KPMG CYLANCE

Proactively guard enterprise endpoints

CylancePROTECT with KPMG Cyber Security Services

There is a new headline every day about a company falling victim to a new cyberattack. Whether the end goal is to use a company's resources to mine cryptocurrency, extort it with ransomware, steal customer and employee information for profit, infiltrate their network to steal intellectual property, or outright destroy their enterprise infrastructure, modern attackers are using next-generation tools, techniques, and procedures that easily bypass current state enterprise defenses. Most often, the attack begins by targeting the most vulnerable layer of defense, the end user (i.e., the endpoint). The current era requires a new approach that leverages advanced technology and services based on artificial intelligence (AI) to help you proactively protect your enterprise endpoints.

A new approach to endpoint security

Cybersecurity leaders carry a heavy burden. They deal with relentless attacks and assaults on endpoints in a rapidly evolving threat landscape that includes cryptojacking, ransomware, and zero-day attacks. Constant phishing attacks attempt to trick unwary users into clicking a link or opening an attachment. The security team must provide enterprise-wide protection of infrastructure and services by monitoring attacks and detecting intrusions. In addition, they help ensure the enterprise is compliant with regulations such as the European Union's General Data Protection Regulation (GDPR) and the United States' Sarbanes-Oxley legislation. If data theft does occur due to an intrusion, these leaders are on the hook to manage the impact to the company's bottom line and reputation when it is made public. And all this must be done while operating under the constraints of a historic shortage of cybersecurity talent.

Compounding these stresses, the traditional antivirus software deployed by most companies to protect infrastructure and data at the endpoint uses reactive prevention methods that only work if attacks are known and familiar, meaning systems must suffer a breach or exposure before that attack can be identified and stopped. Even the most advanced techniques of signature-based detection, exploit prevention, whitelisting, and application controls all fall into a victim-first model. Clearly, from all the cyber breach news making the daily headlines, this reactive approach is no longer viable.

AI and machine learning (ML) have had a revolutionary impact in their application-to-endpoint protection. Through their alliance, KPMG and Cylance are able to assist security professionals in better guarding enterprise endpoints with the latest in machine-learning-based endpoint security technologies. The experience and coverage of KPMG Cyber Security Services teams coupled with Cylance's powerful endpoint protection platform (EPP) and endpoint detection and response (EDR) solutions provide the services and technologies that help enable security teams to prevent, not merely respond to, rapidly evolving attacks from adversaries. Even better, KPMG and Cylance can help achieve these security enhancements while also reducing costs and providing a rapid return on investment.

KPMG: In-depth cybersecurity know-how

Professionals in KPMG's Cyber Security Services practice possess the business acumen, technological insights, and industry knowledge to guide enterprises through strategy and governance, organizational transformation, cyber defense, and response. With skilled security specialists around the world, KPMG can recommend and implement solutions that provide ongoing integrity, availability, and protection of the most sensitive enterprise data assets.

Through its alliance with Cylance, KPMG adds advanced, AI-enabled endpoint security technology to its complete portfolio of security transformation, strategy, and road map services. These specific technical capabilities for EPP and EDR requirements can help companies prevent attacks before they occur. At a time when cybersecurity specialists are in short supply, KPMG professionals can help companies enhance cybersecurity programs, use AI to detect network intrusion or anomalies, provide greater insight into networks with data and analytics, integrate endpoint technology with compliance requirements, and align organizations to prevent, and if necessary, to rapidly respond to and remediate a breach.

Cylance: Proactive endpoint protection

Cylance uses AI to deliver prevention-first, predictive security products and specialized services that change how organizations approach endpoint security. Cylance's security solutions combine AI-driven predictive prevention with dynamic threat detection and response to deliver consistent protection and visibility across the enterprise.

Cylance's integrated, threat prevention software and services include:

— **CylancePROTECT®** delivers industry-leading malware prevention powered by artificial intelligence, combined with application and script control, memory protection, and device policy enforcement to prevent successful cyberattacks. Without the use of signatures or the need to stream data to the cloud, CylancePROTECT delivers protection against common threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and many other attack vectors, no matter where the endpoint resides.

— **CylanceOPTICS™** is an AI-driven endpoint detection and response component providing consistent endpoint visibility, root-cause analysis, scalable threat hunting, and automated threat detection and response. Augmenting CylancePROTECT prevention, CylanceOPTICS focuses on automatically detecting and responding to hard-to-find threats across the enterprise. CylanceOPTICS is designed to automate the threat detection and response tasks using existing resources, reducing the workload on security analysts without increasing costs.

— **ThreatZERO™** Services provided by KPMG's Cyber Security Services specialists, in concert with the Cylance team, provide a distinct mix of technological know-how and personalized white glove service to enhance CylancePROTECT and CylanceOPTICS and move environments into prevention while providing measurable results of progress throughout the process.

Qualifying questions

Consider these questions when evaluating EPP and EDR solutions:

— Is the solution capable of protecting against the next generation of external and internal threats?

— Does it protect your endpoints from unknown threats or threats that do not yet exist?

— Does it leverage AI and ML to protect your enterprise endpoints?

— Does the solution have a cloud-based infrastructure for simplified deployment, monitoring, and remediation?

— Will it quickly allow you to have greater insight into your enterprise and be able to quickly respond to incidents should they occur, regardless of physical location?

Software and services that transform endpoint security

Deploying Cylance's security solutions in conjunction with KPMG's Cyber Security Services can help organizations optimize their endpoint security environment. KPMG professionals can help assess environments to strategize efficient and effective deployment of Cylance's security solutions and configure CylancePROTECT and CylanceOPTICS for distinct requirements. Combining KPMG's experience with Cylance's AI and ML provides a platform for identifying and managing the presence of compromises and sophisticated threat actors to ultimately achieve a state of prevention.

The services and technology combined in this alliance can help companies with:

- **Endpoint protection and threat prevention:** Use advanced AI and ML technology to instantly identify, detect, and protect the most vulnerable facet of enterprise networks, the endpoint
- **Rapid incident response:** Quickly deploy an AI-driven, cloud-based EDR solution to rapidly respond to incidents regardless of network size or endpoint location
- **Compromise assessments:** Generate deeper insight into enterprise networks through advanced data and analytics to rapidly detect compromises and intrusions
- **GDPR compliance:** Help ensure the integrity and confidentiality of sensitive data
- **Cyber due diligence:** Every merger, acquisition, and/or divestiture should include a cybersecurity posture assessment that thoroughly and efficiently completes cyber due diligence to identify and remediate any gaps that could have significant impact on a deal
- **Third-party risk assessments:** Help ensure that critical third parties that access your network are clean and free of malware
- **Managed response services:** Provide support for endpoint protection, including strategy, implementation, monitoring, response, and reporting.

Have confidence in endpoint security solutions

With services to efficiently deploy, monitor, and respond with CylancePROTECT and CylanceOPTICS within distinct security environments, the KPMG and Cylance alliance delivers a modern approach to security that:

- Provides AI and ML technology to proactively protect data and systems without inhibiting performance
- Delivers real-time analytics on endpoints to provide greater insight into corporate networks
- Offers cost savings and strategic value such as freeing IT security professionals to work on long-term projects instead of constantly responding to reactive alerts.

Together, KPMG and Cylance can increase your confidence in your company's endpoint security.

Contact us

Edward Goings
Principal, Cyber Security
T: 312-925-8547
E: egoings@kpmg.com

David Shin
Director, Advisory
T: 323-445-8848
E: dhshin@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.