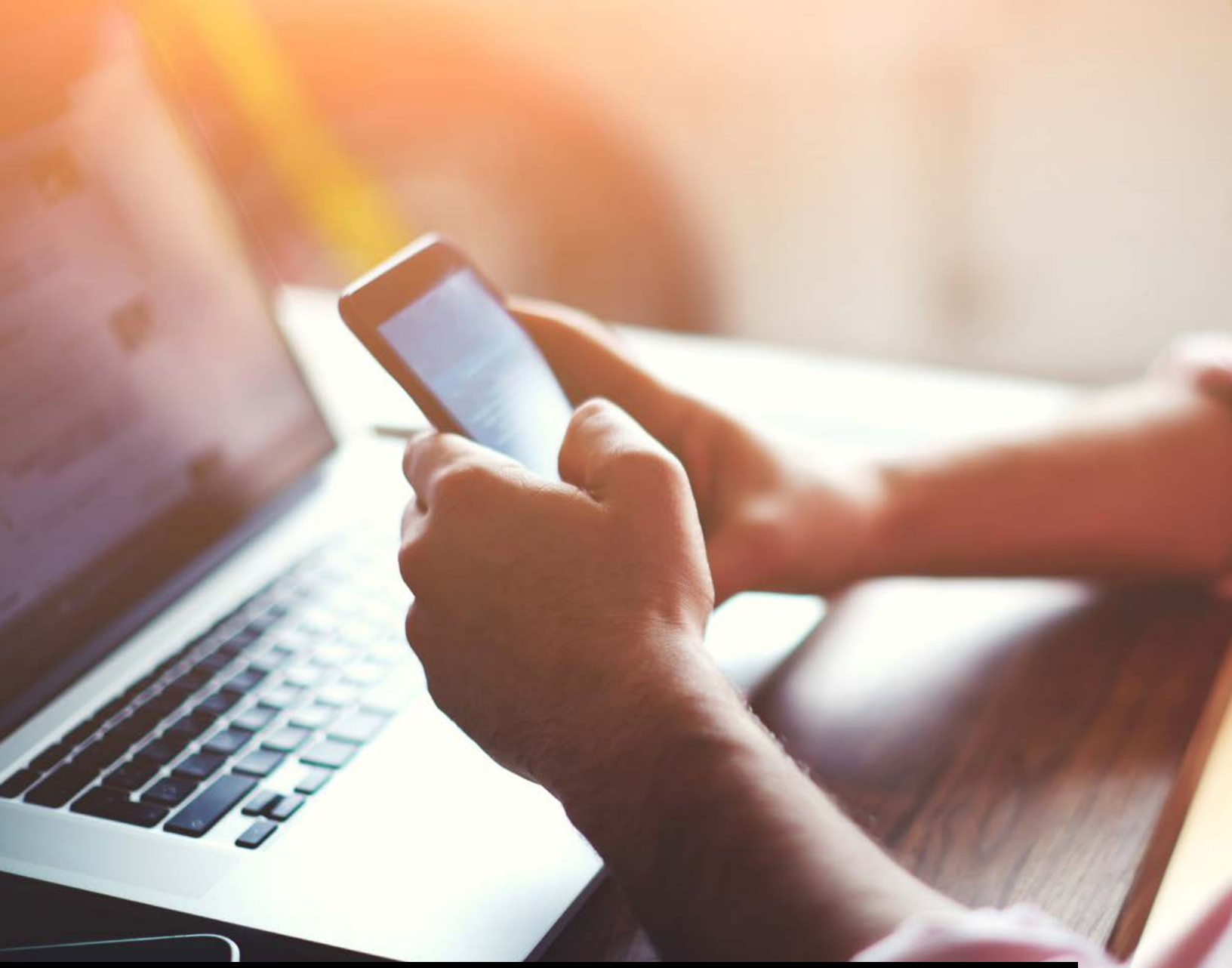


Trust in the Digital Age

A White Paper by Cylance's Office of Security and Trust

CYLANCE™

Our productivity, knowledge, and communications have accelerated at a remarkable rate because we have effective and efficient devices, applications, and networks. Unfortunately, these technologies are vulnerable. Frequently, we see them used for fraud, exploitation, and deceit. Malicious actors, aided by poorly informed users, have created a crisis in trustworthiness, which is quickly becoming a central feature of the modern world.

Citizens, customers, employees, suppliers, and others have raised their expectations that trust requires services to be reliable, available, secure, and private. Around the world, governments have debated, passed, and implemented laws and regulations requiring protection of personal information. Businesses and governments have lost value and reputation through security breaches.

Cylance® was formed specifically to address the privacy and security of information assets. It understands the need for trustworthy products and services and has incorporated safeguards into its design, development, deployment, and operations activities. Cylance provides its customers and partners with effective anti-malware solutions that are trustworthy.

Here at Cylance, we believe it is necessary to discuss trust in the digital marketplace in bold and clear terms. We believe that these discussions should be integrated into the evaluation of costs, efficacy, efficiency, and resources that typically occupy the sales cycle. We believe that consideration of the security and privacy safeguards that are embedded in our services and products are as important as these other factors.

Preventing Malware — Protecting Data

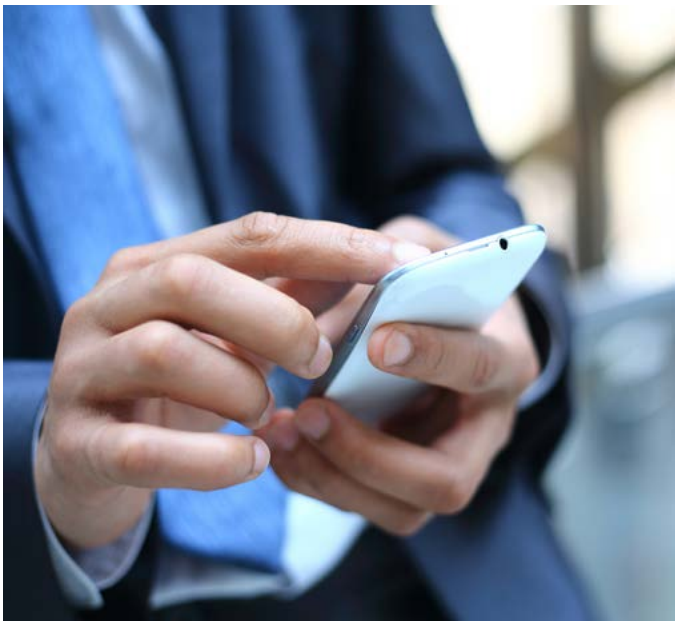
Let's begin with the challenge of threats to trust in the marketplace. In your professional work, do you ask yourself, "Is this software trustworthy? Will it do what it claims? If I deploy it, will it solve one challenge while creating another? Does protecting one set of vulnerabilities just create other compliance challenges?"

It is no wonder that systems managers feel under attack. Every day, new variants of malware pop up, probing vulnerabilities, exploiting software vulnerabilities, and stealing data. Some solutions claim to increase security, but may compromise security and privacy by collecting proprietary and personal information, perversely expanding the client's attack surface.

As individual users, we have to ask ourselves, "Is this email authentic? Is it OK to click on the embedded link? Is this free app safe? Should I answer this text? What will happen when I go to this website?" These are good questions that require good actions to maintain information safeguards. Cylance's automated solutions prevent bad actions from having bad outcomes.

Because everything we say, read, or view is now online, our challenge is to learn how to recognize what is OK and what is malicious. Too often, we fail. Malicious actors exploit our desire for convenience, our need for connecting with others, our vanity, and our simple naiveté about how software and computer systems work. Perhaps we should let the machines do more of our thinking for us. After all, they aren't bored, or lonely, or vain. They are binary, neutral, rational, and focused; all attributes we'd like to foster in ourselves, but don't seem to have sufficient time or capacity to accomplish.

How do we identify and thwart these threats when malware attacks mimic health epidemics at lightning speed, rapidly spreading through and between networked systems? CylancePROTECT® analyzes abnormal executables/processes and embedded suspicious content, ignoring customers' data to protect their intellectual property while still protecting the end-user. Cylance technology evaluates and scores the file to determine good or bad using millions of previously analyzed files. For agents connected to Cylance's cloud, the file is stripped of attribution data, hashed, and uploaded for evaluation and decision scoring. Either way, the decision is made in milliseconds. As needed, alerts and reports are posted to a management console and the score is loaded into the next update for appropriate distribution.



People create software and we know that they can make errors and create vulnerabilities. People use laptops, desktops, and mobile devices to conduct daily tasks and, unfortunately, it is a simple fact that most of us are not trained computer scientists, and we often increase system vulnerability through our actions. Attackers creating malware, bots, viruses, and other variants exploit software vulnerabilities and human weaknesses to advance their criminal opportunities. Most antivirus solutions need for a piece of malicious software to execute on at least one system before they are able to stop it. Cylance's predictive analysis engine is different – and better. It can evaluate a software object in 100 milliseconds, at the earliest moment of the run-time process, and prevent its execution.

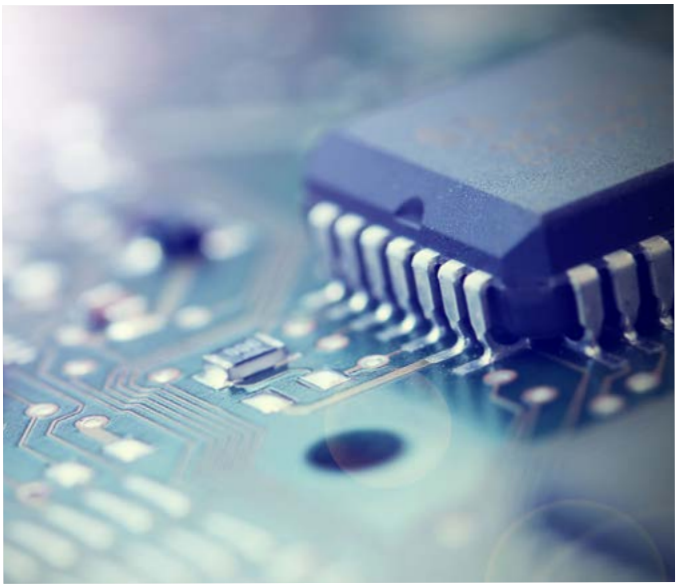
The obvious advantages include rapid detection and prevention, near real-time analysis, and immediate deployment of new scoring information. The system utilizes the advantages of a lightweight client agent, powerful cloud computing, and advanced algorithmic science. System design features such as local scoring, data minimization, one-way hashes, and adherence to customer policy, protect personal and confidential information, enforce limits on the processing purposes, and prevent man-in-the-middle attacks.

Reliability — the Machine Learning Differentiator

Cylance has leveraged advances in artificial intelligence and developed machine learning algorithms based on millions of data inputs to provide malware detection at the point of attack. It's solution, CylancePROTECT, makes rapid-fire decisions at the endpoint computer, recognizing with high accuracy which executable files are more likely to be malicious, allowing benign files to operate normally. The resulting computer and network protection improves performance, eliminates massive data transfers, and creates low-cost opportunities for centralized threat management oversight.

Cylance developed its next-generation antivirus solution, CylancePROTECT, to detect and prevent malware intrusions to secure systems and confidential information, and to protect and respect its customers' confidential information. Cylance believes that providing security and protecting privacy is not a zero-sum gain proposition. Information that is proprietary to an organization or personally identifies individuals deserve the highest levels of protection.

Artificial intelligence based predictive analysis enables a small footprint on the endpoint and requires no connectivity to work. To protect confidential information, it examines executable files and specific processes at the endpoint, minimizes any data needed for further processing, and implements robust security throughout its processing.



Machine Learning

CylancePROTECT leverages mathematical models that predict the probability of a file being good, abnormal, or bad, and utilizes machine learning to continuously advance its knowledge and breadth of coverage. Developing these models requires hundreds of hours of iteration and processing with massive volumes of files for training. This training, customer-reported scores, and thousands of hours spent by human analysts, create learning opportunities to protect vital information from loss, corruption, or disclosure that can resuts from unpatched or out-of-date computers or malware variants not previously seen.

CylancePROTECT not only protects endpoints from malware, it also protects confidential information by minimizing data transfers as it focuses on executable files and malicious processes, not the associated data irrelevant to the purpose of the agent.

Availability — How the Endpoint Agent Works

The CylancePROTECT agent runs on the endpoint, operates automatically, and requires no connectivity. Endpoints do not need connectivity for the agent to effectively detect and prevent malware. The agent generates a secure one-way hash, passing it through the local scored cache, often resulting in an immediate score. If this file hasn't been scored before, the endpoint agent determines a score in about 100 milliseconds and allows or prevents the file/process to run with no transmission. Endpoints with connectivity simultaneously pass the algorithm to the Cylance cloud for a score lookup and response, which takes two to three milliseconds. The first score returned determines whether the file/process runs and the two scores are trued up within seconds.

When an endpoint sees a file that hasn't been seen by the cloud before and the customer policy allows it, the process uploads the file to the Cylance cloud for analysis and scoring. Although previously unseen files, network trouble, or other issues may delay the response, the process generally takes less than 10 seconds.

Regardless of the conditions (local only, cloud transmission, file upload), the process is subject to customer policy and is protected throughout by encryption, secured environments, tested procedures, and minimized and targeted data. CylancePROTECT utilizes the best available technologies to continuously train and manage the endpoint agent. Inside high security environments, the cloud-based processes and applications engage continuous learning and constant management of the solution.

Much like other cloud-based solutions in wide use for marketing, sales, payroll, benefits, engineering, and health care services, CylancePROTECT offers malware training and management applications that run in a secure cloud environment, support endpoint detection, and prevent malware operations.

Managing the Solution

Unlike common AV solutions, CylancePROTECT utilizes only the endpoint agent and does not require customers to install malware server components or network appliances on their systems. Customers may choose a cloud-based service interface that manages deployment, policy, monitoring, alerts, reports, and troubleshooting. The management console enables administrators to examine and manage network activity and status for desktops and laptops as well as fixed-function devices like POS and ATM installations.

Security — the Core Mission

Cylance is first and foremost an information security company. It employs highly trained and experienced professionals who are committed to maintaining the confidentiality, integrity, and availability of information. The company understands the critical role it plays in protecting customer confidential information against malware exploits. While malware detection and prevention are the focus of its activities, information confidentiality and privacy safeguards are deeply embedded in all its information handling.

We have a long-held commitment to support customer compliance with state and national breach disclosure rules for U.S. companies. We understand and have addressed the severe financial risks to our customers by investing in the operational security and integrity of our processes handling customer information. As breach disclosure rules promulgate across the globe, our history of supporting breach prevention serves our customers well.

Cylance works only with reputable cloud service providers holding ISO 27001 certifications. Amazon Web Services is currently utilized. Providers cannot access or disclose confidential information by contract and by technical controls.

To address regional compliance requirements and customer concerns, Cylance has established data centers in Germany, Japan, Brazil, and North America to respect national regulations. Administrative, technical, and physical controls include immutable audit logs of configuration changes, SAML support for customer authentication control, customer policy adherence, regular penetration testing, a bug bounty program, network segregation, data encryption, and shards.

The endpoint agent, CylancePROTECT, utilizes the least data possible to make its decisions when evaluating executable files, avoiding data files. When the agent encounters abnormal, potentially unwanted files, it strips out information irrelevant to determining if it is malware at the first opportunity. Abnormal files or processes that the agent cannot determine as being either good or bad are sent to the cloud service only according to customer policy.

Software Development Lifecycle

Cylance utilizes a secure software development lifecycle focusing on security engineering, assurance, organizational management, and risk identification. By concentrating its efforts in these areas, Cylance not only produces best-of-class products and services, it also runs its operations according to these security and privacy-by-design principles, creating a comprehensive culture of security inside the company.

The company understands that its commitment to security and privacy require rigorous attention to processes dedicated to eliminating defects at the earliest possible stage of development. Products and services are developed with security-by-default and privacy-by-design safeguards as foundational conditions. This commitment yields demonstrated accountability in the development, testing, deployment, and implementation of Cylance software, at the endpoint, in the customer network, and in the cloud.

This focus on rigorous security and privacy safeguards in software development is further supported by the company's robust embrace of structural and process excellence for operational data protection. In other words, creating safeguards is matched with maintaining those safeguards in real-world application and operation.

Information and Asset Protection

Cylance employs strict security protocols in each of its software and service components, enforcing protections of intellectual property and personal information. Communications encryption, enforced authentication (including multi-factor), and portal usage restrictions are just part of the protections. Management console sessions are protected by an OAuth bridge, which provides a comprehensive security token server that integrates with enterprise identity and access management systems, providing the latest Web and API security standards, including OpenID and OAuth.

Privacy — Comprehensive Data Protection

Cylance is a participant in the E.U.-U.S. Privacy Shield framework and takes a comprehensive approach to information security and privacy within a top-to-bottom security culture. The company has built and maintains a robust information management program by hiring an experienced and skilled workforce, developing a policy framework consistent with strict regulatory compliance requirements, implementing standards of care through monitored process controls, and developing sophisticated technical models using applied artificial intelligence, algorithmic science, and machine learning.

As data protection and privacy regulations strengthen around the world, most recently with the implementation of the General Data Protection Regulation in the E.U. in May 2018, Cylance is well-prepared to support customer compliance.

Cylance operates a parallel European system hosted in Frankfurt that shares no data with the general system and prevents data transfers without explicit permission. It also hosts a fully replicated parallel, but separate, system for the U.S. federal government.

Cylance recognizes that in certain markets workers councils or other internal regulation may prohibit the collection of certain employee information. It is working with affected customer companies to enable them to prevent this information from being captured during security incidents. While these efforts maintain breach prevention while complying with local employee rights, insights into incidents may be reduced.

As industry-specific regulations emerge, Cylance works with specific industries to maintain strict compliance such as specific architectural options like on-premises proxy aggregators.

Data Minimization

Cylance has designed its software from the ground up to not only maximize security but to minimize data collection. Minimizing data minimizes risks of exposure. Assuring that data loads are lightweight enhances performance. Anonymizing data at submission protects individual identities and activities. By replacing origination elements with hashes, individual personal information is protected. Hash tables are deleted whenever they are no longer needed for managing abnormal or hostile executables that are detected and prevented. Cylance's prevention product can perform highly effective local analysis and prevention for threats without ever having to upload files outside the organization. This approach is not only unique in the market, it also provides high levels of protection for systems that are offline or fully disconnected.

Data Uploads — User Choice

As in any learning environment, new information yields increasing awareness and knowledge. The Cylance machine-learning engine is massively scalable to develop math models based on executable files. Cylance has created a globally applicable scoring model that creates broad-based environmental awareness of malware threats. Literally, the more data events observed, the smarter and more effective the model becomes. We encourage uploads to increase situational awareness, though customers are free to choose to participate in file uploads by setting internal policies according to their own preferences.

Managing Threats — Cloud-Based Management Console

Centralizing the management console using a cloud-based service improves efficacy, performance, and oversight. The off-premises management console creates cost and resource savings, 24X7 service standards, and superior resiliency.

As noted earlier, Cylance's strict adherence to, and implementation of, security protocols lowers in-network resource demands. Its stringent security measures to assure information confidentiality, integrity, and accessibility extend customer security safeguards.

Conclusion

The speed of malware distribution challenges people's abilities to make fast, good decisions and avoid costly mistakes. We lack global awareness and deep knowledge. We often depend on emotional rather than rational foundations for our decisions. We frequently can't see through the opaque layers of digital communications to understand the ultimate result of simple actions like opening email attachments, website links, or downloaded applications.

Cylance's commitment to providing reliable, available, secure, and private services is foundational to its commitment to trustworthiness in a troubled marketplace. From the endpoint agent to the machine-learning engine in the cloud to the management console, Cylance supports data minimization, limited purpose, legitimate use, and accountability, principles at the heart of its certification under the E.U.-U.S. Privacy Shield framework.

CylancePROTECT cuts through the historically generic AV clutter and makes rapid, rational, and broadly aware decisions to protect confidential information and support customer compliance with security and privacy requirements. It runs light and fast without needing an online connection. It utilizes cloud-based security services for continuous learning and constant management. Cylance's secure software development lifecycle is inherently robust and respectful of personal information privacy and data protection compliance.

While machines cannot and should not make certain decisions, CylancePROTECT makes appropriate and relevant decisions to protect and respect confidential information to maintain security and privacy across information systems processing high-volumes of diverse data.

With robust security and privacy protection a core aspect of the development process, CylancePROTECT promises to provide trusted high performance, high efficacy solutions without compromising confidential and personal information.

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

20170915-1713