Frequently Asked Questions

Cylance®

What Is Cylance?

Cylance is a cybersecurity company headquartered in Irvine, California. Cylance's mission is to protect everyone under the sun. Cylance leverages artificial intelligence, mathematics, and machine learning to prevent threats from ever causing harm.

What Is Cylance's Elevator Pitch?

Cylance is revolutionizing cybersecurity with products and services that proactively prevent the execution of advanced persistent threats and malware at the endpoint, enabling a level of security that far exceeds the effectiveness of current industry solutions deployed throughout enterprises, government, and institutions worldwide.

When and Where Was Cylance founded?

Cylance was founded in June of 2012 in Irvine, California.

Who Are Cylance's Founders?

Stuart McClure, former Worldwide CTO of McAfee/Intel Security, and Ryan Permeh, former Chief Scientist of McAfee/Intel Security.

Is Cylance a Private or a Public Company?

Cylance is a venture capital funded private corporation. To date Cylance has raised $177M across four rounds of funding led by Blackstone, Khosla Ventures, Fairhaven Capital, Dell Ventures, DFJ, KKR, Capital One Ventures, Ten Eleven Ventures, and several other firms.

Who Are Cylance's Clients?

Cylance has thousands of clients, including several Fortune 100 organizations, and the company's technology protects millions of endpoints worldwide.

In Which Verticals Does Cylance Operate?

Cylance's products and services work well in any industry that is determined to lower risk and protect its endpoints. Cylance's greatest adoption rates to date occur in oil, gas, energy, critical infrastructure, finance, healthcare, retail, transportation, heavy manufacturing, and defense.

In Which Locations Does Cylance Operate?

Cylance operates globally from its headquarters in Irvine, California, as well as regional offices throughout the U.S. and around the globe.

CylancePROTECT®

What Is CylancePROTECT?

CylancePROTECT is an advanced threat prevention product that sits on each endpoint (desktop, laptop, mobile devices, server, or virtual machine) within an organization. It applies artificial intelligence and machine learning to instantly identify and prevent malware and cyberattacks from ever executing on the host machine.

How Does CylancePROTECT Work?

CylancePROTECT is a small, lightweight software agent that is deployed to every endpoint in an organization to prevent cyberattacks on the operating system and in memory. Prior to any binary being executed on the host, CylancePROTECT uses static analysis and predictive modeling to determine if the binary contains malicious features. If deemed a threat, local host policy takes action to alert, notify, and/or quarantine the object.

In addition, CylancePROTECT Script Control lets customers know in real time when a script is about to run and provides the ability to quickly allow or deny reviewed scripts. When deployed on servers, CylancePROTECT's Memory Protection prevents the exploitation of many of the most common classes of vulnerabilities, such as exploits for buffer overflows. As an add-on to CylancePROTECT, CylanceOPTICS™ provides full clarity into any attack that has been attempted, including insight into what malware is in an environment, where it came from, who put it there, when it first showed up, and how it got there.

How Is Cylance's Approach To Endpoint Protection Different from the Rest of the Cybersecurity Industry?

Cylance takes a non-signature, non-heuristic approach to malware detection. All of our detections are predictive and preventive in nature. Legacy endpoint protection and antivirus vendors rely on outdated methods for malware detection using signatures, behavioral analysis, sandboxing, micro-virtualization, and cloud lookups to virus definition databases. All of these approaches are no longer viable in today's threat landscape.

How Does Cylance Prove Its Efficacy in the Real World?

Cylance conducts numerous public, real-world cyberattack tests of our CylancePROTECT product in major markets around the globe. In our testing, we demonstrate the efficacy of CylancePROTECT live using zero-day malware and the latest threats — many of which were first seen less than 24 hours before our demo.

Can CylancePROTECT Replace Existing Antivirus and Endpoint Protection?

Yes. CylancePROTECT is PCI-DSS section 5.0 compliant, HIPAA antivirus compliant, a member of the Microsoft Virus Initiative, and recognized by Microsoft as an antivirus product. CylancePROTECT can entirely replace an existing legacy AV solution or work together with any existing solutions in your environment.

What Is the Performance Impact of CylancePROTECT?

Very minimal — CylancePROTECT does not sit and scan continuously like traditional solutions. In testing, CylancePROTECT uses less than 1% of a typical desktop CPU and less than 60MB of memory.

On Which Operating Systems Does CylancePROTECT Run?

- Windows XP SP3
- Windows Vista
- Windows 7 (32-bit or 64-bit)
- Windows 8 and 8.1 (32-bit or 64-bit)
- Windows 10 (32-bit or 64-bit)
- Windows Server 2003 SP2
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2
- Windows Server 2016
- Mac OS X Mavericks*
- Mac OS X Yosemite*
- Mac OS X El Capitan*
- macOS Sierra*

*Complements Apple's built-in XProtect

- Linux RHEL/CentOS 6.6 (32-bit and 64-bit)
- Linux RHEL/CentOS 6.7 (32-bit and 64-bit)
- Linux RHEL/CentOS 6.8 (32-bit and 64-bit)
- Linux RHEL/CentOS 7.0 (64-bit)
- Linux RHEL/CentOS 7.1 (64-bit)
- Linux RHEL/CentOS 7.2 (64-bit)
- Linux RHEL/CentOS 7.3 (64-bit)

Does CylancePROTECT Require an 'Always On' Internet Connection?

No. CylancePROTECT was designed with sensitive and air-gapped environments in mind. The CylancePROTECT agent runs entirely on the host endpoint and requires no outside Internet connection to predict and prevent malware from executing.

How Is CylancePROTECT Managed and Deployed?

CylancePROTECT has an easy-to-use web console to handle alerts, zone and policy management, and reporting. Endpoint agents report into the console only for policy and occasional updates. The CylancePROTECT agent does not require an Internet connection to provide protection to the endpoint itself. CylancePROTECT can be easily integrated into any of the top SIEM solutions via REST API, including native integration with Splunk. CylancePROTECT is delivered as a standard MSI and is deployed the same way an organization deploys any other type of software.

Cylance Artificial Intelligence and Machine Learning

Why Does Cylance Use Artificial Intelligence (AI) and Machine Learning?

AI and machine learning allow Cylance to build mathematically sound relationships between features and correlate seemingly disparate features far beyond human ability. Both disciplines are proven to be more powerful, efficient, and accurate than any human or semi-automatic approach to cybersecurity. Using this approach allows Cylance to quickly build highly accurate predictive models that enable our endpoint agent to make autonomous, intelligent decisions on file binaries before the files are able to execute.

How Accurate Is This Approach?

Extremely accurate — computers are designed to enable very complex processing in real time. Cylance's application of machine learning eliminates concern over false positives and negatives. In live demonstrations, CylancePROTECT displays a threat detection accuracy of over 99% and a false positive rate of less than .0002%.

Are False Positives an Issue?

In all types of malware detection, false positives are a concern — including malware detection done entirely by humans. We specifically optimize our solution to obtain the lowest possible false positive ratio. Our rates are lower than traditional antivirus vendors. Additionally, a false positive is a minor issue compared to a successful malware attack.

Is AI Effective for Cybersecurity?

Yes. Artificial intelligence is a broad field of study with a myriad of theoretical and practical applications. The most important considerations when attempting to use artificial intelligence and machine learning to solve complex problems are the scale of the supporting infrastructure, the talent and creativity of the data science team attached to the project, the ability to engineer new and exotic features to create a self-learning environment, and the boldness to experiment with new and unexpected techniques.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

Have Other Cybersecurity Companies Attempted To Use AI and Machine Learning?

Several other cybersecurity companies have attempted to use artificial intelligence and machine learning but many have been plagued by high false-positives and lack direction when it comes to identifying what problems to solve. While several other organizations have attempted to use machine learning to isolate post-attack anomalous behaviors and events, Cylance has instead built a system to classify and learn how malicious files operate to prevent them from executing.

Is Cylance Just Another Antivirus Vendor?

Cylance's revolutionary approach is redefining endpoint security to be proactive and preventive instead of reactive. Traditional antivirus technology based on signatures is outdated. Cylance has built a solution that does not require any previous knowledge about a malicious binary file in order to identify its intention.

Additional Cylance Offerings

Does Cylance Offer Consulting Services?

Cylance's products are complemented by a full suite of consulting services that combine deep domain expertise with an innovative, artificial intelligence and machine learning based approach to endpoint protection. Among these services are compromise assessments, penetration testing, emergency incident response, training, and staff augmentations.

Cylance's ThreatZERO™ Services optimize operationalization of Cylance products, expediting deployment, mitigating risk immediately, providing immediate ROI, and bringing clients to a state of zero active threats. The Cylance Consulting team offers industry-specific services, such as the Industrial Control Systems Application Penetration Test, which assesses the security of ICS and human machine interface applications, and Med Secure Assessment Framework, which helps healthcare organizations quantify the security risk posed by non-traditional connected assets such as medical devices. The group also specializes in critical infrastructure and key resources protection activities for government entities and select industries.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20171205-1907