


# Futureproofing Your IT Career: Skills for Securing Hybrid Cloud Environments



**The opportunities for cloud services are endless. So are the business benefits that the cloud offers, such as more efficient use of resources, scalability, and customized applications.**

The challenges of cloud security are significant. Some of these challenges, such as complexity, are long-standing in IT.

Those benefits can be delivered anytime, anywhere, and on any device. They extend to software, data, and documents. Rapid access to new software is always available to manage workloads or to innovate. On top of all this, cloud services deliver impressive cost efficiencies.

Leveraging the cloud also means that IT must manage a mashup of technology setups from both inside and outside the organization. This is an enormous new challenge, and its complexity can cause security risks and vulnerabilities.

The challenges of cloud security are significant. Some of these challenges, such as complexity, are long-standing in IT. Others have arisen with the cloud—especially with the public cloud. The lure of quick access to hot new apps has tempted many organizational departments to bypass the security measures put in place to protect information.

As a result, the data centers that host cloud services are experiencing whiplash. Lingering security concerns, data sovereignty, and regulatory requirements have led many organizations to claw back some sensitive workloads away from the public cloud. In fact, 65 percent of respondents in a Forbes survey pulled back from the public cloud due to a variety of concerns, including security and the need for a multicloud strategy.<sup>1</sup>

Now organizations are seeking to hire data center professionals with the necessary skills to manage and secure these hybrid environments. Could they be looking for you?

This white paper will accomplish the following:

- Provide an overview of cloud adoption at the enterprise level
- Examine the security considerations around public clouds
- Review the IT skills needed to plan, implement, and manage security for hybrid IT infrastructures
- Outline the Cisco certifications for hybrid IT security skills
- Present the case for certifications as key to long-term career success

## The cloud has become a value strategy

Cloud has come a long way since the days of point-to-point data circuits and virtual private networks (VPNs). The Cloud Security Alliance (CSA) predicts that software as a service (SaaS) will grow at 19.7 percent between 2016 and 2020.<sup>2</sup>

1. Forbes Insights, "[When Clouds Connect: How Hybrid IT Is Transforming Enterprises](#)," November 2016.

2. Cloud Security Alliance, "[Mitigating Risk for Cloud Applications](#)," (PDF) August 2016.

By design, cloud computing is on-demand and shared. That means enterprises must be prepared to protect users, data, applications, and physical security wherever they operate.

Why the rush to leverage the cloud? Because it is now regarded as a strategy for maximizing shareholder value, the CSA points out. Decisions about adopting the cloud are being made in the boardroom. Gartner predicts more than \$1 trillion in IT spending will be impacted directly or indirectly by the cloud.<sup>3</sup>

With the cloud in a strategic role, everything in IT is changing. Innovation is rapidly shifting to the cloud.<sup>4</sup> A growing number of businesses use a cloud-first approach to product design, while some technology and business innovations can be accessed only as cloud services. This includes advances in the Internet of Things (IoT) and artificial intelligence (AI).

But there remain concerns around cloud adoption. “Keep in mind that not all projects can utilize cloud services due to regulatory or security concerns or even the money that has been invested in the projects,” Gartner adds. “Also, some enterprises might lack the correct skill sets and talent.”

## Cloud security has become a priority

By design, cloud computing is on-demand and shared. That means enterprises must be prepared to protect users, data, applications, and physical security wherever they operate. This raises some security issues. The CSA surveyed industry experts to put together a list of top cloud computing security concerns.<sup>5</sup>

Of those who responded to the survey, 93 percent are still concerned about shadow IT, or the use of cloud-based applications without express approval of the organization. Some 62 percent of respondents’ organizations have policies discouraging the use of unsanctioned apps, while 38 percent block unapproved apps. Only 29 percent use a proxy or firewall to redirect insider attempts to access cloud apps.

Most of those surveyed have reported cloud security incidents. Of those reporting such events, 59 percent were related to external sharing, and 47 percent were about access from unauthorized devices. Respondents also were concerned about the lack of visibility into cloud activity. Fewer than half (49 percent) know where and when sensitive data is being downloaded from the cloud. Other challenges include not enough threat visibility in the network or across workloads and applications. These challenges impact the cloud’s ability to deliver on its promise of better business efficiency, and it must be addressed.

3. Gartner, “[Gartner Says by 2020 ‘Cloud Shift’ Will Affect More than \\$1 Trillion in IT Spending](#),” July 2016.

4. Kasey Panetta, Gartner, “[Cloud Computing Enters Its Second Decade](#),” January 2017.

5. Cloud Security Alliance, “[Mitigating Risk for Cloud Applications](#),” (PDF) August 2016.



The rise of cloud services is causing an explosion of data center traffic because all those services are hosted and processed in the data center.

## Cloud traffic hits the data center

The rise of cloud services is causing an explosion of data center traffic because all those services are hosted and processed in the data center. As a result, the data center is undergoing an extreme makeover. And it's bringing the rest of IT along for a wild ride.

The Cisco Global Cloud Index predicts a more than threefold rise in data center traffic between 2015 and 2020.<sup>6</sup> That's up from 3.9 zettabytes (ZB) per year to 14.1 ZB a year. By 2020, 92 percent of global data center traffic will stem from cloud services and applications.

In turn, soaring data center traffic is pushing storage needs through the stratosphere. By 2020, data center storage installed capacity will zoom to 1.8 ZB from 382 exabytes (EB) in 2015, growing nearly five-fold. Globally, the information stored in data centers will quintuple to reach 915 EB by 2020.

Today's data center is far different from what it was just five years ago. It is more powerful and agile, and it incorporates digital technologies such as virtualization, integrated analytics, and threat mitigation.

All of this indicates a greater need for investments in data centers that can handle the explosion of IT infrastructure, along with restrictions on space.

Investments in data centers are growing at a 5.8 percent higher compound annual rate than before and will rise to \$16 billion, according to IDC's Worldwide Datacenter Network Forecast, 2015–2019.

Organizations are updating their data centers. They are modernizing and merging smaller ones into bigger centers with the capacity to run the cloud and a wide range of other digital technologies. Data center security is necessary to protect workloads and physical environments everywhere.

## The hybrid data center is more flexible

IDC predicts that through 2018, 65 percent of data center investments will be used for client-facing systems. That includes engagement, analytics, and IoT, although not as much for back-office systems such as ERP. Further, 60 percent of companies will rely on highly automated data centers to boost efficiency.

The goal? To tie data center investments to business value.

Hybrid data center strategies are frequently being deployed, as they enable flexibility, efficiency, and appropriate technology choices that support specific business requirements. This approach allows organizations to have applications hosted wherever they make the most sense for the business.

---

6. Cisco, "[Cisco Global Cloud Index: Forecast and Methodology, 2015–2020](#)," 2016.

IT managers everywhere are saying that security is now a responsibility for everyone in the organization.

The hybrid data center concept also enables organizations to divide their IT workloads. These traditionally have been located in conventional enterprise or legacy IT systems. In the hybrid model, workloads and data can be split. For example, one group is on-premises private clouds for sensitive or critical missions. The rest reside in off-premises providers of managed or hosted services.

Hybrid IT is a way for organizations with legacy IT systems to implement appropriate applications in the cloud with the ability to run the other business workloads on their traditional IT infrastructure. Balancing workloads between older IT systems and the cloud is a challenge. However, its flexibility makes it outstanding for meeting business needs.

Hybrid IT makes an organization much more flexible, better able to control costs and develop new products, find new markets, or create new business models much faster. As a result, the IT workforce will be required to adapt its skills to this new environment while also acquiring new skills.

## Now IT pros must broaden their skills

IT managers everywhere are saying that security is now a responsibility for everyone in the organization. That means protecting both physical infrastructure and workloads wherever they are critical concerns.

IT organizations typically have dedicated security specialists responsible for comprehensive security strategy and in-depth implementation and monitoring. Data center practitioners are involved in far more of the infrastructure than ever before, including elements of data center security. They often work in conjunction with the team's security specialists.

Data center professionals are often asked to have knowledge of data center security in several areas:

- Remote connectivity solutions
- Data center firewall technologies
- Maintenance for network integrity and security
- Access control
- Security protocols
- Data storage protection

Senior data center professionals work hand in hand with the security leads within the IT team to design, implement, and ensure compliance with respective company policies. For example, this can entail automating security-related policies across the networked resources.

IT professionals can earn any number of certifications to demonstrate that they have knowledge and skills for hybrid IT and cybersecurity.

According to Enterprise Strategy Group, 46 percent of organizations globally reported a shortage of cybersecurity skills in 2016.<sup>7</sup> The previous year, just 28 percent of organizations reported the same—an 18-point hike in just 12 months.

Breaking the numbers down, 33 percent of organizations say they are short on cloud security skills. Another 28 percent cite a lack of network security expertise, and 26 percent say they are missing data security specialists.

IT professionals in an increasingly hybrid environment cannot afford a narrow view of what they do. They must expand their thinking to embrace a holistic perspective of both the on-premises data center and the cloud. The role of an IT professional in any capacity has greatly expanded.

## Cisco certifications are ideal for hybrid IT

So, where do all these developments leave IT professionals? With one heck of a career opportunity. IT professionals can earn any number of certifications to demonstrate that they have knowledge and skills for hybrid IT and cybersecurity. Cisco's certifications cover all key aspects of data center planning: design, setup, managing, and troubleshooting. These skills include policy-driven infrastructure, application-centric infrastructure (ACI), fabric, virtualization, SDN, secure data center, and cloud integration. Additionally, Cisco offers certifications specifically for those professionals who are focused extensively on security skills.

The [Cisco Certified Network Associate \(CCNA\) Data Center certification](#) is ideal for anyone with one to three years of relevant work experience. It is appropriate for a network administrator or systems engineer. Workdays consist of setting up and deploying network management systems—monitoring and tweaking the performance of data center components.

The position also requires installing, configuring, and scheduling equipment maintenance, along with upgrading data center systems and network devices, such as switches, hubs, routers, bridges, and storage. In this role, the top priority is ensuring the best performance of the center's hardware and software.

The CCNA Data Center certification validates skills at installing, configuring, and maintaining the data center. It covers networking, data center storage, virtualization, authentication, and authorization, along with understanding automation and orchestration to participate in cloud projects, and ACI. It's a great on-ramp certification for validating essential skills, and it can provide a competitive edge for a first hybrid cloud or IT job.

7. Jon Oltsik, Enterprise Strategy Group, "[ESG Blog: High-Demand Cybersecurity Skill Sets](#)," May 2016.

The CCNP Data Center certification is a great choice because it helps develop deeper skills. It also demonstrates that the professional has attained a career level of proficiency in new data center technologies.

Those who wish to expand or validate their skills as a security-focused IT professional may consider the Cisco Security track, starting with the [CCNA Security certification](#). A prerequisite is to earn the Cisco Certified Entry Networking Technician (CCENT) certification and to have at least one year of experience in networking.

The next step is the [Cisco Certified Network Professional \(CCNP\) Data Center certification](#). This certification is for those who have five to eight years of experience as a senior network engineer, a presales engineer, a design engineer, or a data center administrator. A technical degree in IT, computer science, or engineering is required.

This certification might be ideal for those who work in a medium to large data center. The focus is wide, ranging from designing and implementing to troubleshooting and operating the data center infrastructure. This can involve unified computing, networking, storage, automation, data center security, virtualization, and ACI. All this is necessary to securely provide high service levels. The job holder also may supervise data center staff and help make the data center serve business needs.

The challenge is balancing troubleshooting with expanding job requirements. These professionals may be working on large projects and wish to improve their skills to keep pace with factors such as cloud or automation. They also may wish to implement a policy-driven infrastructure, which is especially valuable in hybrid data centers.

The CCNP Data Center certification is a great choice because it helps develop deeper skills. It also demonstrates that the professional has attained a career level of proficiency in new data center technologies. Cisco also offers the [CCNP Security certification](#) for those who wish to take a deeper dive into security.

One of the highest levels of data center certification is [Cisco Certified Internetworking Expert \(CCIE\) Data Center certification](#). It is an excellent choice for IT professionals with at least eight years of experience. They typically work in a leading role, such as data center architect, senior network engineer, or senior systems engineer.

This role is changing rapidly due to emerging new data center technologies, such as cloud and automation. The challenge is to understand how the data center serves business requirements. Professionals in this area are also expected to have hands-on deep technical expertise.

Perhaps a major new project with expanded job responsibilities has prompted an IT professional to raise the skills level even further. The CCIE Data Center certification demonstrates that professionals have attained the highest level of expertise in everything related to data center. It also provides a competitive edge in the job market.

Today's savvy employers are looking for talented professionals who can leverage ever-changing technologies to operate the business more efficiently, serve external and internal customers better, and develop new markets and even new business models.

The CCIE certification is different from the certifications that precede it. Typically, this level of expertise is in the order of eight or more years of IT experience in progressively senior-level contributor or leadership roles. CCIE is the industry's most prestigious certification, validating the career achievements that brought a professional to this point. [CCIE Security certification](#) is also an option for those who wish to validate their high-level network security expertise.

## Looking ahead

The overall outlook is positive because today's hybrid computing model houses the services, information, and applications that deliver value to the business.

Today's savvy employers are looking for talented professionals who can leverage ever-changing technologies to operate the business more efficiently, serve external and internal customers better, and develop new markets and even new business models.

With Cisco certifications, today's IT professionals can master the challenges of an ever-changing hybrid IT and security landscape. Join us and learn more about our excellent training resources for [data center](#) and [cybersecurity](#).