Cylance® Axiom Alliances Program

Program Overview
The Cylance Axiom Alliances Program is a community of cybersecurity solution providers working together to deliver a prevention-first approach to security. Unlike other ecosystems built around the assumption of compromise, Axiom vendors are committed to using AI to continuously prevent adversaries from harming organizations by delivering added security controls that, when combined, minimize an organization’s attack surface and enable swift action across the organization’s entire environment, whether it be on-premises, IoT devices, hosted, or public cloud.

ax·i·om
axē əm/Submit
noun
A statement or proposition that is regarded as being established, accepted, or self-evidently true.

“The axiom that a lack of security personnel exposes customers to attacks”

Synonyms: accepted truth, general truth, dictum, truism, principle
This unique grouping of cybersecurity solution providers:

- Dramatically reduces the cost, time, and complexity usually associated with integrating security solutions
- Delivers an integrated, prevention-first approach to security
- Improves the efficiency of security teams by collaborating, at a technology level, across the cyber kill chain, minimizing alerts and maximizing visibility
- Enables real-time decision making without a large administrative burden, driving down time to respond and cost

Real-Time Decision Making
The cybersecurity industry is experiencing a sea change, sparked by new approaches and techniques that leverage both human and artificial intelligence. Knowing that every day could be zero-day, Cylance strives to lead the charge by providing innovative, AI based solutions, and by giving customers a fully operational and integrated architecture.

The Cylance Axiom Alliances Program has been established to provide clarity and simplicity to the increasingly complex cybersecurity challenges facing our customers. The Axiom Alliances Program is comprised of the following four key segments:

- Technology Alliances
- OEM Partners
- Assurance Alliances
- Global Alliances
Cylance Security Solutions are designed to integrate with next-generation security operation centers. By leading with a prevention-first strategy, Cylance technology partners benefit from a signal-rich feed that has been filtered by noise dampening algorithms and classified for urgency. Cylance partners leverage connectors to the cornerstone prevention product, CylancePROTECT®, in three stages to deliver unrivaled prevention, unified visibility, and superior decision making.

These three stages are referred to as Avert, Analyze, and Action:

**AVERT - Unrivaled Prevention**
The Avert stage follows the principles of CylancePROTECT, which is the most accurate, efficient, and effective solution for preventing advanced persistent threats and malware from executing on an organization's endpoints. Through alliances with network access control providers, cloud access control brokers, and mobile threat protection providers, Cylance favors instantaneous decision making with a prevention mindset to avert the attack.

**ANALYZE - Unified Visibility**
CylancePROTECT significantly improves the signal to noise ratio that makes other products an operational burden. Critical to corroborating and correlating data events is the alliance with security information and event management, or SIEM. This ability to aggregate several feeds, adding greater context and visibility for decision making, proves valuable to customers in the Analyze stage. Such partnerships empower customers with a single spotting scope for unified visibility into risk factors and ultimately, the cyberhealth of their organization.

**ACTION - Superior Decision Making**
CylancePROTECT removes the guess work. Within milliseconds, a determination can be made on an executable and a decision made on whether to alert, block, or permit. Whether manual or automated, decisive actions on threats and events must be consistent laterally, across platforms, and at all entry points to the organization.

Cylance Technology Alliances Program Benefits:
- Expanded coverage to avert, analyze, and take action on threat events
- Introductions to channel partners through webinars and events
- Co-sponsoring opportunities to reach larger audiences with joint messaging
- Access to licenses of Cylance products for testing and integrating for use cases that demonstrate a market advantage
- Access to early releases of Cylance products and the ability to influence the roadmap

For more information about Technology Alliances, contact partnersupport@cylance.com.
OEM Partners

Technology is only as effective as the security defending it. Cylance OEM partners that integrate Cylance products into their offerings are provided the tools needed to effectively market and sell combined solutions.

Cylance OEM Partner Program Benefits
OEM partners benefit from Cylance’s deep domain expertise across security, data science, and software development. Cylance has flexible commercial models that align licensing and pricing with partners to drive mutual success in the market. Cylance values technical partnerships and is open to collaboration across both technical integration and go-to-market programs. This includes education, sales and channel enablement, and increased exposure through Cylance’s marketing efforts.

No matter the vertical market, Cylance can deliver unmatched protection:

Security OEMs
Cylance OEM partners harness the power of artificial intelligence and machine learning to detect threats that other solutions miss, stopping malware before it executes. Cylance technology allows OEMs and their customers to identify and stop attacks at previously unachievable rates in both online and offline environments. Cylance technology also easily integrates within security products.

Internet of Things (IoT)
IoT devices continue to account for the bulk of new Internet connections. Many were designed for function, resilience, and redundancy – but not security. Modern cybersecurity must be designed into IoT products to defend against new attack types and threat vectors. Cylance technology can secure IoT devices.

Healthcare Systems and Medical Devices
Securing medical devices is beyond the scope of traditional signature-based solutions. Because Cylance solutions are autonomous and don’t rely on cloud connectivity to update or be effective, OEMs can protect devices online, offline, and when intermittently connected.

Industrial Control Systems
Critical infrastructure such as power grids, water treatment plants, and transportation systems provide ample opportunities for cyberattacks. Cylance OEM solutions secure SCADA, PLC, DCS, and other critical ICS systems while achieving significant resource and cost savings.

Automotive
Automakers must design cybersecurity into their platforms from the ground up. Cylance is currently working with automakers to identify and shut down threat vectors evading traditional cybersecurity approaches, and does so in online, offline, or intermittently connected environments.

Aerospace
Commercial aerospace system Wi-Fi networks, in-flight entertainment, and crew and ground management systems expose airlines to new online attack vectors. Cylance OEM solutions deliver high security at a low impact, protecting airline networks and passenger data without introducing additional technology layers or operational costs.

For more information about becoming an OEM Partner, contact partnersupport@cylance.com.
Cylance partners with law firms, and cyber insurance carriers and brokers to reduce risk for their customers. Cylance understands cyber risk and helps the insured to quantify that risk for their industry. Heavily regulated markets such as financial, healthcare, energy, and utilities require targeted services to enable companies to come into compliance. Whether it is GLBA, DFS, HIPAA, or GDPR, there are significant consequences for lack of preparation or improper execution during an incident. Fines for non-compliance are substantial, regardless of whether a customer is an SMB, mid-market, or large enterprise.

Cylance prevents negative business outcomes. Fast, thorough containment and remediation are essential to keep businesses up and running. Cylance works closely with breach coaches and claims departments to resolve issues fast and on budget.

Cylance’s Consulting Services identify and mitigate risks, including: Compromise Assessment, Incident Response (IR) Readiness, Red Team, Pen Testing, Risk Assessments (ICS/SCADA/NIST), IoT and Embedded Systems, and Incident Containment/IR Retainers. Cylance Consulting Services are vetted in advance by counsel and insurance partners and are designed to materially advance an organization’s network security profile.

Cylance Assurance Alliances Program Benefits:
- End-to-end solution under one brand
- Leading IR team with over 1,200 incidents contained
- 24x7 global team with follow-the-sun capability
- Technology solution contributes to rapid completion of engagements
- Custom proactive services to get the insured on the right track
- Tailored services and reporting

Key Customer Advantages:
- 365-day protection available
- Measured risk reduction
- Industry compliance assured
- Fast response with immediate results

For more information about Assurance Alliances, contact partnersupport@cylance.com.
Global Alliances

Cylance has developed techniques and technologies that provide unique opportunities to create strategic advantages for global service providers and their customers. This program recognizes and accommodates offerings from carriers, consultants, MSSPs, outsourcers, and system integrators. Each relationship is crafted individually to support the business structure and go-to-market model of the alliance partner.

Cylance Global Alliances partners leveraging Cylance Security Solutions benefit from reductions in alerts, trouble tickets, and re-imaging, as well as virtually complete elimination of ransomware.

To accelerate achieving these results, Cylance implemented a comprehensive framework to guide the growth and maturation of its Global Alliances partners. Cylance recognizes the need for tactical success to fuel mutual investment. Cylance executes on a straightforward engagement model to drive short-term wins and build momentum for relationships within its alliance partners and the customer community. This model successfully activates relationships and builds momentum to drive growth.

As Cylance partners move their businesses into new service lines, there is a blurring of capabilities. To best support evolving go-to-market strategies, Cylance developed a simplified approach to deliver solutions specific to the partner’s use cases.

**Thought Leadership**
Engage Cylance executives to educate at the board level on AI based security

**AI Enhanced Consulting Services**
Compromise Assessments, Incident Containment, Security Transformation, and SOC Integration

**Subscription Services**
Create integrated OpEx offerings leveraging the Cylance Prevention Platform

**Resale**
Bundle solutions into CapEx transactions

For more information about Global Alliances, contact msspchannel@cylance.com.