

# The Beginner's Guide to Secure Cloud Configurations

A micro e-book for using CIS Benchmarks™ and  
CIS Hardened Images® to secure public cloud accounts,  
cloud products and services, operating systems, and more.

## Contents

Introduction .....	1
Understanding Shared Cloud Security Responsibility .....	2
Begin at the Beginning: What are CIS Benchmarks? .....	3
New Resource: CIS Cloud Product Benchmarks .....	3
The Specifics of CIS Cloud Product and Services Benchmarks .....	4
An Evolution of Secure Cloud Configurations .....	5
A Faster Way to VM Security: CIS Hardened Images .....	6
Contribute: Get Involved with CIS Benchmarks Communities .....	7
Learn More: Access These Cloud Security Resources .....	7

## Introduction

Over the past decade, organizations around the world rapidly shifted how they use IT platforms, networks, and devices to support their missions. Technological advances in the cloud made it possible to outsource data storage to cloud service providers (CSPs) so seamlessly that most end users never even noticed the transition.

The ongoing improvements to the speed, capabilities, and reliability of cloud computing provides efficiencies of scale that enable rapid deployment of cloud products and services. This transformation has not been without its challenges, however. Chief among them is the need to ensure security and the protection of data in a cloud environment.

This micro e-book from the Center for Internet Security, Inc.® (CIS®) includes the following topics:

- Understanding shared cloud security responsibility
- Begin at the beginning: What are CIS Benchmark?
- New resource: CIS Cloud Product Benchmarks
- The specifics of CIS Cloud Product and Services Benchmarks
- An evolution of secure cloud configurations
- A faster way to VM security: CIS Hardened Images
- Contribute: Get involved with CIS communities
- Learn more: Access these cloud security resources

## Understanding Shared Cloud Security Responsibility

Responsibility	On-premises	IaaS	PaaS	SaaS	FaaS	CIS Controls Cloud Companion Guide	CIS Foundations Benchmarks
Data classification and accountability		●	●	●	●	●	✓
Client and end-point protection		●	●	●	●	●	✓
Identity and access management		●	●	●	●	●	✓
Application-level controls		●	●	●	●	●	✓
Network controls		●	●	●	●	●	✓
Operating systems		●	●	●	●	●	✓
Physical security		●	●	●	●	●	

Source: Amazon Web Services, <https://aws.amazon.com/compliance/shared-responsibility-model>.

● Cloud Customer ● Cloud Provider

CSPs recognize the importance of implementing security measures to protect their data centers from recognized threats. However, the ultimate responsibility for organizational data security always rests with the IT and information security professionals at the client organization.

Rather than leaving the responsibility and trust solely in the CSP's hands, the security actions an organization is responsible for and the security actions the CSP should manage go hand-in-hand.

This creates an ongoing burden for the cloud consumer to securely configure and maintain their environments. Resources like the CIS Benchmarks and CIS Hardened Images (both explained further into this e-book) help companies achieve a portion of their shared responsibility.

## Begin at the Beginning: What are CIS Benchmarks?

The CIS Benchmarks are secure configuration guidelines designed to safeguard devices and systems against today's evolving cyber threats. Available at no cost in PDF format, they include more than 100 configuration guidelines across 25+ vendor product families. CIS Benchmarks are available for operating systems, servers, cloud service providers, mobile devices, desktop software, and network devices.

Developed by a global community of cybersecurity experts, the CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia worldwide. The recommendations map to the CIS Controls where applicable, to further support an enterprise's overall security against cyber-attacks.

Recognized as an industry standard and referenced specifically by FISMA, FedRAMP, PCI DSS, NIST, HIPAA, and more, many organizations use the CIS Benchmarks for regulatory compliance. The CIS Benchmarks don't just state what to configure; they also provide extensive details on how to configure each setting, including a description, rationale, audit, and impact.

→ [Download a free CIS Benchmark](#)

## New Resource: CIS Cloud Product Benchmarks

As the cloud progresses with more products and services, CIS has responded with more resources to assist in securing the capabilities in the cloud. To do this, CIS called upon its global network of expert volunteers to expand their guidance for the public cloud. This effort resulted in CIS Benchmarks specific to the CSP's products and services.


Rather than create a CIS Benchmark for every unique service, CIS followed the lead of the CSPs and grouped services by CSP product. Each CSP offers dozens of products, which groups cloud services based on the function they provide.

For example, in the product, [AWS End User Compute Services](#), one of the services, [Amazon WorkDocs](#), helps users create and store content in the cloud.

These product-level CIS Benchmarks complement the CIS Foundations Benchmarks. This symbiosis is rooted in security at your first access point (your cloud account), and then an additional layer of security is built into services that you use within that account. CIS works directly with the CSPs to identify the top-used products and services on each platform, and then uses that information to inform the development plan for future CIS Benchmarks.

All CIS Benchmark recommendations reference other guidelines and additional resources. With these cloud guides, CIS demonstrates the relationship between the CIS Benchmarks and the CSP documentation. The intention is to inform the user of the guidance available from the CSP, for both security and other topics. Becoming familiar with both CIS and the CSP's documentation helps the user recognize the responsibility the CSP has, and is assisting with, when running the service.




## The Specifics of CIS Cloud Product and Services Benchmarks



**CIS AWS End User Compute Services Benchmark**  
Secure configuration guidance for AWS core computing services

### CIS Benchmarks for Cloud Products

Secure subsets of related cloud services


 <b>Amazon WorkSpaces</b> Virtual desktops in the cloud	 <b>Amazon AppStream 2.0</b> Stream desktop applications to a browser	 <b>Amazon WorkDocs</b> Create and store content in the cloud
--	--	--

The first release of a cloud product-level CIS Benchmark is the [CIS AWS End User Compute Services Benchmark](#). This includes configuration recommendations for:

- Amazon WorkSpaces
- Amazon WorkDocs
- Amazon AppStream 2.0
- Amazon WorkLink

The user can choose the applicable services and configure accordingly to what's running in their environment.




In some cases, the configurations needed for services warrants a CIS Benchmark specific to one cloud service. In these cases, the product-level CIS Benchmark will include a section for the service, but it will point to the CIS Benchmark for the service. An example of the standalone cloud service CIS Benchmarks are the CIS Kubernetes Benchmarks.



**CIS Amazon Elastic Kubernetes Service (EKS) Benchmark**  
Securely run Kubernetes applications with CIS guidance

### CIS Benchmarks for Cloud Services

Extensive guidance for commonly used public cloud services

 <b>Worker Nodes</b> Configure file permissions and ownership for kubelets	 <b>Managed Services</b> Using AWS Key Management Service and other tools for security	 <b>Pod Security Policies</b> Minimize admission of certain unwanted containers
---	---	--

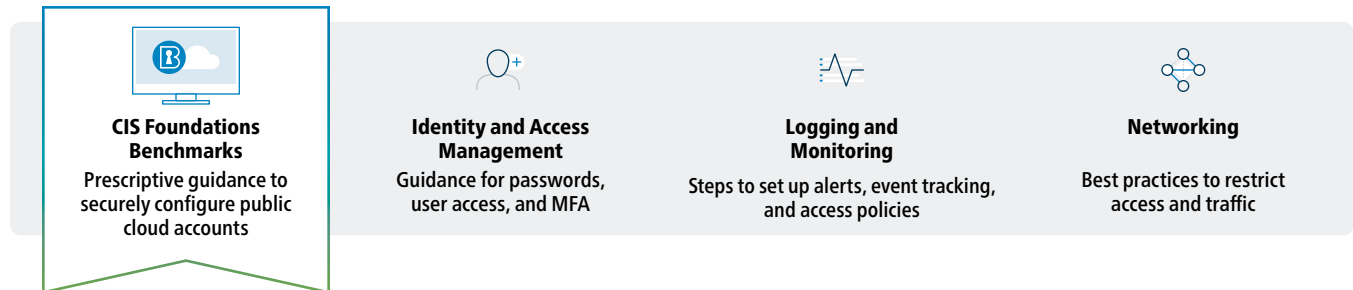
CIS currently offers multiple CIS Benchmarks for Kubernetes:

- Amazon Elastic Kubernetes (EKS)
- Google Kubernetes Service (GKE)
- Oracle Container Engine for Kubernetes (OKE)

CIS plans to release CIS Benchmarks for Azure Kubernetes Service, Alibaba Kubernetes, and Red Hat OpenShift Kubernetes in the coming months.

→ [Download a CIS Kubernetes Benchmark](#)

## An Evolution of Secure Cloud Configurations



Similar to the product and services CIS Benchmarks, CIS works with the CSPs and the consensus community to develop prescriptive guidance for cloud account security. This guidance is known as the CIS Foundations Benchmarks.

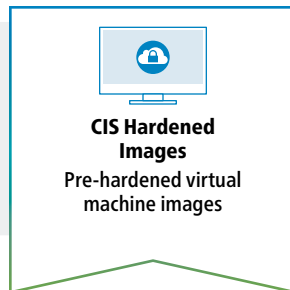
With this in mind, know that the CIS Foundations Benchmarks are the first step to secure a public cloud account. The CIS Foundations Benchmarks are part of a portfolio of globally-recognized resources provided by CIS to help organizations secure their operations in public cloud environments. While all CIS Foundations Benchmarks offer recommendations tailored to the tools and services of their respective CSPs, the documents all have common features and are organized with a similar structure. The guidance covers identity and access management (IAM), logging and monitoring, networking, and more.

CIS now offers Foundations Benchmarks for:

- [Amazon Web Services \(AWS\)](#)
- [Microsoft Azure](#)
- [Google Cloud Platform \(GCP\)](#)
- [Oracle Cloud](#)
- [IBM Cloud](#)
- [Alibaba Cloud](#)

CIS Foundations Benchmarks help users take action for a portion of their responsibility in the shared responsibility model.

## A Faster Way to VM Security: CIS Hardened Images



**CIS Benchmarks in the Cloud**  
Hardened to CIS Benchmark recommendations



**Compliance Mappings**  
CIS Benchmarks and Hardened Images are recognized by a variety of compliance frameworks



**Audit and Assess**  
All CIS Hardened Images include an assessment report for easy configuration audits

If an organization provisions operating systems from the cloud, securing them should be a top priority. Unlike securing the simpler cloud services, the configuration needs of operating systems (OS) are unique and complex.

CIS Hardened Images can help cloud consumers meet the expectations of the shared responsibility model (as previously mentioned) at the OS and application level.

Whether you're using Windows or Linux, CIS offers hardened virtual machine images (CIS Hardened Images) configured to CIS Benchmarks for operating systems.

There are currently 30 different CIS Hardened Images available on the following marketplaces:

- [Amazon Web Services](#)
- [Microsoft Azure](#)
- [Google Cloud Platform](#)
- [Oracle Cloud](#)

CIS Hardened Images significantly reduce common threats such as malware, insufficient authorization, and remote intrusion. CIS Hardened Images are updated on a monthly basis to align with any updates to the CIS Benchmarks. The images are also patched according to any updates to the OS. To easily audit the configurations in the images, each CIS Hardened Image includes an assessment report from CIS's configuration assessment tool, CIS-CAT Pro®. The report notes any CIS Benchmark recommendations not included in the image along with a score of conformance to the guide.

→ [Learn more about CIS Hardened Images](#)



## Contribute: Get Involved with CIS Benchmarks Communities

CIS relies upon the community and its partners to assist in developing and maintaining CIS Benchmarks. The CIS Community includes subject matter experts, vendors, technical writers, and CIS SecureSuite Members from around the world. Together, with the CIS teams, they work to develop, review, and maintain the CIS Benchmarks, bringing real-world experience and expertise to the process. Without community participation, there would be no CIS Benchmarks, as they are the heart of what drives development and consensus.

All CIS Benchmark development occurs on [CIS WorkBench](#), a community development platform. It starts with creating the scope and initial draft for the technology. Subject matter experts are key to creating this initial content, as it is the foundation for the continued development and publication of the CIS Benchmark.

After the initial draft is complete, announcements are made via social media and to members that the draft is available; volunteers are invited to join the community to review, test, and provide feedback. This is the consensus process, and can lead to more discussion and adjustments to the CIS Benchmark as necessary, ensuring that the recommendations are complete and represent comprehensive guidance.

Once all feedback is reviewed and addressed, CIS makes a final call for participation to the community. The final review period lasts an average of two weeks. Any final feedback received is addressed, and once complete, the CIS Benchmark is published and made publicly available.

→ [Join a Community](#)





## Learn More: Access These Cloud Security Resources

- [CISecurity.org](#)
- [CIS Controls Cloud Companion Guide](#)
- [CIS Shared Responsibility Model Guide](#)
- [CIS Benchmarks](#)
- [CIS Foundations Benchmarks](#)
- [CIS Kubernetes Benchmarks](#)
- [CIS Hardened Images](#)
- [CIS WorkBench](#)



The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit [CISecurity.org](https://www.cisecurity.org) or follow us on Twitter: @CISecurity.

-  [cisecurity.org](https://www.cisecurity.org)
-  [info@cisecurity.org](mailto:info@cisecurity.org)
-  518-266-3460
-  [Center for Internet Security](https://www.linkedin.com/company/center-for-internet-security)
-  [@CISecurity](https://twitter.com/CISecurity)
-  [CenterforIntSec](https://www.facebook.com/CenterforIntSec)
-  [TheCISecurity](https://www.youtube.com/channel/UCTheCISecurity)
-  [cisecurity](https://www.instagram.com/cisecurity)