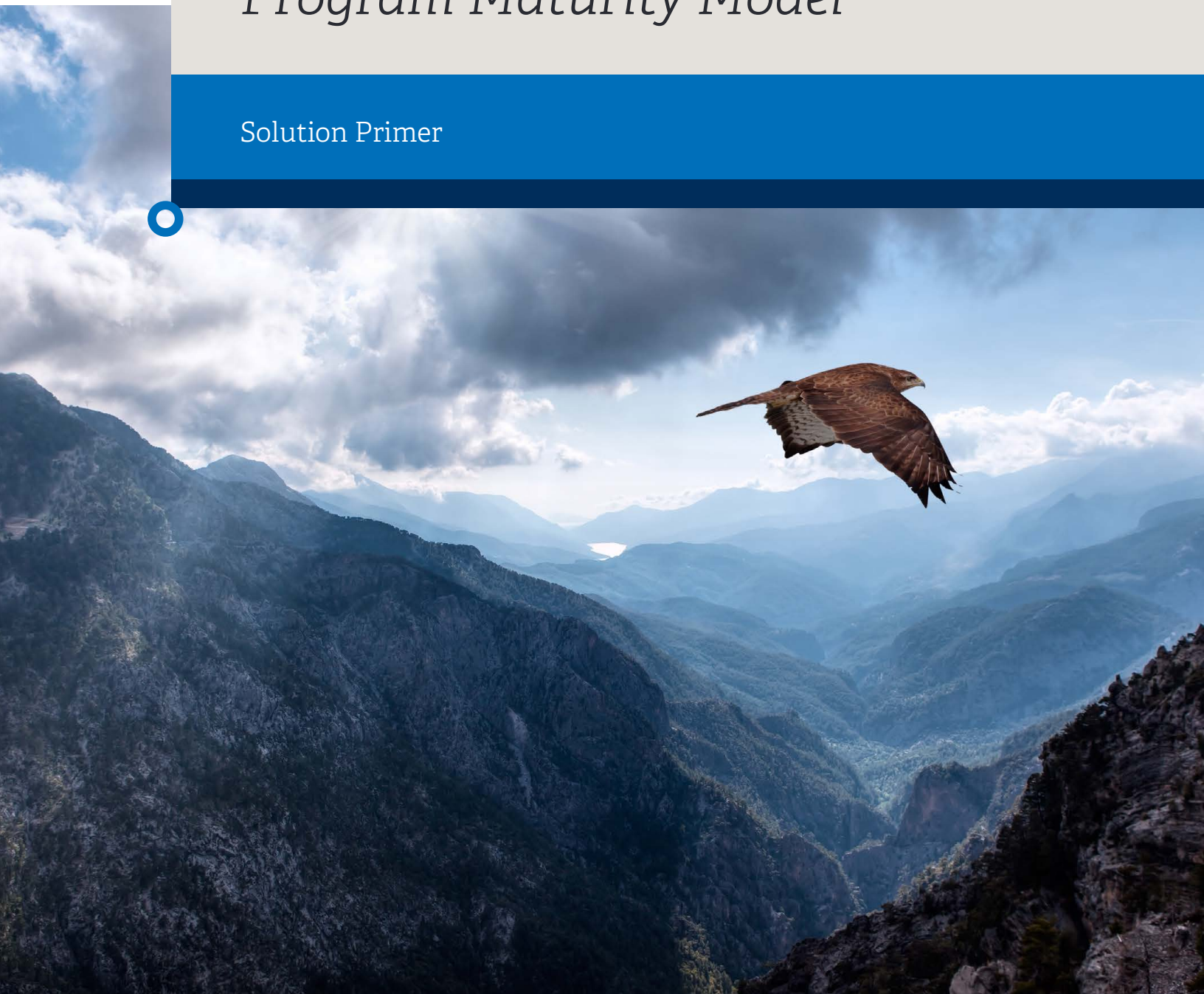


IAAS/PAAS CLOUD SECURITY

Program Maturity Model

Solution Primer



Executive Summary

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.¹ 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.²

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.³ 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?⁴

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.

Problem 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.

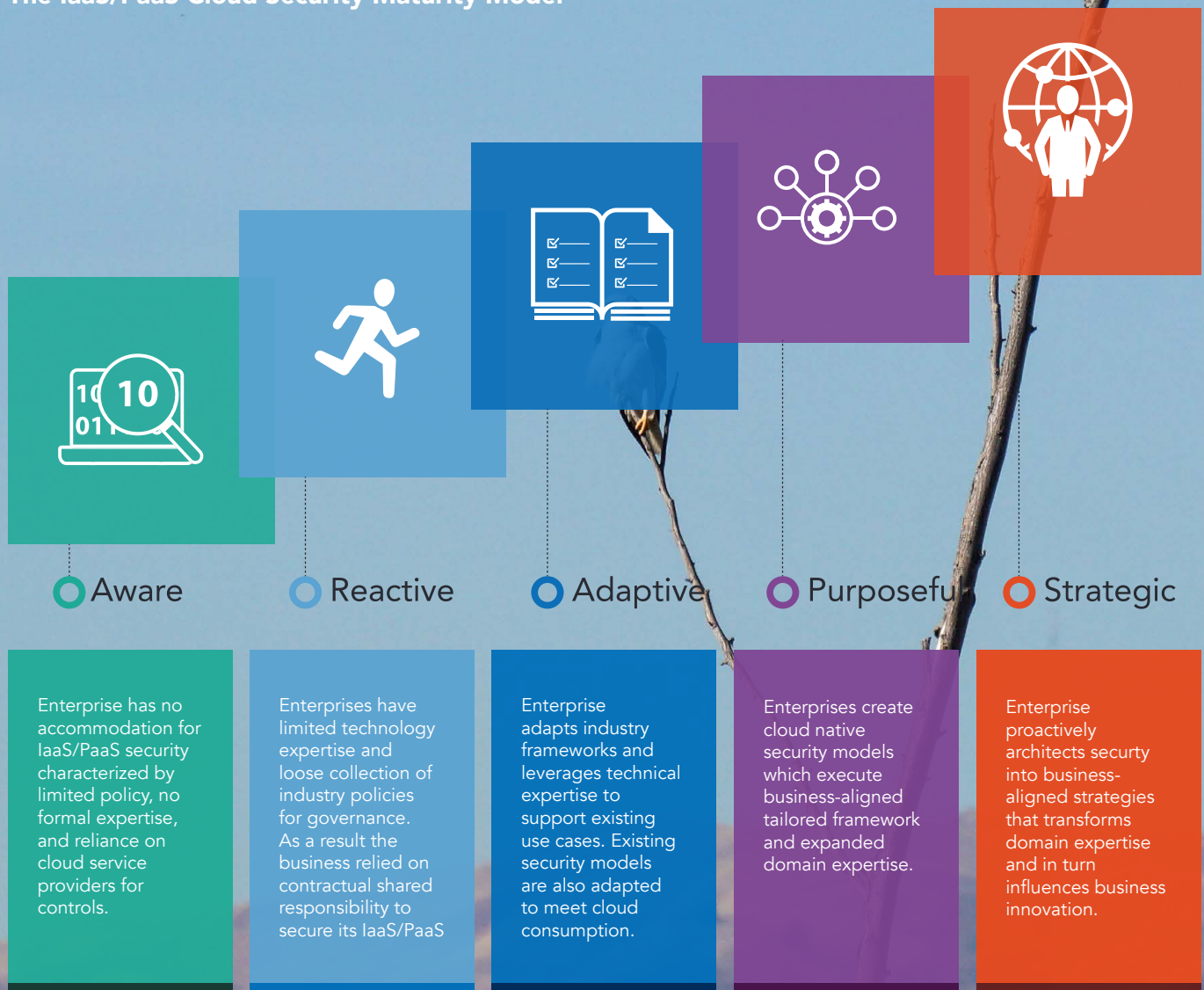
Program Strategy Approach

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.

Model Driven Program Development

The IaaS/PaaS Cloud Security Maturity Model



Model Driven Program Development

Program Core

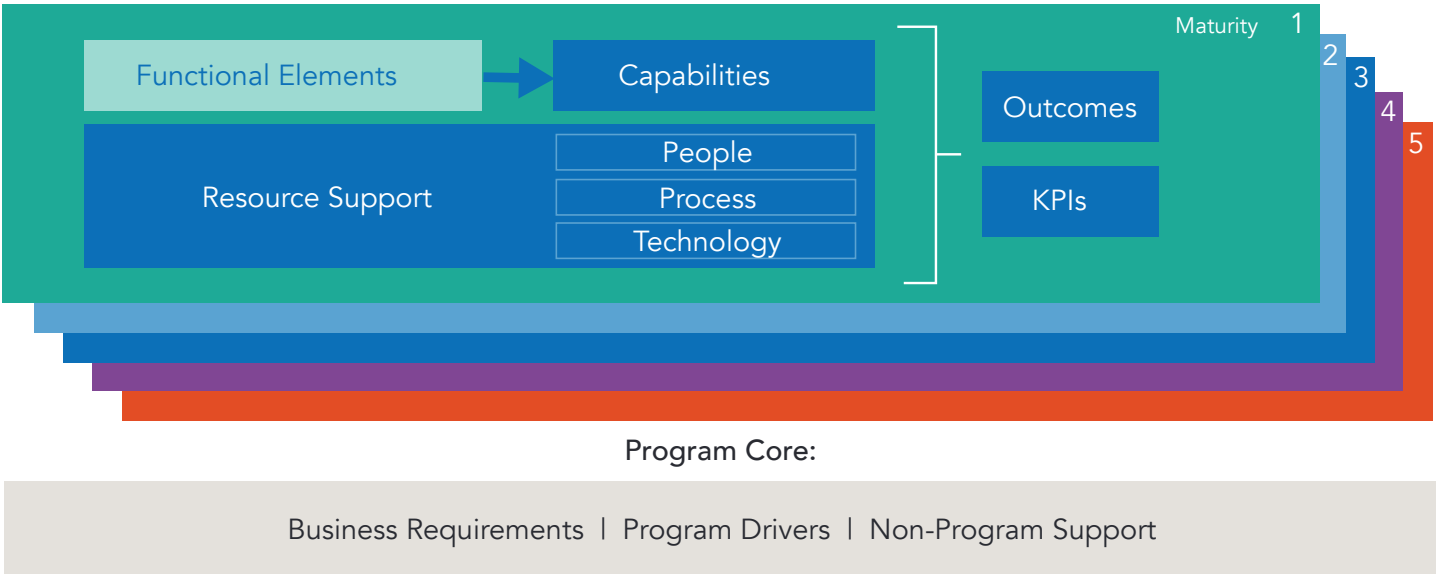
The program core includes the business drivers, the requirements and the outside support upon which the program foundation is established.

Program Drivers

Cloud security IaaS/PaaS business drivers consistently include but are not restricted to the following: regulatory and compliance, third party risk management, external requirements (e.g. client or partner driven) and board demands. The drivers serve as points of engagement between the business and the security practice to achieve measurable outcomes that are in alignment with business objectives. The program drivers are, in reality, the

business case for developing a strategy for and operationalizing an IaaS/PaaS-based cloud security program.

- Cloud-first initiatives to reduce total cost of ownership (TCO)
- Visibility to assess and manage risks
- Regulatory and compliance, including export controls (e.g. ITAR, EAR)
- The explicit need for security to support an agile high performing, scalable, resilient cloud computing environment (e.g. DevOps)



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.

Outcome	Description
Policy	The manner in which the IaaS/PaaS cloud security program is framed, operationalized and activities governed
Understanding	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
Execution	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

Model Driven Program Development

Modeling Outcomes to Maturity

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

Model Driven Program Development

Functional Elements – Building Blocks of Program Development

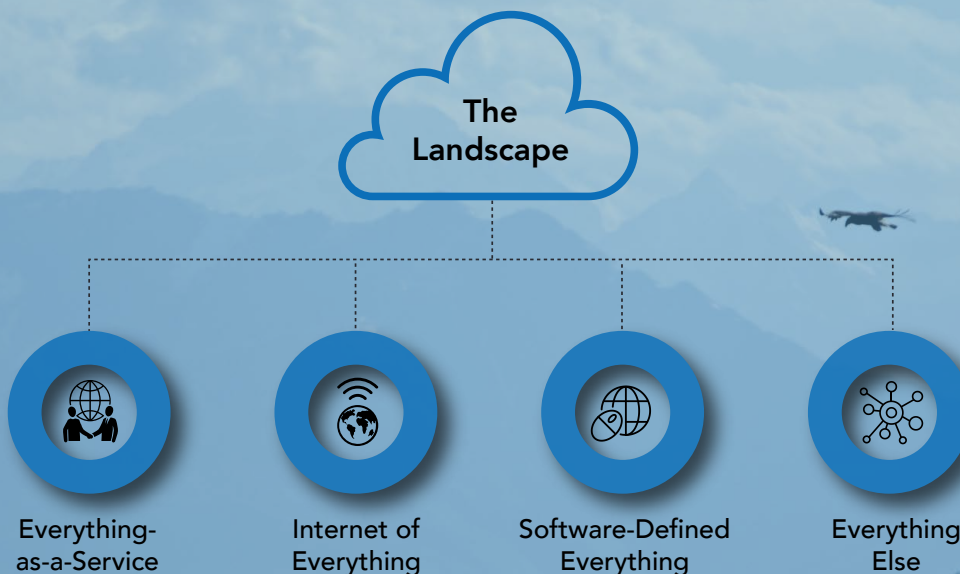
Functional elements are the effective building blocks of the program. Every program Optiv provides guidance on has these essential building blocks that support the level of desired outcomes. From these functional elements we determine capabilities at specific maturity levels, and can derive client-specific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

Functional Element	Description
Architecture	The design of IaaS/PaaS cloud environments and security measures that support them
Identity and Access Management	The manner in which the organization plans, builds and operationalizes the various identities and roles used for IaaS/PaaS-based cloud services.
Threat Protection	How the organization prevents, detects, responds and recovers from the threats to IaaS/PaaS-based cloud workload usage and associated infrastructures
Visibility	The manner in which the organization obtains and maintains insight into risks within IaaS/PaaS environments
Vulnerability Management	The framework for identifying, evaluating and taking action on vulnerabilities within IaaS/PaaS workloads and associated infrastructures
Application Security	The method of incorporation of application security principles and requirements into the design, delivery and maintenance of IaaS/PaaS cloud workloads
Governance, Risk, and Compliance	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
Data Security	How the organization applies data security principles such as encryption, data masking, data loss prevention in IaaS/PaaS ecosystems

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

1 "Rightscale 2016 State of the Cloud Report," accessed August 14, 2016 <http://www.rightscale.com/lp/2016-state-of-the-cloud-report>

2 Adrian Sanabria, "Cloud, DevOps and the New Security," (paper present at Cloud Security World 2016, Boston, Massachusetts, June 13-15, 2016).

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

4 Derek Abdine and Bob Rudis, accessed November 14, 2016 "Project Heisenberg Cloud: Cross-Cloud Adversary Analytics," <https://information.rapid7.com/rs/495-KNT-277/images/heisenberg-cloud-research-report.pptx>



1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

© 2016 Optiv Security Inc. All Rights Reserved.