WHITE PAPER

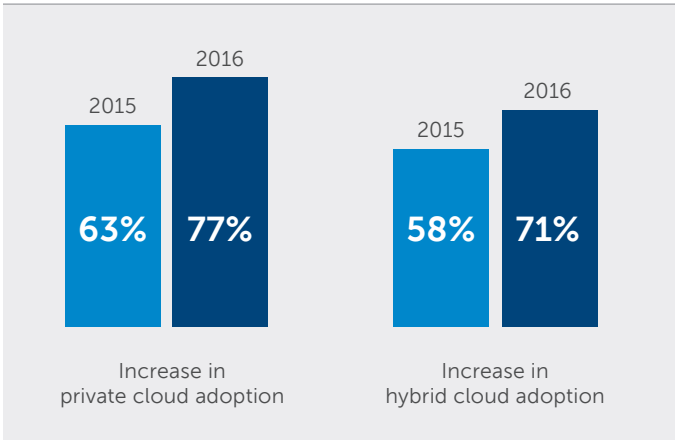
Make Hybrid IT Secure

Gain Visibility, Reduce Risk and Strengthen Governance

Executive Summary

Business agility, globalization, competition and "everything as a service" — these drivers have changed the IT landscape over the past 10 years. Cloud and on-premises technology is now increasingly appealing to organizations, offering advantages in flexibility, speed, cost savings and service delivery.

CIOs are increasingly drawn to public clouds, but there are still significant legacy applications, data centers and mission critical systems that remain on the inside. Thus, distinct approaches to hybrid IT combine co-location, infrastructure as a service (IaaS), software as a service (SaaS) and outsourcing with on-premises and internally managed applications and data centers. According to a recent survey of 1,060 IT professionals, "private cloud adoption increased from 63 percent to 77 percent, driving hybrid cloud adoption up from 58 percent to 71 percent year-over-year."[1] Whether you are only using the cloud for limited applications and workloads, or the cloud is a major component of your IT strategy, your security needs to keep pace with hybrid IT.



[1]Weins, Kim, Right Scale Cloud Management Blog, "Cloud Computing Trends: 2016 State of the Cloud Survey," February 9, 2016, http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey; http://creativecommons.org/licenses/by/4.0/

What You Will Learn

- 12 cloud security threats that put hybrid IT at risk
- 5 considerations for ongoing cloud security governance
- The advantages of unified visibility across on-premises and cloud environments

Who Should Read This White Paper

» CISOs/CSOs
» CIOs
» Directors of Security/IT
» Security Architects

Hybrid IT Doesn't Have to Mean Hybrid Security with Lots of Management Hassles

Hybrid IT will be the de facto practice for most organizations moving forward, leaving you with an IT landscape not entirely virtual, not entirely in the cloud and not entirely within the confines of on-premises network architecture. From a security standpoint, that's a lot of surface to cover. The onslaught of threats makes security monitoring imperative, yet a dearth of security talent means there are fewer qualified people to keep their eyes on your environment. The task of monitoring and managing security logs from point solutions across a hybrid environment is overwhelming. With attacks increasing, security skills scarce and budgets flat, conventional security for hybrid IT simply won't work.

Your organization needs a new approach to secure hybrid IT — one that accounts for business risk across various cloud models like IaaS and SaaS, outlines and enforces policies for acceptable use, and enables strong security control and visibility for hybrid environments.

Regardless of your level of cloud adoption, **take three steps for stronger security for hybrid IT:**

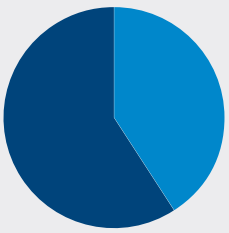
1. **Conduct a strategic risk acceptance process**
   Any amount of externally provisioned cloud services make it vital to define security risk and requirements based on data classification.

2. **Implement strong governance and regular oversight**
   Confidential data in the cloud, concerns about shadow IT and outdated policies all highlight the need to revisit policy.

3. **Seek unified visibility for hybrid IT security**
   Cloud diffusion and poorly defined security policy can result in disparate security management consoles; you need unified security visibility across cloud and on-premises environments.

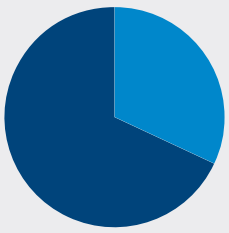
Place Cloud In The Context of Risk

A race to the cloud may have neglected an appropriate assessment of risk. Even if security considerations were carefully reviewed, it's never too late to evaluate the risks to your data with regard to cloud adoption. One of the most important steps is determining when cloud is the right choice — and when it's the wrong one — for valuable data and applications. Even with the cloud's advantages, including self-service, elasticity, scalability and pay-as-you-go pricing, it's not the absolute best option 100 percent of the time.



41%

of midmarket and enterprise organizations use IaaS today.



32%

say it is difficult to coordinate security operations consistently across their public/private clouds.

Source: Jon Oltsik, Enterprise Strategy Group, "The Cloud Computing Cybersecurity Challenge," May 7, 2015

On the other hand, some organizations may be unnecessarily limiting their use of public cloud services based on unwarranted security concerns. Many preconceived notions about the insecurity of public clouds have proven to be false. Cloud providers continue to drive significant resources toward securing their infrastructure — in some cases achieving much stronger security than individual organizations. However, simply moving applications and workloads to the cloud without careful consideration of business requirements, security operations and oversight can lead to exposure.

Don't Let Hybrid IT Disguise Threats

Corporate leadership must fully understand and accept the security risks in the cloud with regard to business processes, advantages and cost savings. More specifically, organizations need to understand the major threats facing cloud environments and how they might affect data and applications hosted in the cloud. The Cloud Security Alliance (CSA) outlined the "Treacherous 12" top threats to cloud computing as a helpful resource to grasp and address risk[2]. The CSA's top 12 cloud security threats include:

- Data breaches
- Lost or stolen credentials
- Hacked interfaces
- Exploitable bugs and system vulnerabilities
- Hijacked user accounts
- Insider threats
- Advanced persistent threats
- Permanent data loss
- Inadequate diligence
- Abuse of cloud services
- Resurgence of DoS attacks
- The dangers of co-tenancy and shared technology

Any choice to use public clouds will cede some control over how your information and processes are stored and protected. It is essential to assess what could happen to vital assets, the impact of an actual breach and the frequency of such attacks. Then, organizations can prioritize and plan for protection and mitigation strategies more appropriately. Proper cloud governance is crucial to this effort, especially for hybrid environments where responsibility for security varies.

Make Governance and Privacy a Priority for Hybrid IT

One key challenge to securing hybrid IT that is not always addressed is governance—the issue of who owns data in the cloud, what policies govern that data, and how policies are enforced. Governance is policy-driven and policy, in turn, is driven by the organization's computing culture and the need to maintain data privacy. Some data is prohibited by law from being used for secondary purposes other than the reason it was originally collected. In addition, some data is restricted from being shared with third parties. Once you enter the world of the cloud, maintaining data governance and privacy becomes much more complicated since your provider hosts your data. The need for up-to-date policies that account for cloud deployments and cloud access is paramount.

Advances in cloud technology further highlight the need for ongoing governance. Consider self-service cloud analytics and data preparation capabilities that would enable an individual within an organization to move data into a cloud ecosystem quickly and easily. Even now, cloud service providers are working on solutions that reduce the complexity of data integration and transformation, making it possible for users with minimal technology background to drop data into cloud warehouses.

> As public clouds, private clouds, and community clouds are adopted, the 'old' IT environment is rarely completely replaced.
>
> — Bob Hayward
> KPMG Managing Director

Source: Eileen Yu, ZDNet, "What hybrid cloud? It's hybrid IT," May 11, 2015, http://www.zdnet.com/article/what-hybrid-cloud-its-hybrid-it/

To make the most of hybrid IT, organizations should review cloud security governance across five key areas:

- **Transparency** — Organizations should ask cloud providers to demonstrate their robust security controls and clear policies for information access, change, replication and deletion. In the case of public cloud platforms, how is information segregated between customers in the cloud?
- **Compliance** — How will cloud providers deliver information for required audits? Are standards of compliance built into existing cloud provider SLAs?

[2] Rashid, Fahmida Y., Infoworld.com, "Introducing the 'Treacherous 12,' the Top Security Threats Organizations Face When Using Cloud Services," March 11, 2016, http://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

- **Data Locality** — When data can be stored anywhere in the cloud, issues related to local jurisdiction can arise. For example, different countries have different rules governing personally identifiable information. How does information stored offshore affect the scope of compliance?
- **Privacy** — What privacy controls are in place for various cloud platforms? Cloud migrations and hybrid IT encompasses an opportunity to implement two-factor authentication and train the workforce on its importance.
- **Certifications and SLAs** — Who is ultimately responsible for security in the cloud? With an IaaS model, cloud providers are responsible for protecting their own infrastructure, whereas cloud clients are responsible for securing their own data and applications. Different cloud platforms and providers offer varying SLAs for security, and maintain different certifications and standards of compliance.

Maximize Visibility Across the Hybrid IT Security Landscape

A hybrid IT environment means more management consoles, and that means more challenges with regard to visibility and integration. This is already a problem for IT and it can quickly produce unmanageable volumes of security data. If an organization wants to take full advantage of hybrid IT, it will need global security visibility across cloud and on-premises environments.

A lack of security talent puts pressure on existing IT resources to manage more devices and perform more analysis. Moving applications and workloads to the cloud can add another dimension to security management. Many practitioners already describe the task of winnowing the real threats from within massive volumes of data to finding a needle in a haystack. Instead of adding more haystacks, organizations need a security management console that can capture data from cloud and on-premises systems to help quickly identify, contain and mitigate threats — regardless of whether or not they originate in the cloud.

Flexibility is just as important for hybrid environments. As organizations assess risk and governance and migrate data and applications to the cloud accordingly, some assets will remain within on-premises environments. You need the ability to see and manage security across all facets of hybrid IT from a single console. Otherwise, calculated decisions designed to increase efficiency and reduce costs, may actually introduce security monitoring and management burdens.

Enjoy the Best of Both Worlds — Safely and Securely

Hybrid IT balances the best of both worlds: the control inherent in on-premises technology with the scalability of public cloud. But Hybrid IT environments are not "one size fits all" when it comes to security. They demand a thorough risk assessment and a tailored approach to governance and protection that help enterprises reap the full rewards of cloud computing. Take steps to assess your risk against the top 12 threats to cloud computing, establish ongoing governance with special consideration for the data most affected by cloud access, and seek a security management console with unified visibility for hybrid IT.

For more information, call **877-838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com