Cloud computing has been around since at least 2000 when Salesforce.com emerged as one of the first major “software as a service” (SaaS) providers, offering sales automation tools for the CRM application market.

Since then cloud computing has exploded, with both major vendors and lean start-ups rolling out a growing variety of cloud-based services for enterprises, including storage and computational services as well as software (applications) and infrastructure. In addition, cloud services such as Dropbox that target the consumer market are increasingly being used by employees to store enterprise data—often without IT’s knowledge.

Yet many enterprises have avoided cloud computing altogether or dabbled tentatively. The main obstacle to enterprise cloud deployment, according to a new survey of more than 350 IT executives by Unisys and IDG Research, is security. More than 70% of the respondents cite security concerns as their biggest hurdle in deploying cloud-based strategies at their organization, while nearly half of respondents (45%) express concerns about information governance.

Despite widespread apprehension about security, enterprises and government entities will continue to increase cloud deployments as the benefits—lower software and hardware costs, virtually unlimited storage, improved collaboration, faster development cycles, increased productivity, and enhanced analytics—become increasingly obvious. A recent study from research firm IHS Technology predicts that enterprise spending on cloud computing will reach $235 billion in 2017, triple the $78.2 billion spent in 2011.
What can enterprise IT professionals do to ensure that their cloud deployments are secure? The answer can be complex, given the wide variety of cloud platforms (public, private, and hybrid) and models (SaaS and infrastructure as a service, or IaaS).

By taking into consideration a number of fundamental security principles and best practices, by understanding the specific security needs of an enterprise and evaluating different cloud environments and models, and by asking vendors the right questions, IT pros should be able to leverage essential cloud services while meeting enterprise security requirements.

**Rogue clouds in the enterprise**

The first step on the road to cloud security is to conduct an initial assessment of current cloud use in your enterprise. Even if an enterprise does not have a cloud vendor under contract, it is likely that some employees and even entire departments are using cloud services without notifying IT. Many enterprise workers use free cloud services to share large, confidential corporate documents, some of which contain product plans, sales reports, strategy roadmaps, and other proprietary information. Even if done with the best of intentions, this rogue use of cloud resources presents dangers to an enterprise.

“There’s always a risk that anyone using unacknowledged or unauthorized cloud services may not be following policy,” says Amy DeCarlo, principal analyst, security and data center services, for IT research and consulting firm Current Analysis. “There’s also risk if the provider does not have all of the appropriate security controls. There may be other issues that aren’t specifically security related, but might put the integrity of data at risk. And there are questions around compliance: Will rogue cloud use in some way endanger a company’s compliance with a government regulation or industry mandate, or even its own corporate governance?”

Rogue cloud use also poses a threat to the enterprise beyond introducing specific security vulnerabilities, DeCarlo says.

“It can feed a renegade culture, one of less control, less caution, and fewer concerns about following enterprise policy,” she says. “So you enable an environment in which different organizations feel they can create whatever IT services they need on the fly, and these may not actually map well to the efficiency of the business and its overarching corporate goals.”

The way to avoid such a potentially damaging scenario is to bring rogue cloud out into the open in a way that doesn’t threaten employees—and even turns it to the enterprise’s advantage.

“Being a little realistic, some of this is going to happen. So trying to get a handle on rogue cloud use without making people feel like they’re going to be punished by it is important,” she says.

**Public, private, and hybrid clouds**

In order to set effective in-house cloud security policies, enterprise IT professionals need to understand the basic types of clouds as well as their unique security needs, risks, and compliance requirements. This knowledge is essential when enterprises embark upon a search for a formal cloud services vendor.

Public clouds—in which a hosting provider stores data and applications for multiple tenants—are the most popular cloud option, in large part because of their low cost. But public clouds are inexpensive (and sometimes free) for a reason: Tenants share the host’s hardware, software, and network devices; nothing is dedicated to any one client. Further, public clouds are accessed across the public Internet.

More than 70% of the respondents cite security concerns as their biggest hurdle in deploying cloud-based strategies at their organization, while nearly half of respondents (45%) express concerns about information governance.
“There are all kinds of concerns about public clouds having a lot of points of exposure for data,” DeCarlo says. “There’s a risk of commingling data with another tenant in a public cloud environment, so another client may end up with access to your company’s data.”

That’s if the data is contractually yours. Data ownership disputes are common with public cloud vendors, many of whose contracts claim ownership of the data they store as legal protection in the event of data loss or theft. Asserting contractual ownership also allows public cloud hosts free access to a tenant’s data. Remember, there’s the danger of disgruntled employees everywhere.

Public clouds also can introduce serious compliance issues for an enterprise. Further, if a public cloud host uses virtualization software, it may be vulnerable to exploits that can attack virtual servers and guests. This requires close management of the patch processes.

Since the inherent risks and limitations of public clouds usually make them impractical for running mission-critical apps or storing proprietary data, larger enterprises typically opt instead to use a private cloud.

Private clouds offer enterprises a single-tenant environment in which the host dedicates the use of specific hardware, servers, and network assets to one client. This difference alone makes private clouds inherently more secure than public clouds—at least in theory.

“With a private cloud, it depends on how the cloud is architected,” says DeCarlo. “You may have a private cloud running on a customer’s premises, and it may also be on a third-party provider’s data center with a private connection (co-location comes to mind). But there may be some gap or some area where you’re going through the third-party provider’s data center. So you don’t necessarily have control within the private cloud provider’s data center. You don’t inherently know that there is no exposure of that data to another client.”

Hybrid clouds, a third option, offer enterprises a chance to store less important data and apps in a multitenant environment while reserving dedicated cloud services and equipment for higher-priority data and applications.

**SaaS and IaaS**

Beyond understanding the unique security concerns of different cloud environments (public, private, hybrid), it is important that enterprises grasp security considerations for SaaS and IaaS. The oldest and most popular cloud delivery model is SaaS. Apps are delivered via the Internet from third-party providers (such as Salesforce, Google, or Microsoft) to customers who can access the applications with a Web browser. The SaaS vendor manages all aspects of service delivery, and client downloads and installations are kept to a minimum.

Because SaaS essentially is a public cloud, most software delivered through this model tends to be less mission-critical. DeCarlo says that is changing, however.

“We’re beginning to see more enterprise-class applications and more operationally important SaaS applications,” she says. “It’ll be interesting to see how they can be handled in terms of security in a public cloud without compromising performance.”

Cloud infrastructure services, or IaaS, offer customers a full range of equipment and services, including storage, networking, and computational power. IaaS provides tenants with an infrastructure upon which they can implement platforms. Customers install a virtual server on the provider’s IT infrastructure and are billed based on resources used.

IaaS tenants also must manage several components. In addition to applications and data, this includes middleware, application runtime, and operating systems. This ability to manipulate within the cloud introduces the possibility of compromising data. IaaS tenants, for example, may inadvertently delete or alter data they neglected to back up, or they may allow unauthorized access to confidential or proprietary data.

While the various cloud environments and models each have some unique security challenges, they also share fundamental characteristics that introduce elements of risk to an enterprise.
“With cloud, you’re talking about handing over some level of control to IT resources and application workloads, in some cases to a third party,” DeCarlo says. “That opens up exposure, even in a private cloud, to unauthorized use, misuse of data, and other issues.”

These security issues are inherent to the basic nature of cloud computing. Other potential dangers can be vendor-specific. And enterprises must weigh cloud concerns against the vulnerabilities of on-premises data centers, too.

“There’s the risk that the third-party provider—and I think this is the biggest risk—doesn’t have the proper physical and logical security controls in place, and may not be following best practices,” DeCarlo says. “Also, the provider may be dealing with another provider. So there are all kinds of potential complications that might apply to all of these.”

**Putting it all together**

Enterprises face a number of considerations and trade-offs when shopping for a cloud vendor, including performance, price, and feature sets. Still, while security “is not the only criterion someone should look at,” DeCarlo says, “it is really critical.”

“If you have a mission-critical application and you think there’s some big advantage to putting it into the cloud, but it contains some kind of trade secret or something that is absolutely critical to the way the company is run, then security is the top priority,” she says.

Once decision makers determine which cloud environment and model they want to use for their enterprise, they should approach vendors seeking specific information about security-related issues.

“There are fundamental things that need to be addressed,” DeCarlo says. Among the questions to ask cloud providers are:

- Where geographically will your data and apps be stored, and in what cloud data center(s)?
- What kind of encryption does the vendor use?
- How are encryption keys managed?
- Does the vendor employ multifactor authentication?
- Who will see and have access to your data?
- What is the vendor’s disaster recovery plan?
- How does the cloud vendor handle incident response and notification?
- Where is the physical data center, and how is it secured?
- What is the age and condition of the provider’s physical equipment?
- Are there regular third-party audits of the host’s services and facilities?
- Does the vendor meet compliance requirements?
- What security details and agreements are written into the SLA?

Further, while it’s important to pin down cloud providers regarding security-related logistics and guarantees, enterprises also need to be aware of the bigger picture.

“It’s not just all about line items,” DeCarlo says. “It’s about the provider being able to have your trust, either through past experience or from the provider’s reputation in terms of its ability to deliver something that’s reliable and secure.”