Assess Your Cloud Security Readiness

Leverage Forrester's Custom Tool To Assess Your Cloud Security Maturity Across Six Major Technology Competencies

by Andras Cser
May 29, 2020

Why Read This Report

As firms migrate computing and data resources to the cloud, security remains a top concern and priority for both operational and compliance reasons. S&R professionals should use our custom tool, a quick, 20-question assessment (available both as a spreadsheet and online), to: 1) establish your firm's maturity of cloud security and 2) get actionable guidance on how to improve and expand cloud security coverage to reduce threat surface and protect cloud workloads and data more effectively.

Key Takeaways

Assess 20 Activities In Six Competency Areas
We identified 20 activities and divided them into six competency areas: governance, measurement, people, process, strategy, and technology. You can use the spreadsheet assessment to answer a question about each activity. We then roll up your answers to activity questions to formulate a score and level of maturity of each competency.

Beef Up Cloud Security Before Starting Your Cloud Migration
For organizations that have not yet started their migration to the cloud, this assessment is a great starting point for learning how to strengthen your cloud security posture.

Use The Tool To Create Cloud Security Targets And Track Progress Over Time
It's vital to complete this cloud security assessment at least once every 12 to 18 months to get an updated picture of your company's cloud security posture and to reevaluate strategy. Good strategy, measurement, and reporting on cloud security's coverage of workloads are the most effective means for getting and maintaining executive support to protect cloud data and resources.

Assess Your Cloud Security Readiness

Leverage Forrester's Custom Tool To Assess Your Cloud Security Maturity Across Six Major Technology Competencies

by Andras Cser
with Merritt Maxim, Benjamin Corey, and Peggy Dostie
May 29, 2020

Table Of Contents

Related Research Documents

Best Practices: Cloud Governance

Best Practices: Selecting And Deploying Cloud Security Gateways

The Forrester Wave™: Cloud Workload Security, Q4 2019

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Data In Dynamically Changing Clouds Brings Security Challenges

Although the cloud creates numerous benefits, it also creates numerous security headaches when it comes to planning migrations from on-premises to the cloud and protecting data and resources in the new cloud workloads. Consider these four challenges:

- **Lots of disparate data creeps into many locations.** Firms have a primal fear of losing data, whether via data breaches, misconfiguration, or user error, any of which can reduce a firm's goodwill and brand value and lead to expensive remediation costs and potential regulatory fines. Firms have to look in many places and cover a lot of bases: They must protect structured data (databases, data in SaaS/PaaS) and unstructured data (documents, spreadsheets, schematics, files) across clouds. With sporadic encryption, as with Salesforce's native Shield encryption, the inventory, search, sort, and filtering of sensitive data is harder still: Even when cloud services support encryption, it may be clunky or challenging to use. Privacy regimes and data and route sovereignty compliance requirements only exacerbate the problem.
- **Security must coexist in a multicloud world.** In today's mishmash of on-premises, edge computing, and private and public cloud environments, it's difficult to keep track of workloads and understand where they live and the security controls managing them. A North American financial institution told Forrester that its IT security department in general can't keep up with the rate of migration of on-premises workloads to the cloud. Forrester Analytics survey data indicates that 75% of global infrastructure decision makers would describe their cloud strategy as hybrid.[1] Almost every firm follows a multicloud strategy because of legacy infrastructure ("we have a little bit of everything") or to avoid vendor lock-in.
- **Cloud setup is easy to (mis)configure.** With cloud platforms, and integration of continuous integration/continuous development (CI/CD) pipelines, identity and credential management of administrators, cloud instance, and storage configuration are not only easy and quick to configure, they're also easy to misconfigure. McAfee's 2019 Cloud Adoption and Threat Report found that threat events in the cloud, such as compromised account, privileged user, or insider threat, have increased 27.7% year-over-year.[2] The recent July 2019 CapitalOne and Imperva breaches are examples of cloud security breaches stemming from cloud misconfiguration.
- **Multiple varied stakeholders are all (trying) to call the shots.** We regularly talk to internal departments dueling over who should own cloud security. Invariably, IT security and operations, along with Dev(Sec)Ops are at the table, but we often hear about compliance, network ops/security, and cloud architecture wanting to have a say about cloud security governance, strategy, and tooling. Adding to the complexity is that many currently deployed (and often legacy "lift-and-shift" security tooling) struggle to provide a customizable but single pane with remediation capabilities for all of these relevant stakeholders. Cloud governance vendors such as CSG and CloudKnox help with automation here.

Six Competencies Paint The Whole Picture Of Cloud Security Posture

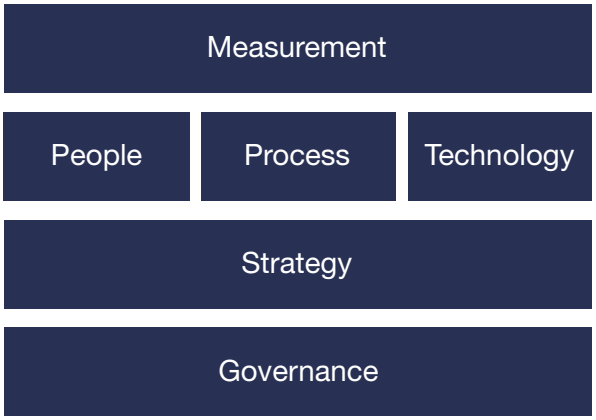
To help you gauge your firm's cloud security maturity, we created Forrester's Cloud Security Maturity Assessment (see embedded Excel file). We include six major competencies and their weightings: governance (20%), measurement (10%), people (10%), process (10%), strategy (10%), and technology (40%) along with subsets of activities for each (see Figure 1):

- **Governance lays the groundwork and organizational support of cloud security.** Governance is the starting point of any robust cloud security regime.[3] Advanced firms define various activities and overlay the definitions with RACI charts.[4] Firms should also conduct detailed cloud provider vendor assessments to ensure that vendors meet regulatory compliance requirements and are able to ensure data and route sovereignty. Finally, to underpin organizational support, firms need clear, written, and periodically updated internal ownership definitions for cloud security.
- **Strategy provides outlook to what's happening in the broader cloud security market.** Cloud security is not a static process. As cloud platforms mature, they offer more functionality and more native security features. Cross-cloud coverage is also a key requirement. Firms should plan to update their documented cloud security strategy at least annually and put cadence into investigating new cloud security technologies (such as serverless security and network path validation).[5] A UK financial services firm has half a full-time employee (FTE) dedicated to this.
- **People can make or break the entire cloud security posture.** As with any security initiative, people a play a great role in making it a success. Involving DevOps, DevSecOps, and traditional application development professionals in decisions ensures that your firm can cover all kinds of cloud workloads in an agile, scalable way. Separation of duties for cloud admins is also important: No admin should have unfettered access to all cloud resources all the time; this includes various production and nonproduction environments, cloud platforms, and service types. A French manufacturer ensures through cloud platform reporting that admins don't have simultaneous access to configuring instances and starting/stopping instances.
- **Process is critical for repeatability, accuracy, and cost-effectiveness.** Cloud security requires a repeatable process of ensuring that workloads enter a rigorous security regime, especially for migrating workloads from on-premises to the cloud (as the cloud may offer vastly different security features, data storage, configuration options, etc.). The firm also needs to codify and periodically update security policies it must or desires to follow, for example, what encryption to use, how to manage encryption keys, and what cloud storage configurations are acceptable.
- **Technology tooling delivers automation to free you up for strategy decisions.** Cloud security is easier and less expensive to automate using tools. Firms should use tooling to centrally manage, enforce, and audit: 1) administrative access to cloud service provider consoles; 2) data encryption and decryption in cloud workloads; 3) all network egress and ingress points; 4) sensitive cloud data governance; 5) analytics to detect threats and misconfiguration; 6) the integration of third-party threat analytics to provide a 360-degree view of their threat model; 7) cloud workload

security (CWS) solutions that continually track and manage security posture of cloud workloads; and 8) cloud security gateways to intercept and block sensitive or malicious data moving between workloads.

› **Measurement ensures that tools and process are effective.** No cloud security regime is complete without actual measurements. Since there are so many data breaches related to lost or stolen cloud platform credentials, it's a good idea to measure and track the unmanaged admin credentials and keep them at less than 5% of all your active credentials. AWS and Azure Security Center logs will help discover which credentials have to be managed. Detecting and reporting the number and risk level of the compliance and security violations also goes a long way toward understanding and minimizing your organization's security exposure.

FIGURE 1 Six Functional Areas Of Cloud Security Readiness



Expand The Scope Of Cloud Security Competencies Gradually, Evenly

Once you've completed the spreadsheet assessment, it will generate an overall maturity level between 0 (nonexistent) and 5 (optimized) and help translate maturity levels into characteristics of overall maturity (see Figure 2). Then it's time for you to take action. Here's what to do at each level:

› **Beginner.** Map out your business processes and data that impact your organization's cloud security strategy. Focus on getting a sound governance and process around cloud security so that you can show senior stakeholders that cloud security isn't just a bunch of disparate technology investments but also takes careful coordination and planning. Work on engaging your compliance, DevOps, and network operations peers in cloud security strategy planning meetings. Ensure you have a central, single pane of glass for insight and interception of threats.

› **Intermediate.** Lay the technology foundation of cloud security and be sure you have at least 50% coverage across all activities listed in the technology competency. Aim for covering at least 50% to 60% of cloud workloads. Invest in security of the CI/CD process for container creation, container scanning. Ensure that you have complete coverage of network ingress and egress points. Lastly, be sure to formally update and track changes to your organization's cloud security strategy. Many firms will also have to use cloud security tooling to rationalize cloud infrastructure utilization in order to reduce operating costs.

› **Advanced.** Firms at this stage should expand their coverage of cloud security to at least 90% of workloads and unify all cloud security management of public, private, managed, and edge computing clouds to a single console. At this stage, it's important to have equally strong and cost-conscious protection of workloads (file integrity and malware), hypervisors (attacks against the hypervisor and storage), containers (shift-left scanning and orchestration platform protection), and serverless (understanding and securing API communications).

FIGURE 2 Legend For The Cloud Security Assessment Scale

Level	Characteristics
0 — Nonexistent	Not understood, not formalized, and need is not recognized
1 — Ad hoc	Occasional, not consistent, not planned, and disorganized
2 — Repeatable	Intuitive, not documented, and occurs only when necessary
3 — Defined	Documented, predictable, evaluated occasionally, and understood
4 — Measured	Well-managed, formal, often automated, and evaluated frequently
5 — Optimized	Continuous, effective, integrated, proactive, and broadly automated

Recommendations

Tune The Model To Fit Your Organization

S&R pros should be prepared to adjust the model based on your organization's unique requirements and incorporate dialogue, collaboration, and feedback from colleagues in cloud procurement, cloud architecture, DevOps, security, infrastructure and operations, enterprise architecture, application development, audit, and lines of business. To get the best value when adopting the model, keep these key tactics in mind:

› **Reduce scope as needed.** Our model is meant to provide broad coverage of several key cloud security functional areas. Some areas may have priority and relevance to your organization based

on your current environment. You can use the model's weightings to reflect these priorities and, if needed, exclude specific areas.

- **Establish a baseline and maturity level targets.** Although aiming for a level 5 maturity score in every area is a lofty goal, it may be impractical for personnel or budgetary reasons. Use your initial results to identify unacceptable gaps or areas, based on factors such as risk, budget, or compliance, that you can easily improve. These quick wins can build momentum, show progress, convince naysayers and executives, and keep the team engaged. For larger organizations with more autonomous business units, consider separate assessments, heat maps, and strategies for individual business units or geographies.
- **Measure and report progress at regular intervals but at least biannually.** Evaluating your cloud security maturity is not a one-time effort; this is meant to be a straightforward and repeatable exercise, so make sure you create a schedule for measuring progress over time. Regularly reporting to executive management (preferably quarterly but at least biannually) helps demonstrate the value of security investments and the results of implementation efforts.

Supplemental Material

Online Resource

The online version of this report includes a maturity assessment, which can be accessed online or downloaded as a spreadsheet. Click the links at the beginning of this report on Forrester.com to access both formats.

Endnotes

[1] Base: 3,359 global infrastructure decision makers whose firms are planning, implementing, or expanding cloud adoption. Source: Forrester Analytics Global Business Technographics® Infrastructure Survey, 2019.

[2] Source: "Cloud Adoption and Risk Report," McAfee, 2019 (https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf).

[3] See the Forrester report "Best Practices: Cloud Governance."

[4] Each letter in the acronym RACI represents a level of task accountability: responsible, accountable, consulted, informed.

[5] See the Forrester report "The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019."

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.