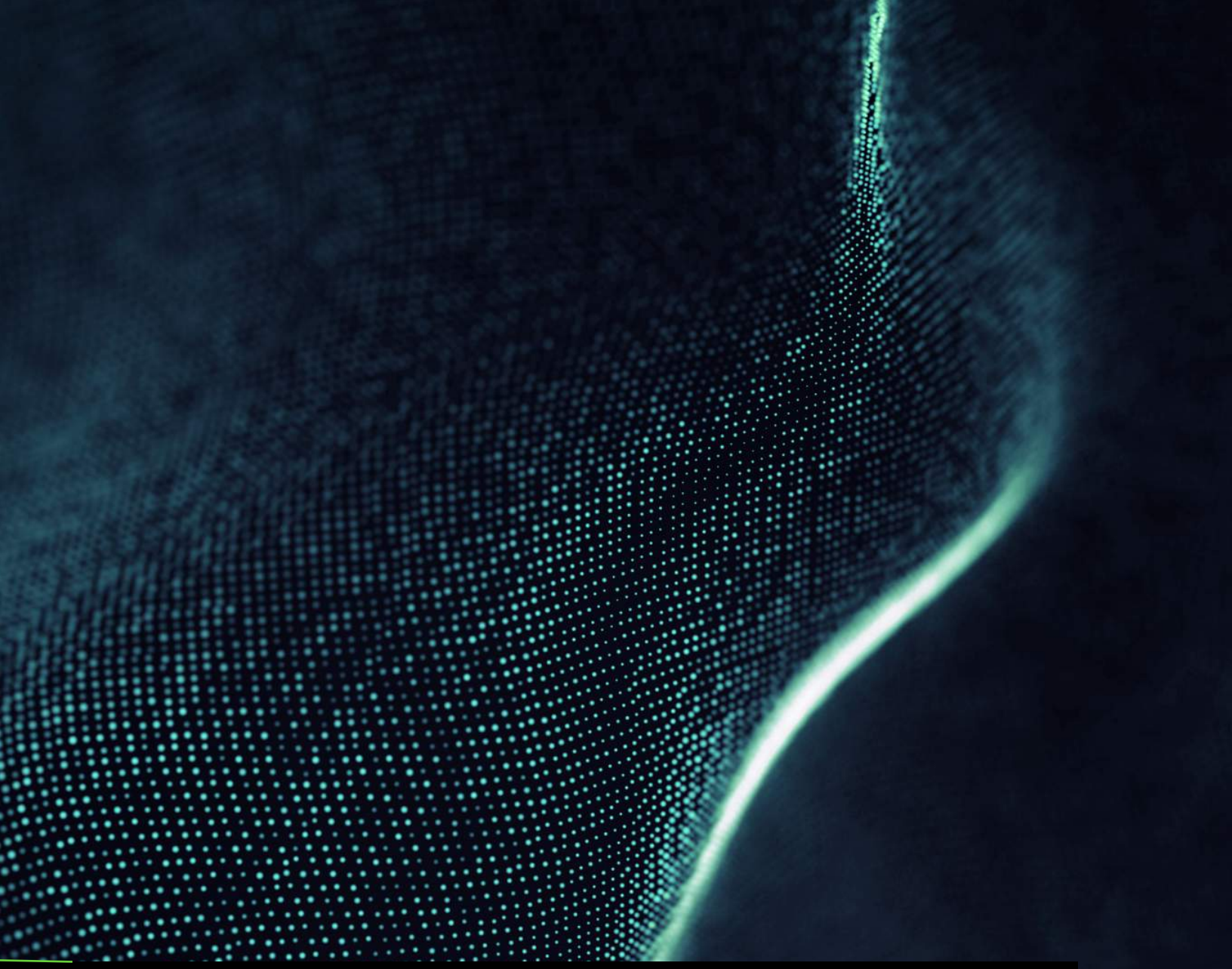


The Artificial Intelligence Revolution in Cybersecurity

How Prevention Achieves Superior ROI and Efficacy

CYLANCE™

Why You Should Read This eBook

The answer to real threat protection is artificial intelligence (AI) based prevention. **Prevention achieves everything detection can't.** The time and costs involved with traditional antivirus (AV) are exorbitant and prohibitive. Moreover, the control friction — the drag on resources and productivity — through layered technology is staggering. Rely on the cloud? Then you can't protect in a disconnected environment.

When you move to **100% prediction, you save time, money, and resources.** You no longer need to buy and maintain multiple security technologies that can't keep up with custom enterprise attacks that flood an organization's defenses. You don't have to worry about network traffic, memory use, CPU overhead, and the cost of re-imaging computers or performing network scans. Your help desk tickets go from the thousands to the few.

The following eBook walks you through the problem of traditional security, the radically new solution, and the myriad of attainable benefits — and includes real-world examples and third-party **research demonstrating 250 % ROI.** Can you afford a successful breach? Or worse, can you afford not knowing? Let us show you a better way.

The Evolution of Cyberthreats: Mechanized Malware

Traditional AV Is Dead

The world of cybersecurity has changed. Signature-based solutions, whitelisting, application controls, and heuristics fail in the modern threat landscape. Why? **Attackers have learned to automate malicious code and vary it to flood an enterprise** until a breach occurs. And the reality is — many enterprises, from mid-size organizations to multi-national brands, have likely been **infiltrated without detection.**

For decades, traditional AV vendors operated using the same model: detect and respond. Cylance®, a data science company, introduces a new paradigm — applying AI to pinpoint bad actors in your network, prevent malware and other threats, and protect against both known and unknown attacks.

The Increased Threat Landscape

You Can't Afford To Stay Stagnant:

- The cybersecurity market grew from $3.5 billion in 2004 to $75 billion in 2015
  - Forecasted to reach $170 billion by 2020
- $1 billion: the cost of ransomware attacks alone this year
- $158: the average global cost of data breach per lost or stolen record
- 25% of large organizations experience recurring incidents
- 229 days: the average time to identify a malicious attack

Predict, Prevent, and Protect

The Business Use Case for AI

When you protect through AI based prediction and prevention, you allow cybersecurity to go from business inhibitor to business enabler. The means you elevate threat protection from a tactical objective to a strategic mission by supplying:

- Streamlined Operations: Eliminate the need for EPP firewalls, device controls, host IPS, data loss prevention, and encryption, while stopping undetected malware and avoiding ransomware using one simple solution
- Decrease Incidents and Prioritize: Transform your IT from reacting to events to proactively securing your environment. Remove mundane tasks that get in the way of strategic projects like virtualization, cloud security, and IT automation
- Enhance Business Continuity: Fortify against enterprise attacks meant to breach your network, steal credentials, and exfiltrate data. Keep from making the next news headline, while ensuring service to customers
- Improve Compliance: Meet government regulations, from healthcare to financial to critical infrastructure industries, as well your internal security policies, with greater protection efficacy

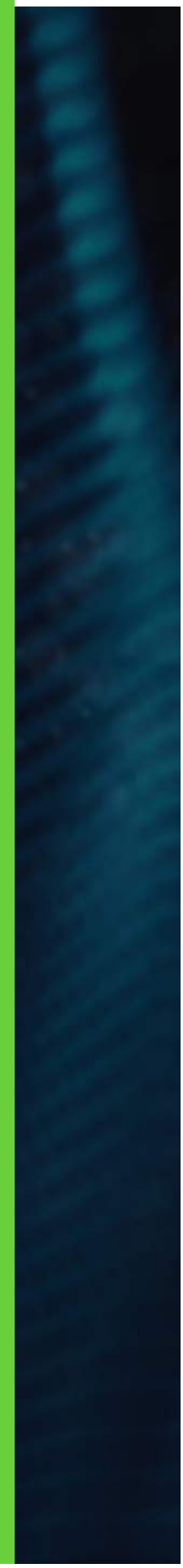
AI Changes the Deployment Game

Make Security Simple

AI not only improves efficacy, but it also changes the deployment model and makes cybersecurity implementation and operation a seamless, smooth process. Because of the advanced features of machine learning, you no longer employ traditional AV technology and tactics, including:

- Incremental storage
- Scanning machines
- Re-imaging machines

Moreover, you can remove large endpoint agents that create performance friction for enterprise users. You also eliminate the tedium of taking machines offline during weekly scans.



Why Prediction and Prevention?

AI and Machine Learning Provide:

- A comprehensive assessment using science and big data analytics
- Greater ROI that eliminates tens of thousands of help desk tickets
- Prediction and prevention of threats pre-execution without a cloud connection and time-wasting daily updates
- A streamlined approach that removes layers of technology and redundant incident response tools

AI and Machine Learning Help You:

- Use minimal system resources (1-2% CPU usage and 40-50 MB of memory)
- Prevent attacks with superior speed (in milliseconds)
- Replace ineffective traditional AV tools (or augment existing security)
- Achieve efficacy rates of greater than 99% (compared to 50-60% with antiquated signature-based AV)

Reap the Benefits

Simple

Organizations can protect endpoints with fewer system resources and reduce network and user impact. When they change their cybersecurity approach to pre-execution, they begin to remove layers of technology. Thus, costs are significantly lowered and they begin to discover ways to consolidate infrastructure. It's easy to deploy and secure your entire enterprise, whether it is 100 or 100,000 endpoints.

Seamless

You can predict and protect across platforms, operating systems, file types, and devices with AI and machine learning. It easily integrates into existing SIEM platforms and works in OEM and embedded devices. In addition, it provides continuous protection for security from system- and memory-based attacks, malicious documents, zero-day malware, privilege escalations, scripts, and potentially unwanted programs (PUPs).

Silent

You can reduce alerts, helpdesk tickets, re-imaging requests, and impact to users when you empower your endpoints with AI based security. You also diminish the need for fire drills and incident response because you eliminate the threat before it manifests. Bolster your endpoint security by using an intuitive web console and simple SIEM integration, with no need for inconvenient signature updates or scan schedules.

Save Millions. Achieve 250% ROI.

Forrester Validation

The Forrester report titled "The Total Economic Impact of Cylance" showcased the real-world value of AI for cybersecurity. With Cylance, companies can reduce threats to almost zero and reduce the costs of remediation, re-imaging, and incident response. It also improves IT and security productivity.

The Forrester study detailed how one state agency changed from traditional antivirus, which placed an enormous burden on IT and security resources, to advanced AI and machine learning from Cylance. The agency significantly reduced its risk of security breaches and boosting productivity.

Read the report.

It Worked for Them. It Will Work for You.

Healthcare Case Study

The Situation

During the rollout of 8,000 virtual machines, a major healthcare provider realized that the company's traditional antivirus solution, which was provided by a tier one AV, was a drain on system resources and wouldn't support performance objectives. The IT and security teams needed endpoint protection for compliance purposes and wanted a lightweight, next-generation solution. The team also wanted a solution that would be transparent to employees while still mitigating the threats posed by ransomware, zero-day attacks, and other exploits.

The Result

By deploying Cylance's award-winning product, CylancePROTECT®, the information security team achieved its goal of attaining endpoint protection that is transparent to the user while enabling a successful transition to VDI. After deploying CylancePROTECT, the information security team realized substantial benefits, including:

- Immediate quarantine of nearly 1,000 items, including adware and PUPs, that were missed by their tier one AV product
- Dramatic reduction in AV-related help desk calls, which cost $22 per call
- Elimination of machines being offline for re-imaging, which cost $400 per machine

Read the case study.

Better Compromise Assessment

An AI based compromise assessment provides the information that executives, board members, senior leadership, and IT staff need. The unique approach goes back in time to the point when each operating system was installed and endpoint deployed. While it uses indicators of compromise, it is not the only mechanism for finding valuable, discerning information. It performs correlation analysis and in-depth interrogation of data, including the entire history of device logs, so you can **uncover every type of possible exfiltration** and gain an accurate classification of good and bad files. The assessment does not impact the enterprise and goes **undetected by bad actors possibly present in your environment.**

An AI based compromise assessment beats other approaches because it is:

- Twice as fast
- Half the cost
- Twice as effective

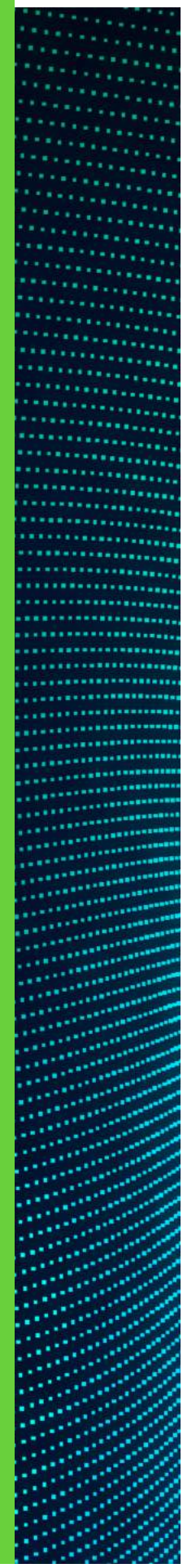
What Next?

Ask the Right Questions

As more cybersecurity vendors make AI and machine learning claims, how can you wade through the options and make the right choice? Start by asking:

- Does it work without requiring a patient zero or sacrificial lamb?
- Does it prevent malicious code from executing on a system?
- How extensive is the math model, and how many years has it been tested in real world environments?
- Is it designed to be useful in both connected and disconnected environments?
- Can it work in milliseconds, with little impact on CPU usage?

Only true AI and machine learning solutions will provide these benefits. Signature-based, heuristic, and behavioral solutions that merely claim to apply AI and machine learning cannot.



Conclusion

You can achieve a level of security and endpoint protection previously unavailable when you employ AI based prevention. Moreover, you can attain a superior compromise assessment, ROI, and efficacy. AI and machine learning have reinvented endpoint protection by providing predictive, preventative security that proactively stops attacks before they impact critical systems. Traditional antivirus requires layers of technology and a first victim, and they can't prevent never-before-seen or unknown threats. AI and machine learning predict and protect systems pre-execution, before an attack occurs, and without a sacrificial lamb. With fewer security layers, network traffic, and memory use, you can reach greater than 99% effectiveness against attacks, while saving time, money, and resources.

Artificial Intelligence. Real Threat Prevention.

About Cylance

Cylance is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect the execution of advanced persistent threats and malware. Our technology is deployed on over six million endpoints and protects thousands of enterprise clients worldwide, including Fortune 100 organizations and government institutions.

Your Machine Learning Cyber Resource

Cylance AI and machine learning protect organizations around the world, and it can protect you. For more information or to request a demo, visit www.cylance.com.

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

20170328-0669