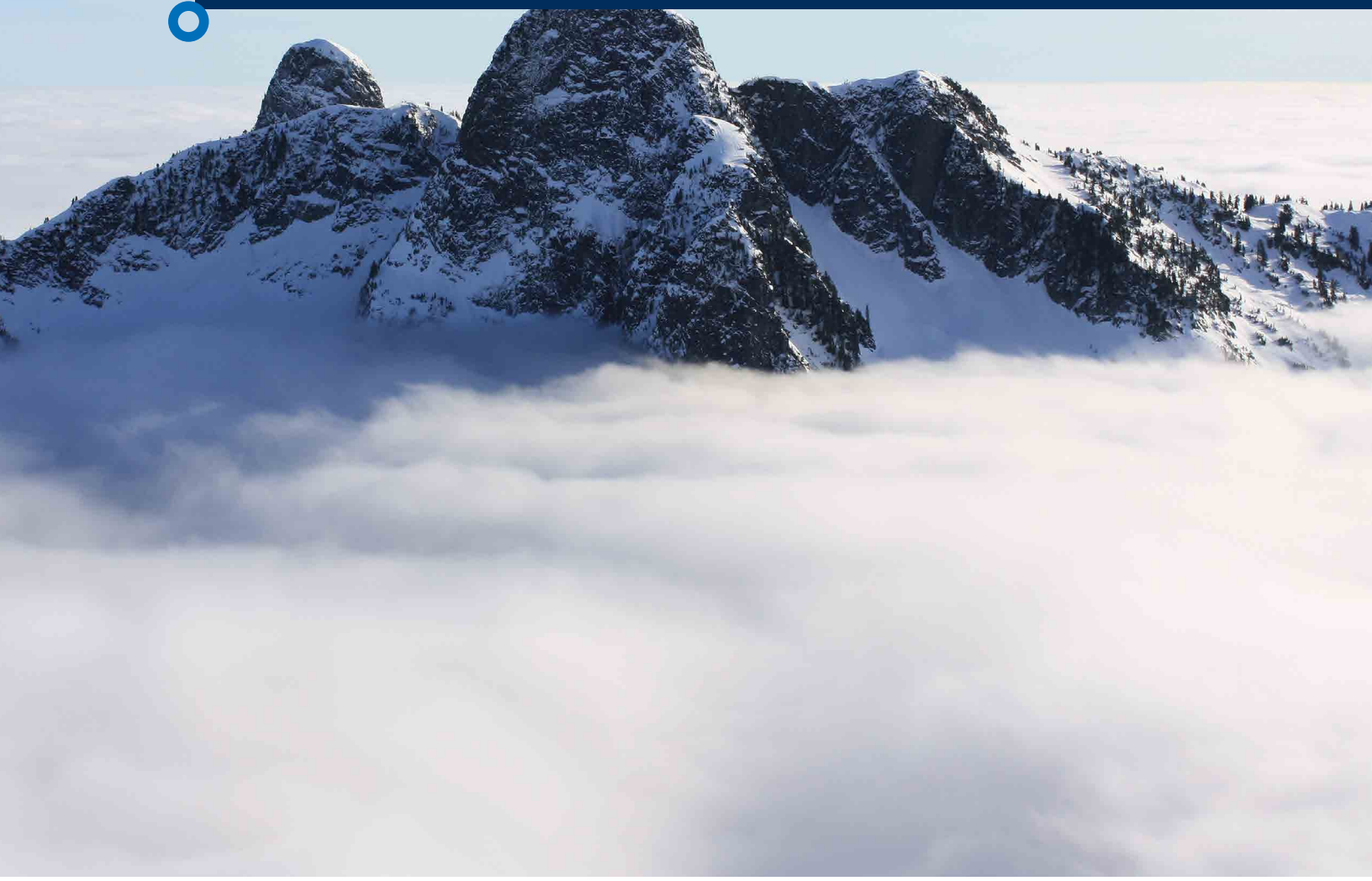
CLOUD SECURITY

Software-as-a-Service

Solution Primer



OPTIV

Executive Summary

There is absolutely no doubt that enterprises are adopting cloud applications using the Software as a Service (SaaS) model. In fact, recent reports from two leading cloud access security broker (CASB) vendors, Netskope and Skyhigh Networks, both show an astounding average number of applications in use in the enterprise. According to the Netskope February 2016 Worldwide Cloud Report, the average enterprise now has about 917 total cloud applications in use. Skyhigh Networks reports an even higher average in their Q4 2015 Cloud Adoption Risk Report, with an average number of 1,154 cloud services in use.

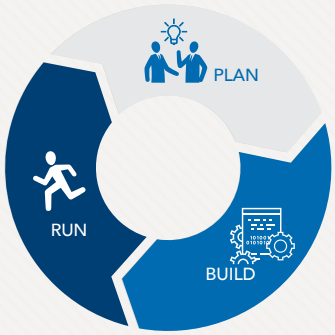
Enterprise users are adopting everything from cloud storage, collaboration tools, office suites and enterprise applications like HR and payroll tools through cloud service providers. Making matters worse for security organizations, many of these tools don't require much more than a credit card to adopt and begin using almost instantly. Data leakage isn't the only risk here, although it is a substantial one. Malware has evolved to leverage cloud applications to "fan out" and expand into organizations in never before seen ways.

When we consider the staggering numbers of cloud applications in use, it's difficult to see how security teams even stand a chance. Identifying cloud applications, monitoring usage and defending against security threats is a monumental task if a cloud security strategy addressing SaaS has not been developed and deployed. Even though tools exist to support the security organization's efforts, without the proper planning the requirements identification and threat modeling for these tools may not be utilized in the most optimal fashion.

It also may not directly align to the business' requirements. Every organization, from small business to large enterprise, must consider its goals, identify available resources to meet those goals and execute in a logical manner. This type of program strategy approach utilizing Optiv's SaaS cloud security maturity model enables the organization to decrease risks, intelligently allocate resources, measure goals attainment and ultimately benchmark against peer organizations that are also adopting the framework.

Problem and Approach

The SaaS cloud security program framework is a holistic approach to planning, building and running a program focused on protecting the organization.



Problem Statement

The Optiv SaaS cloud security program framework addresses the need security leaders have for rapidly maturing their cloud security approach, while learning from the lessons of peers across market verticals and company sizes. This research-backed maturity framework and operational guidance is focused on helping security leaders understand outcomes and orient capabilities development to achieve those outcomes that best suit the profile of the organization.

The SaaS cloud security program framework is a holistic approach to planning, building and running a program focused on protecting the organization. With the SaaS use case specifically in mind, this framework enables the organization to most effectively position its people, processes and technologies to reduce risks right now, while providing a milestone-based roadmap and strategy for achieving future risk reduction on a realistic timeline and budget.

Program Strategy Approach

The Optiv program strategy approach provides the tools necessary to plan, build and operate a successful program tailored to the organization's goals and available resources. The model builds upon a foundation called the program core that defines the program drivers, the business requirements and non-program support needed to achieve momentum and ensure the planning is done effectively. Once the program core is built and verified, the model starts to assist the organization with defining and setting realistic goals. These goals or outcomes offer an approach that starts with the end in mind.

Once the outcomes are determined, the model easily pivots along the functional program elements to define supporting capabilities that can be built up through supporting activities. These activities are supported by staff, process and technology requirements that are gathered and refined from hundreds of hours of research and study of organizations across varying levels of maturity and representative of the many market-verticals.

Overall, the purpose is to measure success. The initial definition of goals via the outcome model allows the IT or security leader to measure at the goal attainment level, then at the individual capabilities level to understand progress. This type of measurement model gives both a high-level executive overview, and insight into each individual capabilities development. Now, once the model is adopted, IT and security leaders can leverage benchmark data to compare their programs against each other.

Model Driven Program Development

The SaaS Cloud Security Maturity Model

Maturity Level	Description
Aware	As the initial level of maturity, "aware" is a realization and acknowledgement that cloud services (SaaS) are being consumed by enterprise employees.
Reactive	Once cloud services usage is acknowledged, the security organization moves to a passive discovery and on-demand assessment or triage model.
Adaptive	Through the reactive ongoing activities, the security organization develops patterns and begins addressing cloud services to meet identified, high-demand business requirements.
Purposeful	This maturity level is a pivot from a model where security teams retrofit security mechanisms onto already adopted cloud services, to one where security drives the conversation and delivers approved services based on business use cases.
Strategic	As the organization adopts cloud services based on use case and necessity, the security organization leads an effort to define strategic direction that may provide competitive advantage leveraging cloud services. Integration with existing security platforms becomes a fluid process.

Model Driven Program Development

Program Core

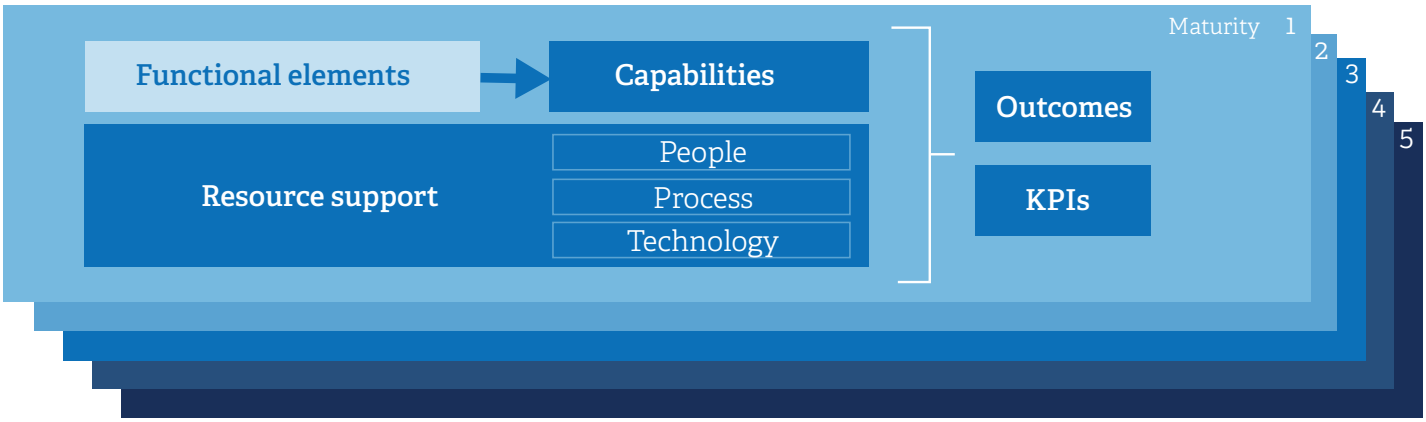
The program core is essentially the set of building blocks that acts as the foundation for the SaaS cloud security program. It includes the business drivers, the requirements and the outside support that the program development leadership needs to plan and build the foundation.

Program Drivers

Program drivers are defined as the base pieces of a business case for program development. These are the answers to the question of "Why would the business fund and support this program?" Often times there are regulatory pressures, internal board requirements as well as customer requirements. These program drivers act as the guideposts for program development goals (outcomes), and help the program lead define the appropriate avenue of engagement between business and security for the development of the program.

From our research, these include the following items:

- Regulations, including export control or other regional and local restrictions including HIPAA, FDA21CFR-Part 11, PCI-DSS and others
- Merger, acquisition and divestiture activity at highly dynamic organizations
- Increased adoption of a cloud-first applications sourcing model among agile businesses
- IT cost-reduction initiatives



Program core:

Drivers | Requirements | Non-program support

These program drivers act as the guideposts for program development goals (outcomes), and help the program lead define the appropriate avenue of engagement between business and security for the development of the program.

Model Driven Program Development

Requirements

Defining business requirements means identifying stakeholders and asking for input. The additional level of meta-analysis and refactoring allows our research process to aggregate several related requirements into a single view, which provides a unique perspective across the various market-verticals, company sizes and maturities. These requirements are generally from business stakeholders as well as IT stakeholders, as evident here.

- Ensure no disruption to processes and services delivery of critical business processes
- Support innovation while minimizing technical risk to the business
- Enable flexibility and collaboration, while maintaining security through confidentiality and enforcement of data ownership
- Support enhanced, next-generation disaster recovery and business continuity efforts with increased levels of security and data integrity

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. These are things that the security executive has influence over, but do not directly control and require partnerships throughout the enterprise and sometimes beyond. Based on data from our comprehensive cloud security focus groups, these include some of the following:

- Relationships to legal, audit, compliance and privacy roles and responsibilities within the organization
- Audit support, often separate from legal to independently validate requirements and policy adherence
- An active or maturing data governance program with identification of key assets within the organization

Outcome-Oriented Program Development

The focus on outcomes is an important differentiator for Optiv's model, in that we focus on an organization's goals to plot the most appropriate path forward. This approach allows us to model the capabilities required and activities to reach those capabilities at the desired maturity level. All of this begins with understanding the three key outcomes for the program, and how they are defined.

Outcome	Description
Policy	Policy helps define the type of approach and the documented framework for the SaaS cloud security program. Defining and setting policy is the first and most important step towards program development.
Understanding	Understanding defines the level of depth a security organization has about the usage of SaaS cloud services, including awareness and context.
Execution	Execution defines the way an organization takes actions to enforce policy, supported by the level of understanding gained at any given maturity level.

Model Driven Program Development

Modeling Outcomes to Maturity

	Policy	Understanding	Execution
Aware	Acceptable use policy (AUP) statement	Identification of cloud services and applications on a manual, per use case basis; no risk visibility	Detection of cloud application usage
Reactive	Tracking compliance to AUP; applying governance process on per incident basis	Cloud applications discovery through passive monitoring (log analysis, etc.); manual risk assessment	Application of appropriate level of action based on permit/deny policy
Adaptive	Regularly reviewed policy statement regarding data security for sanctioned applications	Cloud applications identification leveraging multiple tools, and partially automated risk assessment of sanctioned services	Policy-based enforcement of data security mechanisms on multiple tiers (approve/permit/deny)
Purposeful	Policy extended to define multiple tiers of cloud applications with regular review cycle	Automated identification and risk assessment of cloud applications at the business use case level	Policy-based enforcement of comprehensive security mechanisms on multiple tiers (approve/permit/deny)
Strategic	Published and enforced policy includes multiple tiers and guidelines for enforcement, review and update	Automated identification, and business risk-aligned assessment of cloud applications use	Fully operationalized and automated visibility, data security and monitoring mechanisms aligned to business objectives and use cases

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
Governance	This functional element defines the way the organization defines and delivers policy and then manages adherence to that policy.
Visibility	This functional element defines the manner in which the organization obtains insight into the usage of cloud services and associated risks.
Identity and Access Management	This functional element defines the manner in which the organization plans, builds and operationalizes the various identities and roles used for SaaS-based cloud services.
Threat Protection	This functional element defines how the organization prevents, detects, responds and recovers from the threats to SaaS-based cloud applications usage and associated data.
Compliance	This functional element defines how the organization manages and maintains adherence to policy both technical and non-technical including audit, reporting and recourse.
Data Security	This functional element defines how the organization applies data security principles such as encryption, data masking, data loss prevention and other features to SaaS-based application usage.

Assembling the Program

Optiv solutions research and development studies, develops and publishes program frameworks for the consumption of enterprise security leaders who are planning, building and operationalizing these frameworks as part of the overall enterprise security strategy. These research-based program guidance papers, blueprints, provide in-depth guidance from framing the foundation, to understanding the most appropriate level of outcome, through developing functional elements' capabilities and further into the various activities required to support goal attainment.

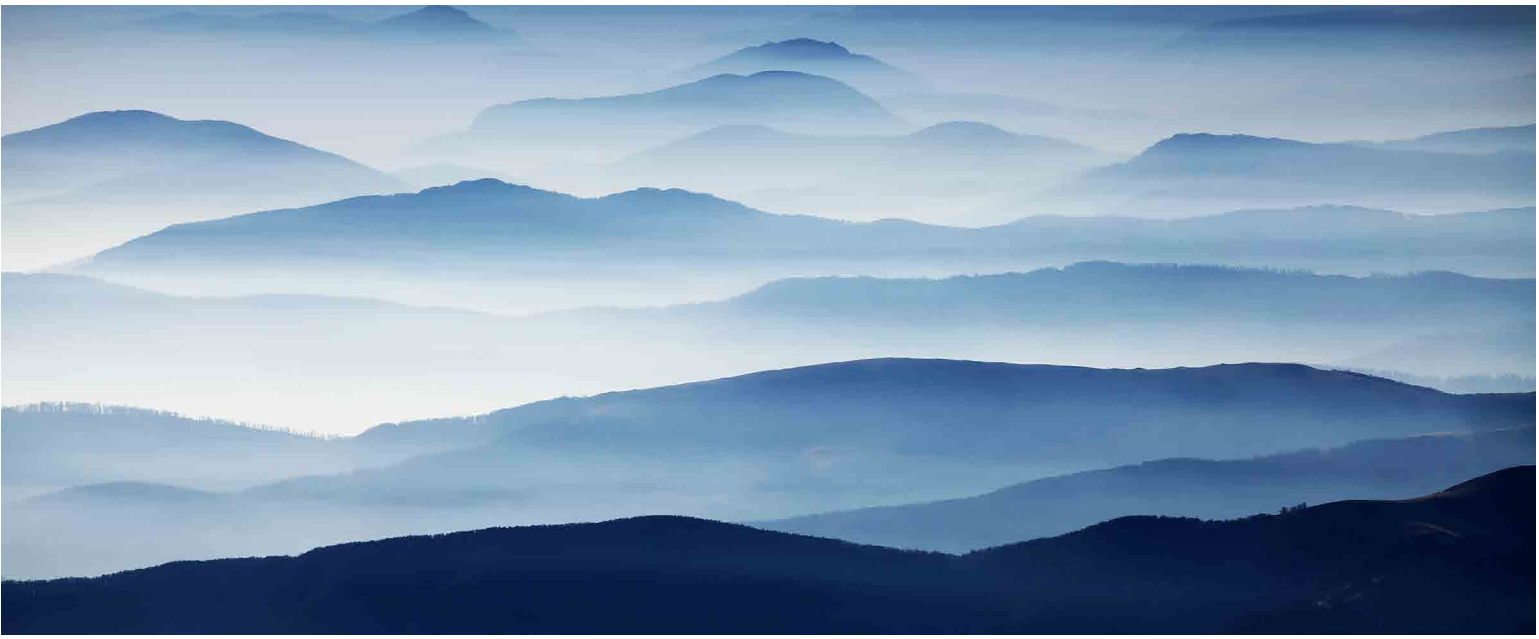
These comprehensive frameworks aide in driving the program development conversation, based on over a thousand hours of individual research, industry-diverse focus groups and one-on-one study of world-class organizations.

The framework presented herein, and expanded on in the blueprint papers, can be adopted independently by an organization or enrolled in a strategic program development program. This Optiv program tailors the blueprint guidance to individual organizational goals and resources while applying practitioner expertise.

The program blueprint is meant to be flexible and applicable to organizations across varying market segments and sizes while providing the benefit of measurement and benchmarking. Additionally, as these frameworks are adopted by organizations, the lessons learned via feedback are incorporated back into the continuously evolving guidance.

Harnessing the power of lessons learned, both successes and failures, is critical to the evolution of security as a discipline – and this framework is a step in that important direction.

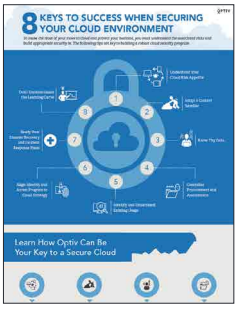
For more information, and to obtain your individually licensed copy of the SaaS Cloud Security Blueprint, contact your Optiv representative.



Want to learn more?

Insight on Cloud Security is an ongoing series of thought leadership at Optiv.
Click the links below to download other corresponding materials on the subject.

Cloud Solution Brief



Cloud Security Infographic

Rafal Los
Managing Director
Solutions Research, Optiv

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

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.