IAAS/PAAS CLOUD SECURITY

Program Maturity Model

Solution Primer
Cloud-first ecosystems with security at the forefront are becoming more commonplace within enterprises. With fewer and fewer obstacles to cloud adoption, the path of workload migration to cloud is becoming less foreboding. In fact, in a recent survey, respondents indicated that security is no longer their number one challenge. In the past, and to some extent in the present, security of workloads has been an afterthought. With automation and orchestration, enterprises are building security into deployment workflow and providing greater levels of assurances to stakeholders.

The rise in security-as-a-service (SeCaaS) solutions, too, reflects the shift to leverage the advantage of the cloud to secure cloud assets rather than reliance on traditional security offerings. A parallel development is the democratization of security, i.e. “If you build it, you own it.” As DevOps surges, the role of security is shifting away from traditional security teams towards the developer and ultimately requires a greater share in the responsibility of security.

However, everything is not utopia. As companies seek to become more agile in the cloud, resources to support those efforts lag significantly resulting in resource challenges thought to be solved by cloud adoption. Beyond the enterprise, companies struggle contractually with service providers over the lines of responsibility and accountability for cloud assets and data. Shared responsibility models have not improved matters. Leaders complain that providers, in theory, provide detailed guidelines of responsibility but in practice are quick to transfer blame when things go awry. The 2016 Mirai outbreak, the massive IoT distributed-denial-of-service (DDoS) attack, showed lingering opportunistic impact could be felt across cloud-service providers, according to the “Project Heisenberg Cloud” project. Most of the blame game focused on human error and omission gaffes (e.g. default passwords, no passwords) that resulted in camera and DVR configurations “gone bad.” More of these attack convergences are predicted, that is, an issue in one medium (i.e. IoT configuration missteps) can have a profound impact on targets in another (cloud). According to authors Rudis and Abdine, cloud configuration issues are also widespread. The project’s modest distribution of cloud honeypots have discovered instances of misconfigured cloud services communicating to non-existent infrastructures. Are the Mirai attacks a harbinger of the future?

Optiv’s infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) research monitors these emerging cloud developments to educate our clients on key issues that concern business leaders. This primer is an executive summary of our cloud security research into IaaS/PaaS to guide businesses in securing cloud workloads. The Optiv cloud security IaaS/PaaS Primer and subsequent blueprint offer businesses of all sizes a pragmatic approach toward maturing cloud security programs that manage the risk and protection of cloud workloads.
Program and Approach

The Optiv IaaS/PaaS cloud security maturity model equips organizations with the necessary guidance to adequately plan, build and protect cloud-based workloads given the current state of the market into the future.

Program Clarity

Today, businesses are tasked with building robust platforms that support and secure cloud-based workloads to empower business objectives. The maturity and capacity to build robust and secure programs, however, varies among company sizes (e.g., small business versus big enterprise) and across verticals. Businesses are taking time to research the complex IaaS/PaaS market in support of their cloud migration strategies to build resilient infrastructures. At the same time, the vendor market is still in the process of positioning itself to meet the demands of IaaS/PaaS. Market analysis shows that IaaS/PaaS investments are down as compared with SaaS solutions, yet growth rates for security are high as workloads shift and enterprises become increasingly aware that they need effective security solutions.

The Optiv IaaS/PaaS cloud security maturity model equips organizations with the necessary guidance to adequately plan, build and protect cloud-based workloads given the current state of the market into the future. Optiv has gathered key insights from interactions with vendors, cloud subject matter experts, and practitioners who have endured the growing pains of architecting sound cloud IaaS/PaaS infrastructures. The aggregate result of these conversations is our cloud IaaS/PaaS maturity model and operational guidance that provides milestone-based strategies, along a path of maturity that aligns with business objectives.

Program Strategy Approach

The maturity model offers security leaders the ability to quickly assess their current state of operations for the purposes of establishing a roadmap to meet program objectives. The maturity model builds upon the program core that serves as a basis for defining program drivers, the business requirements and non-program support to meet the roadmap objectives. This component of the program strategy is crucial for meeting practical achievable goals given the variable scale of IaaS/PaaS environments.

The outcomes are supported by functional capabilities that are characteristic of IaaS/PaaS security programs (e.g., architecture reviews, patching, vulnerability management, monitoring) and their descriptive relevance at each maturity level. This step-wise approach starts with organizational awareness that leads to subsequent states of maturity, i.e., IaaS/PaaS activities mature in an accumulative fashion. Companies, also, measure maturity using recommended key performance indicators to assess capability achievement. Performance indicators are a key objective of the framework for benchmarking and program improvement. Goal attainment measurements as well as an assessment of functional capabilities affords executive management the ability to chart maturity progress. Further, program managers equipped with performance insights can adjust and tweak program timelines and budgets more effectively with the Optiv framework.
The IaaS/PaaS Cloud Security Maturity Model

**Aware**
Enterprise has no accommodation for IaaS/PaaS security characterized by limited policy, no formal expertise, and reliance on cloud service providers for controls.

**Reactive**
Enterprises have limited technology expertise and loose collection of industry policies for governance. As a result the business relied on contractual shared responsibility to secure its IaaS/PaaS.

**Adaptive**
Enterprise adapts industry frameworks and leverages technical expertise to support existing use cases. Existing security models are also adapted to meet cloud consumption.

**Purposeful**
Enterprises create cloud native security models which execute business-aligned tailored framework and expanded domain expertise.

**Strategic**
Enterprise proactively architects security into business-aligned strategies that transforms domain expertise and in turn influences business innovation.
The program drivers are, in reality, the business case for developing a strategy for and operationalizing an IaaS/PaaS-based cloud security program.
Requirements

Business stakeholders across a diverse set of verticals provide insight to Optiv regarding cloud IaaS/PaaS requirements. Successful programs are built upon stakeholders’ requirements, which serve as the foundation of the program effort. Optiv aggregates and normalizes these data to provide a broad reach perspective of trending requirements in this ever-evolving security sector.

- Ensure high availability of secure(d) workloads supporting critical business processes
- Enable agile computing that leverages instrumentation, orchestration and automation for high achieving environments
- Build resilient IaaS/PaaS ecosystems that support scalable business continuity and disaster recovery models as required

Non-Program Support

Non-program support encompasses the components of the program that are required to effectively build and operate the program, but are outside the scope of the enterprise security organization. Security management may have the ability to indirectly influence these resources, but not necessarily control them. Further, a percentage of non-program support is covered by the service providers. Importantly, partnerships with the cloud service providers require close attention to ensure roles and shared responsibilities are understood in support of the program. Our comprehensive cloud security focus groups yielded the following non-program support data points that are crucial for the success of a program:

- Internal and external counsel with expertise in breach protocol, service provider legal liaison, compliance and privacy roles within an organization (role may also cover data governance)
- Procurement role to support contract review and management processes
- Audit function to ensure regulatory-compliance requirements; security role embedded within the audit function to elevate cloud risks

Outcome-Oriented Program Development

The Optiv maturity model is outcome oriented. Given the various deployment models and the myriad of solutions to aid in cloud architectures, the outcome perspective affords practitioners and leaders clarity of focus. Functional capabilities and activities are framed to ensure the desired outcomes.

<table>
<thead>
<tr>
<th>Outcome</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>The manner in which the IaaS/PaaS cloud security program is framed, operationalized and activities governed</td>
</tr>
<tr>
<td>Understanding</td>
<td>The depth and breadth of expertise a company has regarding IaaS/PaaS cloud security, its operational footprint and situational awareness in order to develop protective measures</td>
</tr>
<tr>
<td>Execution</td>
<td>The manner in which organizations plan, build and run their IaaS/PaaS cloud security program and enforce policy at each stage of the maturity model</td>
</tr>
</tbody>
</table>
## Modeling Outcomes to Maturity

<table>
<thead>
<tr>
<th></th>
<th>Policy</th>
<th>Knowledge</th>
<th>Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aware</strong></td>
<td>No specific policy</td>
<td>No formal expertise</td>
<td>Leveraging provider controls</td>
</tr>
<tr>
<td><strong>Reactive</strong></td>
<td>Loose collection of industry policy frameworks (e.g. CSA CCM)</td>
<td>Limited technology expertise</td>
<td>Shared responsibility focused on contractual means</td>
</tr>
<tr>
<td><strong>Adaptive</strong></td>
<td>Industry framework adapted to current use-case</td>
<td>Expertise adapted to existing use-cases</td>
<td>Existing execution model adapted to cloud consumption</td>
</tr>
<tr>
<td><strong>Purposeful</strong></td>
<td>Business-aligned framework</td>
<td>Business-aligned domain expertise</td>
<td>Cloud native security execution model</td>
</tr>
<tr>
<td><strong>Strategic</strong></td>
<td>Proactive, business-aligned and risk-based policy</td>
<td>Transformative domain expertise driving business innovation</td>
<td>Security architected into strategy</td>
</tr>
</tbody>
</table>
Functional Elements – Building Blocks of Program Development

Functional elements are the effective building blocks of the program. Every program Optiv provides guidance on has these essential building blocks that support the level of desired outcomes. From these functional elements we determine capabilities at specific maturity levels, and can derive client-specific activities to develop the capabilities to support the desired measurable outcome.

<table>
<thead>
<tr>
<th>Functional Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architecture</strong></td>
<td>The design of IaaS/PaaS cloud environments and security measures that support them</td>
</tr>
<tr>
<td><strong>Identity and Access</strong></td>
<td>The manner in which the organization plans, builds and operationalizes the various identities and roles used for IaaS/PaaS-based cloud services.</td>
</tr>
<tr>
<td><strong>Protection</strong></td>
<td>How the organization prevents, detects, responds and recovers from the threats to IaaS/PaaS-based cloud workload usage and associated infrastructures</td>
</tr>
<tr>
<td><strong>Visibility</strong></td>
<td>The manner in which the organization obtains and maintains insight into risks within IaaS/PaaS environments</td>
</tr>
<tr>
<td><strong>Vulnerability Management</strong></td>
<td>The framework for identifying, evaluating and taking action on vulnerabilities within IaaS/PaaS workloads and associated infrastructures</td>
</tr>
<tr>
<td><strong>Application Security</strong></td>
<td>The method of incorporation of application security principles and requirements into the design, delivery and maintenance of IaaS/PaaS cloud workloads</td>
</tr>
<tr>
<td><strong>Governance, Risk, and</strong></td>
<td>The functional framework for how the organization defines and delivers policy and then manages adherence to that policy to effectively meet risk and compliance goals and objectives</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Data Security</strong></td>
<td>How the organization applies data security principles such as encryption, data masking, data loss prevention in IaaS/PaaS ecosystems</td>
</tr>
</tbody>
</table>
Assembling the Program

The cloud is already a convergence of ecosystems – everything-as-a-service, the internet of everything, software-defined everything, and everything else – with ever evolving challenges. Challenges acknowledged, Optiv is highly confident that organizations can successfully and securely move workloads to the cloud with this framework in hand and avoid common strategic and operational pitfalls. Whether an organization is faced with issues of shared responsibility, cloud-cyber insurance, building robust architecture, or cloud-incident response – the framework is flexible enough to account for “gotchas” and to meet the distinct needs of a business and technology leaders. Optiv’s model-driven program includes the added benefit of measurement and benchmarking to gauge program effectiveness and most importantly to show progress and maturity for that ever-elusive security return on investment (ROI). As organizations adopt this framework, the Optiv team will continue to evolve and improve the IaaS/PaaS maturity model, leveraging feedback from lessons learned. Harnessing the power of experiences gained, successes and failures, the cloud IaaS/PaaS will continue to evolve in step with advances we observe in the field and in the security marketplace. For more information and to obtain your individually licensed copy of Optiv’s IaaS/PaaS cloud security blueprint, contact your Optiv representative.
Mark Arnold
Senior Research Principal,
Solutions Research and Development, Optiv

Executive Sponsor
J.D. Sherry
Vice President, Portfolio Strategy and Cloud Security
Optiv

References
3 Ibid., p.2 The new number one obstacle to cloud is "lack of resources."