covered Entity)*** of _____ _____ ***(street address, city, county, state, zip code)***, hereinafter referred to as the ***Covered Entity***, and _____ ***(Name of Business Associate)***, hereinafter referred to a ***Business Associate***, located at _____ _____ ***(street address, city, county, state, zip code)***, and includes all office locations and other business locations at which *Business Associate* data may be used or maintained. *Covered Entity* and *Business Associate* may be referred to herein individually as *Party* or collectively as *Parties*.

Business Associate Agreements or Cyber Security Risk Questionnaires Align Security Concerns with Affiliates

About KalioTek

KalioTek's mission is to partner with growing life sciences organizations to provide access to a wide range of IT and security expertise in a flexible, as-needed, and affordable model. Since 2002, our team has served hundreds of emerging and midsize companies. Our client base requires that we stay on top of IT and security technologies as they evolve and understand the solutions that are appropriate for this specific market.

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.

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 4340 Stevens Creek Blvd #250 • San Jose, CA 95129

KalioTek™