WHITE PAPER

Is the Public Cloud Really More Secure?

Insights from the Experts

SecureWorks®

Executive Summary

When organizations consider moving application workloads to the public cloud, a common fear is the safety of their data in the cloud. As with any new technology, the public cloud introduces new risks. However, it also offers significant benefits, not only for agility and transformation, but also for revisiting information security and data integrity approaches. According to Jay Heiser of Gartner Research, "Organizations that haven't taken a strategic approach to the secure use of cloud computing can easily use it in a manner that is less secure than traditional computing, resulting in unnecessary compliance incidents and data losses."[1] In this paper, SecureWorks experts discuss insights and recommendations regarding if, when and how the public cloud can be a more secure deployment choice than your legacy on-premises environment.

Introduction

Migrating computing workloads to the cloud can be a great way to improve application availability, performance, and operational costs. However, perceived issues with public cloud security can be a deterrent. Organizations should overcome their current status quo mindset, along with an aging patchwork of technologies, to modernize and embrace the innovation and automation that secure cloud computing offers. But is the public cloud really less secure than a conventional on-premises or private cloud deployment? Or, is the public cloud potentially *more* secure?

While there are legitimate challenges to public cloud security, they can be managed with smart preparation, management and response. In this paper, experts from SecureWorks share insights garnered across numerous client engagements and IT implementations on evaluating cloud security and provide recommended strategies to safely leverage the cloud in your organization.

[1]Heiser, Jay, Gartner Research, "Clouds Are Secure. Are You Using Them Securely?", July 21, 2016.

"Organizations that haven't taken a strategic approach to the secure use of cloud computing can easily use it in a manner that is less secure than traditional computing, resulting in unnecessary compliance incidents and data losses."

—Jay Heiser, VP of Research, Gartner Research

Five Questions for Assessing the Security of Your Public Cloud

When you put your data in the cloud, you're putting your data and trust in a third-party organization. The wisdom and safety of that choice reflects a balance of several factors, including cloud benefits, risks and your definition of "secure". In some cases, cloud security benefits are readily apparent. For example, a cloud provider's hardened, weatherproof data center generally offers far better environmental security than an on-premises facility in a flood-prone basement. In other cases, assessing the suitability of public cloud security for your requirements is more complex.

It's important to remember there is not a single answer that addresses every cloud versus on-premises question. Evaluating and assessing the viability of cloud security is largely based on the weighted responses to five questions:

1. **What:** What type of data is being considered for cloud deployment?
2. **Why:** Why is security needed? What is at risk?
3. **Where:** Where is the data deployed, and in what type of cloud service model?
4. **Who:** Who is the cloud provider?
5. **How:** How do they provide security?

What

What type of data is being considered for cloud deployment? The suitability of the cloud for your application is heavily influenced by the associated data attributes. For example, extensive security precautions may not be justified for low-sensitivity or publicly available information, such as maintenance schedules or brochures. However, elevated cloud security measures are a necessity in confidential financial reports or regulated data such as credit card information or patient health records. At the extreme, the risk of unauthorized access to confidential trade secrets or national security matters may be so serious the data may not be appropriate to store in any networked computer, anywhere — in the cloud or even on-premises.

> "A key first step is to evaluate what you're trying to protect and how valuable the information is. A cloud provider's security may be suitable for most company data, or you may need to consider controls to limit exposure of data to the provider."
>
> — Ken Deitz, SecureWorks
> Interim Chief Information Security Officer (CISO)

Why

Why is security needed? What's at risk, how is it threatened and what are your security requirements? Do you have special regulatory compliance or data location concerns such as the EU-U.S. Data Privacy Shield ruling? Are there requirements for data replication, physical security or high availability? The answers to these questions help frame critical priorities, selection criteria and performance metrics to evaluate in the cloud discussion.

Where

Where is the data deployed and in what type of cloud service model? Data security in the cloud is based on a shared responsibility model, where the cloud provider and the customer each carry part of the security role. The success or failure of this model largely determines the viability of public cloud security for your application. However, it's important to recognize that boundaries and respective security responsibilities vary by cloud model. In an infrastructure as a service (IaaS) model, the cloud provider is generally responsible for securing the physical environment and network infrastructure. However, their responsibilities typically end at the virtualization hypervisor. As the cloud customer, you are responsible for securing assets and data inside your virtualized environment. In software as a service (SaaS) or similar models, the service provider is responsible for securing all elements of the infrastructure, application and user interface. Because of the increased responsibility and the difficulty monitoring the back-office processes of a cloud services provider (CSP), it's important to assess their ability to meet your

security requirements. Evaluating the specific attributes of a prospective cloud service model and CSP is a critical step in your security evaluation.

> "With infrastructure as a service, the customer generally shoulders the majority of the security responsibility. This can seem daunting due to the loss of direct visibility and control that comes along with the migration to cloud. However, just like with traditional infrastructure, designing in the proper level of monitoring and visibility is critical to staying secure."
>
> — David Langlands, SecureWorks Global Director of Technical Testing

Who and How

Who is the cloud provider and how do they provide security? Although major cloud providers offer extensive security technology and expertise, the same may not be true for a small or under-capitalized vendor. Does your cloud provider understand their security responsibilities, and can they execute? Are you confident in their capabilities and can you get independent validation prior to implementation? It's vital to talk to your cloud provider's security team, assess their capabilities and use third-party verification to evaluate provider security and your required contributions. Selecting a less-capable cloud provider to save computing or storage costs may wind up costing you in the long run in the event of a data breach or negative publicity.

Is the Public Cloud *More* Secure?

Thoughtful evaluation and application of responses to these five questions can facilitate a safe and successful public cloud deployment. The optimal cloud strategy balances the advantages and disadvantages of prospective public cloud options with your security requirements, priorities and on-premises alternatives.

However, one question still remains: Is the public cloud more secure than on-premises environments? In most cases, the answer is a strong "yes!". With appropriate configuration and controls, major cloud providers offer advanced infrastructure, resources and economies of scale that are impractical or impossible for many organizations to replicate. "The public cloud is a very attractive offer for businesses of any size because it allows you to efficiently access world-class IT services, operations and security." said Ken Deitz, SecureWorks interim chief information security officer. "Also, use of the public cloud for your data is not an all-or-nothing proposition. You can have different cloud strategies for different application requirements." Although it's important to select the optimal cloud services provider up front, the primary responsibility for security belongs to the cloud customer and requires a comprehensive security plan that balances cloud security with existing on-premises security in most cases with hybrid environments.

In addition, a properly configured cloud environment can drastically reduce the risk, cost and time required to isolate and eradicate threats. Jonathon Poling, SecureWorks principal consultant for incident response and digital forensics, states, "I would choose a default public cloud deployment with one of the top providers over the average on-premises deployment any day, especially for monitoring and incident response. The resources, capabilities and toolsets offered by some of the top providers can lead to much more effective data collection and analysis, ultimately yielding a substantial reduction in time to respond."

Assuring the security of your cloud vendor, deployment model, and ongoing operations is a critical and challenging process that requires specialized skills and hands-on experience. SecureWorks experts provide the independent validation, expertise and resources you need to safely and successfully transform your organization.

> "Picking the right provider is the foundation for secure cloud operations and response."
>
> — Jonathon Poling, SecureWorks Principal Consultant for Incident Response and Digital Forensics

Conclusion

Cloud computing is forever changing the business landscape, transforming organizations to become more agile, innovative and competitive. SecureWorks understands your requirements to balance speed with security as you adopt new cloud technologies. Take a strategic approach to cloud computing and security; overcome the status quo mindset regarding how you've always done things in house with hands-on control.

The public cloud can be more secure than legacy environments when security is orchestrated up front. Your objectives and risk posture will help you assess cloud alternatives. Insights from SecureWorks experts provide guidelines and recommendations regarding key strategic questions regarding if, when and how the public cloud can be a more secure deployment option.

SecureWorks Cloud Security Solutions

To meet these challenges, SecureWorks offers one of the industry's broadest portfolio of security solutions that are designed to help organizations securely take full advantage of the cloud and hybrid IT. SecureWorks provides end-to-end coverage of all stages of your cloud deployments — from initial evaluation and architecture to ongoing assessments and monitoring. Services include:

Cloud Security Assessment helps you understand strategies such as cloud adoption implications, insights on how to integrate cloud into your existing environment and even how to assess and select a cloud services provider. Our services help organizations make the right choices in their cloud investments, including governance and security strategies.

The first step often involves planning and vendor selection. Picking the right cloud provider at the beginning helps create the right foundation for your secure operations and response. Our cloud provider security assessments include reviews of key staff, documentation and processes relative to applicable security frameworks and best practices.

Cloud Security Design & Architecture assesses your current architecture and its impact on your security posture in the cloud. We work with you to create a cloud architecture that scales as your organization changes and grows over time. With a comprehensive cloud design in place, we help you implement security processes and services that address your unique risk, compliance and operational requirements.

Cloud Penetration Testing leverages proprietary tactics and intelligence from SecureWorks' Counter Threat Unit™ research team to simulate potential threats and test your cloud infrastructure to minimize risks from cyber threats.

Independent validation of cloud provider security and penetration testing of your own cloud environment is essential. SecureWorks delivers a rigorous penetration testing model that not only seeks out vulnerabilities, but also evaluates diverse attack vectors such as social engineering risks, compromised credentials or a bad actor in your organization or the cloud provider.

> "I wholeheartedly believe the public cloud can be more secure than most organizations can provide on their own. When customers want to deploy in the cloud, we help them validate they've done so in a safe way and haven't opened up any unaddressed risks to their data, systems and internal network."
>
> — David Langlands, SecureWorks
> Global Director of Technical Testing

Managed Cloud Services monitor, analyze and distill the thousands of cloud events logged each day into prioritized, actionable security intelligence. This facilitates fast, effective risk mitigation, improved productivity and cost savings for your team. Our managed solutions continuously strengthen defenses and ensure that clients are able to protect and maintain control over their assets and information.

Cloud Incident Response helps organizations rapidly respond to, and minimize the impact of, a security breach. Services include proactive incident management and response, forensic investigation, and incident coordination.

When compared to a conventional on-premises environment, a properly-configured public cloud drastically reduces the time and effort required to identify, isolate and respond to threats. The accelerated response and agility enabled by the public cloud helps reduce the potential damages and costs of a security breach.

Featured SecureWorks Experts

Ken Deitz
Interim Chief Information Security Officer

As Interim Chief Information Security Officer (CISO), Ken is responsible for SecureWorks information security. Ken began his security career in the United States Navy and has nearly 20 years of experience with information security, investigation and response. In addition to the Navy, Ken has also held roles with the National Security Agency (NSA), the U.S. Cyber Command, the Department of Defense (DoD), and public-sector firms.

David Langlands
Global Director of Technical Testing

David Langlands leads SecureWorks Technical Testing business globally, which includes our Red Team Testing, Penetration Testing and Application Security practices. Prior to joining SecureWorks, David led security and infrastructure teams at several Global 500 companies. David has also served as CIO of a publicly-traded manufacturer, and in CSO and CTO roles for several venture-backed organizations.

David holds industry certifications such as the CISM, CISA and CISSP and has over 20 years of experience in information security, global infrastructure management and consulting.

Jonathon Poling
Principal Consultant — Incident Response and Digital Forensics

Jonathon Poling is SecureWorks' resident Cloud Incident Response and Forensics SME with expertise in performing Incident Response and Forensics across all major operating systems (Windows, LINUX and Mac). He serves as the Technical Lead on both US and global engagements across a wide array of industry verticals. Leveraging his experience in government, contractor and private sector roles, he helps clients develop and implement effective strategies to identify and respond to both current and future threats.

Jonathon has a Master of Science in Computer Security and Information Assurance and a Bachelor of Science in Computer Science from The George Washington University.