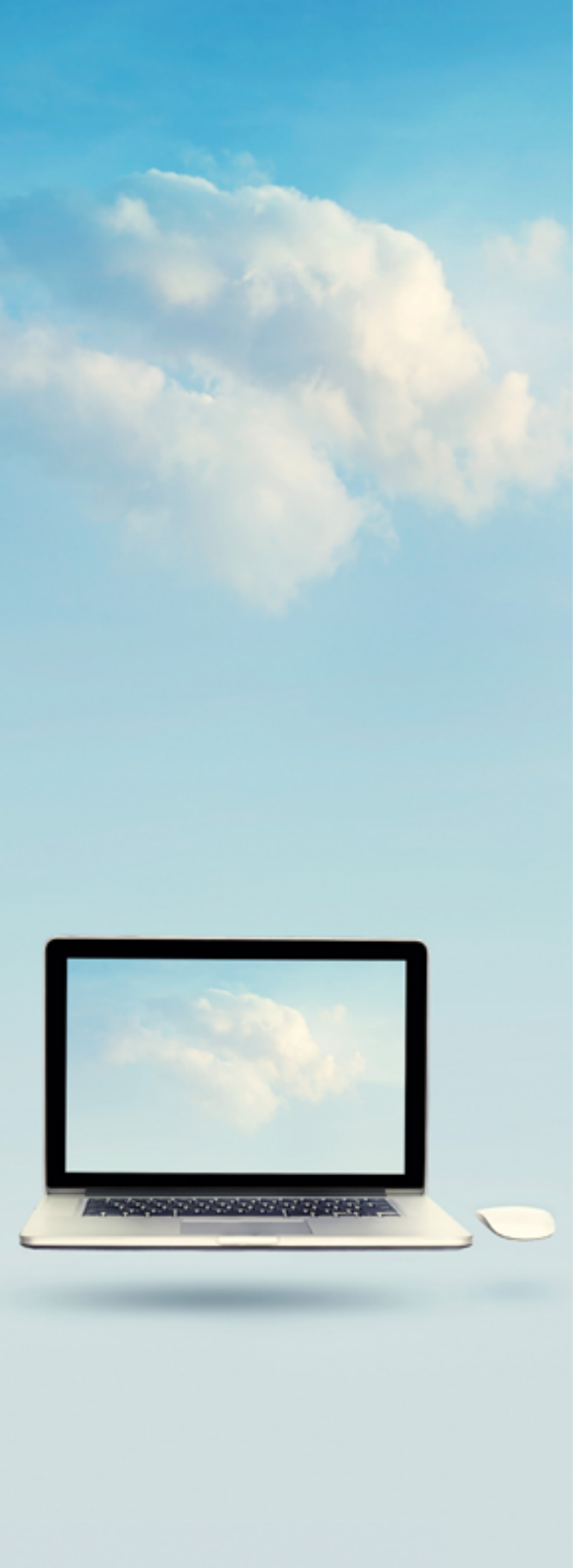
SECURITY COMPASS WHITEPAPER

Cloud Migration: How To Move Your Applications Securely

Security Compass

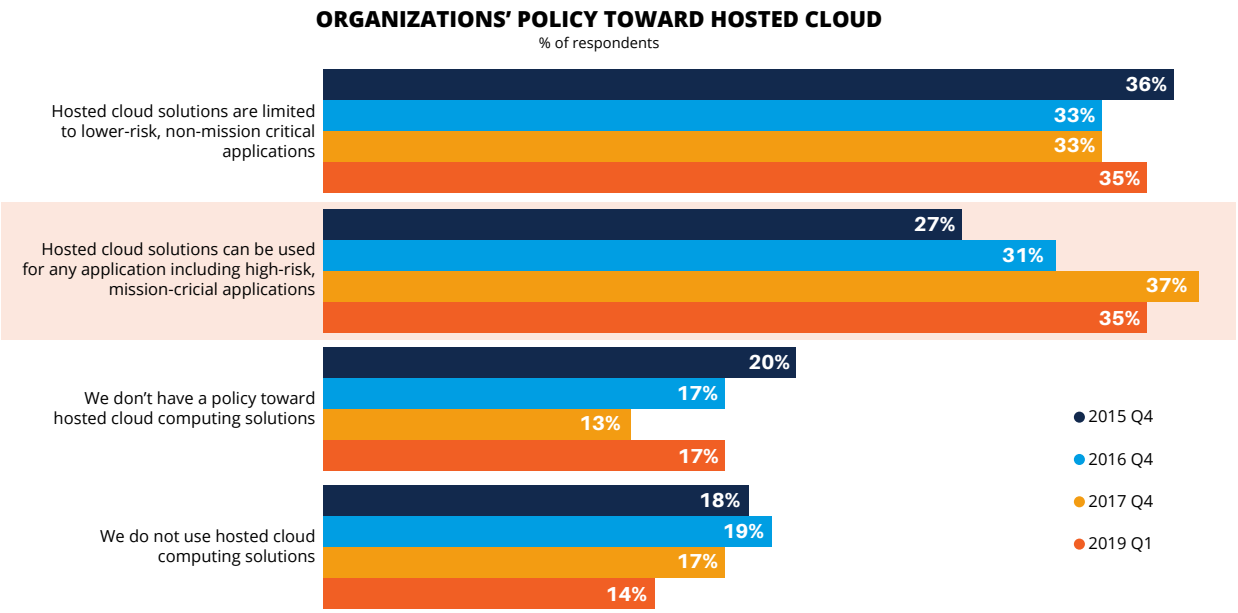


What's spurring the move to the cloud

The journey of moving workloads — infrastructure, applications, and other computing resources — to the cloud has begun. For many organizations, the onset of a global pandemic accelerated this move as people had to pivot to working remotely.

Additionally, the shift in the perception of cloud security risk among organizations is driving the migration of workloads to the cloud. 451 Research, a technology research group within S&P Global Market Intelligence, has been tracking the perception of cloud risk among large organizations since 2015.

The key finding? There are fewer enterprises these days saying the cloud is 'too risky' for high-risk applications.



Source: 451 Research, Voice of the Enterprise Information Security, Budgets & Outlook 2019

Two notable trends have emerged from their study:

1. In 2015, around 15 percent of the organizations were not using any kind of cloud computing infrastructure. This percentage declined to 14 percent in the year 2019.

2. Secondly, about 27 percent of the organizations considered using cloud computing solutions for any applications, including high-risk and mission critical, in 2015. Four years later, about 35 percent of the organizations were considering it for all applications.

So what has changed since 2015 to influence the perception of cloud security risk? A lot.

451 Research explains it succinctly, "Partner networks, marketplace offerings, the controls and guardrails built into the cloud offerings themselves, and a vendor ecosystem of cloud infrastructure security offerings have all improved over time."

As cloud adoption continues, it is more important than ever to boost cloud security, starting from when workloads are moved to the cloud, to reduce the risk of introducing vulnerabilities into these environments — whether they are public, hybrid, or multi-cloud.

Mitigating cloud migration risks when you revise, rearchitect or rebuild applications

Gartner recommends following an application-specific migration plan that adheres to an organization's cloud strategy and principles. For each application you have decided to move to the cloud, according to Gartner, you will need to determine the most appropriate strategy for migrating applications to a cloud-native platform on an application-by-application basis:

Five R's Cloud Migration Framework

This graphic was published by Gartner, Inc.

- **REHOST:** Move the application to new infrastructure. This could include moving from bare-metal or dedicated VM infrastructure in a traditional infrastructure and operations (I&O) model to operating in IaaS to take advantage of cloud computing.

- **REVISE:** Perhaps you are past rehosting and need to reconfigure your app for cloud services. For instance, you may choose to leverage a dbPaaS of MySQL over hosting it yourself on IaaS or introducing an external caching mechanism for session state.

- **REARCHITECT:** Support modernization in your codebase and major architectural components. This requires major revisions to take advantage of cloud characteristics and your CSP's feature set.

- **REBUILD:** Rearchitect is a prerequisite to rebuild and entails moving to your CSP's application platform.

- **REPLACE:** Discard your existing app in favor of a SaaS application." Gartner, How to Modernize Your Application to Adopt Cloud-Native Architecture, March 2020

SD Elements, a Balanced Development Automation tool, helps to ensure security and speed by automating key parts of proactive security processes that currently slow down any cloud migration activities.

Revising in-house applications

The “revise” migration strategy suggests optimization of the infrastructure and supporting services of an application. This requires reconfiguring the application, the system, and the application dependencies while leaving the source code mainly unchanged. For example, you might update an application to make use of an external, cloud-native logging solution (e.g. from syslog to AWS CloudTrail), or queuing solution (e.g. from RabbitMQ to Amazon MQ).

SD Elements offers capabilities that benefit this migration strategy, including:

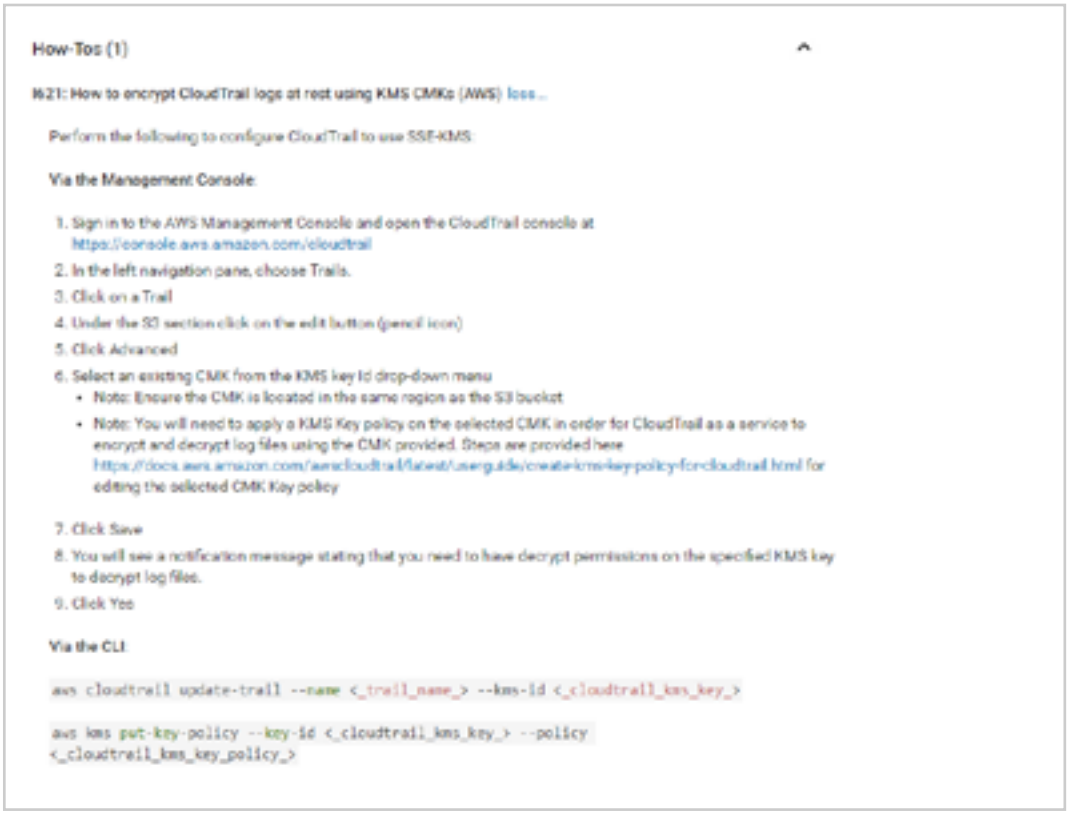
- **Secure configuration of cloud services**

  As you move workloads to the cloud, logical access and risk mitigation controls become paramount. This spans the data (which remains yours), as well as the cloud resources, identities, access controls, and configurations that you provision.

  SD Elements provides detailed configuration guidelines based on the Center for Internet Security (CIS) Benchmarks™ to help you successfully carry out your share of responsibilities in securing cloud resources, including Infrastructure as a Service (IaaS) platforms from market-leading vendors such as Google, Amazon, and Microsoft, container technologies like Docker, and orchestration tools such as Kubernetes.

  SD Elements also provides guidance for DevOps and cloud migration teams to implement essential security concepts, such as Identity and Access Management (IAM) and encryption, for various cloud services.

  Sample encryption guidance for AWS CloudTrail logs in SD Elements:



How-Tos (1)

#21: How to encrypt CloudTrail logs at rest using KMS CMKs (AWS) less...

Perform the following to configure CloudTrail to use SSE-KMS:

Via the Management Console:

1. Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail
2. In the left navigation pane, choose Trails.
3. Click on a Trail
4. Under the S3 section click on the edit button (pencil icon)
5. Click Advanced
6. Select an existing CMK from the KMS key Id drop-down menu
   - Note: Ensure the CMK is located in the same region as the S3 bucket
   - Note: You will need to apply a KMS Key policy on the selected CMK in order for CloudTrail as a service to encrypt and decrypt log files using the CMK provided. Steps are provided here https://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-kms-key-policy-for-cloudtrail.html for editing the selected CMK Key policy
7. Click Save
8. You will see a notification message stating that you need to have decrypt permissions on the specified KMS key to decrypt log files.
9. Click Yes

Via the CLI:

```
aws cloudtrail update-trail --name <_trail_name_> --kms-id <_cloudtrail_kms_key_>

aws kms put-key-policy --key-id <_cloudtrail_kms_key_> --policy
<_cloudtrail_kms_key_policy_>
```

Other configuration services covered by SD Elements include: Storage Services, Domain Name Services (DNS), Notification Services, Key Management Services, Load Balancing Services, Database Services, and more.

SD Elements Supporting Services		
AWS Services	**Azure Services**	**Google Cloud Services**
AMI Aurora Auto Scaling CloudFront CloudWatch Confid DynamoDB EBS ECS ELB IAM KMS Lambda RDS Route53 S3 SNS SQS VPC	Active Directory Azure Functions Key Vault Monitor Multi-Factor Authentication Network Watcher Resource Manager Security Center SQL Database Storage Virtual Machines Virtual Network	Cloud IAM Compute Engine Virtual Private Cloud (VPC) Cloud DNS Cloud Storage Cloud SQL Cloud Audit Logs Stackdriver Cloud Key Management Service Kubernetes Engine

Completed configuration activities can later be verified with Cloud Posture Software Management (CPSM) tools.

- **Reinforcement of security best practices and regulations for cloud computing**

  SD Elements offers guidance for DevOps teams on information security best practices for cloud computing based on the Cloud Security Assurance (CSA) Cloud Controls Matrix (CCM), a cybersecurity controls framework aligned to the Security Guidance v4 and a de-facto standard for cloud security assurance and compliance.

  The controls in the CCM are mapped against industry-accepted security standards, regulations, and control frameworks including but not limited to: ISO 27001/27002/27017/27018, NIST SP 800-53, AICPA TSC, ENISA Information Assurance Framework, German BSI C5, PCI DSS, ISACA COBIT, NERC CIP, and many others.

  To ensure the implementation of these best practices before deployment, applications in SD Elements can be associated with a predefined risk policy that can be leveraged to create security gates in CI/CD pipelines.

  SD Elements also helps ensure compliance with other regulations that have cloud-specific requirements, such as CCPA, GDPR, and ISO/IEC 27001, which is the most commonly used control framework globally, and is commonly and successfully used in the cloud service context.

Rearchitecting applications

This alternative requires materially altering the application so that you can shift it to a cloud-optimized architecture, and make heavy use of cloud-native capabilities.

Once you have decided on the components of your cloud architecture, use SD Elements to model the requirements for a cloud-optimized application, incorporating information security best practices from the CSA Cloud Controls Matrix discussed previously. You can then leverage this as a baseline to conduct an analysis of security gaps with your current application.

Rebuilding applications

The rebuild alternative proposes that you leverage cloud-native application platforms such as Amazon Web Services (AWS) Lambda, AWS Elastic Beanstalk, and Google Kubernetes Engine (GKE) to build, deploy, and operate the application.

Use SD Elements to model the technology stack as well as security and compliance requirements for the applications you have decided to rebuild. As you define the profile of the application, SD Elements automates the identification of known information security & compliance risks and corresponding countermeasures, particularly those covered in the CCM and CIS Benchmarks, that are relevant to your application. It also ranks project risks based on your pre-defined criteria to help your DevOps teams prioritize activities.

The countermeasures recommended in SD Elements are based on best security practices and include code snippets across a wide variety of programming languages & frameworks, including cloud-native systems. Your development teams can quickly incorporate these code snippets into their code so that they can build and integrate secure code faster.

SD Elements also includes short, just-in-time training videos that empower your development and operations teams with the knowledge to carry out the task at hand.

When applications are tested for security vulnerabilities using popular application security testing tools, SD Elements can automatically take feedback from these tools and associate the results back to the task and the requirement. Ultimately, this high-value correlation provides your teams and leaders with the ability to trace and report on current risk mitigation status at the project, application, or business unit level.

To accelerate your time to market for secure software, relevant security and compliance requirements, countermeasures, code snippets and training videos, which are all important building blocks for a secure application, can be delivered directly to your developers' existing toolchain, such as Jira, VersionOne, or Azure Boards. SD Elements' ability to integrate with a wide variety of SDLC systems ensures your DevOps teams comply with security requirements while they are in the code creation and deployment process.

Cloud security governance and operations

Beyond identifying relevant security and compliance guidelines for certain migration alternatives, SD Elements also provides guidelines to mitigate privacy and security risks associated with cloud governance and operations. It incorporates the risks and corresponding controls articulated by the European Network and Information Security Agency (ENISA) in its publication "Cloud computing: Benefits, risks and recommendations for information security" across three categories:

- Policy and organizational (governance and operational policies),
- Technical (provider planning and multi-tenancy risks), and
- Legal (compliance and privacy regulations).

Reporting

SD Elements aides cloud vendors and end users in simplifying the assessment of cloud security controls implementation. The platform generates a report that summarizes the status of application security tasks mapped to the various security frameworks and industry regulations.

The CSA Cloud Controls Matrix Report in SD Elements can be also used as a checklist to assess the security of cloud security providers, particularly in relation to the development and/or deployment of their application.

How SD Elements works

SD Elements infuses automation through four key steps common across proactive security processes, such as threat modeling, risk assessments, and implementation of secure coding and deployment guidelines.

1

Gathers info about your project, either from existing data sources or a configurable survey.

2

It then assigns a risk classification, and a powerful logic engine crawls our expert content library for relevant security and compliance risks. Accordingly, it suggests countermeasures.

3

Based on that, DevOps teams receive detailed requirements, code samples and short, relevant training modules right in their issue trackers, such as Jira.

4

Next, it imports results from your code scanning tools to automatically validate which security activities were completed and which are outstanding.

5

It instantly produces detailed reports so your teams know exactly where their risk lies.

You can view our datasheet for more information on security and technology frameworks, and industry regulations covered by SD Elements. Connect with us for a free demo.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001