AVERTIUM

WHITE PAPER

The Risky Business of SaaS & Hybrid Cloud.

And what you can do about it

AVERTIUM. SHOW NO WEAKNESS™

Hiring a SaaS or hybrid cloud vendor makes your security operation more complex, not less so. In fact, you inherit their security exposures while adding a new level of control fragmentation to your own environment. This brief examines opportunities, risks and best practices for integrating SaaS and hybrid cloud into your overall security posture.

Not so long ago, IT security was based on perimeter protections surrounding racks of on-premises servers. There was a clear distinction between inside versus outside, and it was theoretically possible to admit only authorized users and connections. Today, the undeniable agility benefits of SaaS and hybrid cloud have broken down the notion of a network perimeter and continue to do so as their roles grow in mainstream IT environments.

End users and machine processes interoperate with largely unseen third-party systems that are typically shared with other—often unknown—organizations and individuals. IT security teams usually have no visibility into the remote hosts, which by the traditional view of IT security amounts to a black box inside the perimeter. Making matters even more complex, many of these services are marketed directly to business units and end users, without IT involvement or knowledge, creating an enormous and constantly growing shadow IT problem.

Manage the Inherent Risk of SaaS and Hybrid Cloud

The extraordinary benefits of adopting cloud models such as SaaS and hybrid cloud produce more liabilities than some companies expect. Through the 2024-2025 timeframe, Gartner sees challenges ahead for companies as they work to mitigate cloud risk:

- 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data
- The majority of enterprises will continue to struggle with appropriately measuring cloud security risks
- 99% of cloud security failures will be the customer's fault

Gartner finds that users are typically to blame for failing to manage the controls used to protect an organization's data, offering the guidance that, "CIOs must change their line of questioning from 'Is the cloud secure?' to 'Am I using the cloud securely?'"

To realize the opportunity of these new business models while also protecting the business, security postures must shift to be more rigorous, more responsive and more relevant. Older approaches that focused on physical systems and infrastructure must adapt to a world where technology is purchased and implemented in many cases as services that do not have dedicated or even identifiable hardware associated with them. Like the business processes that create demand for these capabilities, security must focus on data and services, rather than on infrastructure.

Strategic Benefits of SaaS and Hybrid Cloud

The agility that comes with adopting new software or infrastructure on demand is extraordinary. Unlike older models that required infrastructure to be deployed, SaaS applications operate on provider-owned cloud infrastructure that is configured, optimized, and awaiting customer workloads. IT organizations can select the features and capabilities they need from menus of options that have been established by providers in advance. Customers are often able to implement these offerings simply by subscribing to them and establishing login credentials.

What's more, these SaaS offerings are part of a cloud-native approach to business computing, where workloads can be deployed in containers and interoperate across any environment. Adoption of hybrid cloud is likewise becoming a mainstream approach to computing, with on-premises systems and public cloud services sharing resources and workloads. Large technology providers offer a sophisticated range of solutions that deliver the on-premises portion of these infrastructures as turnkey, managed appliances.

Shifting to this service-oriented model of procuring and implementing software and infrastructure offers a range of benefits to businesses seeking greater operational agility, including the following:

- **Accelerated time to deployment.** Services can be implemented in days or even hours instead of the months that are typical for traditional full-stack deployments. That acceleration corresponds to a faster quote-to-cash transition, ultimately improving the project's impact on the business's balance sheet.
- **Facilitation for virtual and remote work environments.** The cloud-native approach is well suited to the dispersed workgroups that are increasingly the norm for the modern workplace, including operation anywhere, on any device as a first-order usage model.
- **Scalability on demand.** The ability to transparently spin capacity up and down on an as-needed basis is a core value proposition for both SaaS and hybrid cloud. This advantage equates directly to bottom-line savings as businesses pay only for what they use, rather than having to maintain resources for surge capacity.
- **Outsourced infrastructure.** As more infrastructure is abstracted away from the services consumed by an organization, service providers handle a greater share of implementation, patching and maintenance. That shift frees up IT resources for higher-value activities.

While these benefits are compelling to business units and the company as a whole, they also equate to a reduction in IT's control over the environment. The value of those benefits makes it problematic for the security organization to reduce the attack surface by locking down access to external services. Instead, the organization must recalibrate its threat assessment to accommodate new classes of risks.

Business Considerations Redefine the Threat Landscape

SaaS and hybrid cloud have the effect of decentralizing IT, in the sense that they disperse the budgets, buying decisions and technology vendor relationships from IT to the business units. As these technologies are deployed beyond the reach of IT, they also tend to become more removed from centralized cybersecurity planning, including a place in the overall framework for security in depth.

In fact, many business users assume that SaaS and hybrid cloud resources are protected entirely by their providers and therefore inherently secure. The reality is that the customer necessarily inherits some cybersecurity risk and complexity along with the services and other resources from these providers.

Managing that cybersecurity risk is largely beyond the purview of the business units themselves. The IT security function must be engaged to handle requirements such as the following:

- **Compliance with regulations and standards.** Both regulatory frameworks and internal technology standards may dictate how data can be shared and distributed, with concerns as diverse as encryption requirements, retention periods and data sovereignty.
- **Safeguarding accounts from compromise.** End users commonly set up login credentials for subscription-based SaaS and cloud services directly with the provider. This approach bypasses and fails to take advantage of IT investments in identity management and authentication measures.
- **Protecting data wherever it resides.** IT can help establish best practices and guidelines around topics such as encryption and password protection for data sharing and distribution using public resources such as file drop boxes and virtual collaboration services.
- **Vendor and technology assurance.** Enabling the IT security function to vet SaaS and cloud providers and technologies before they are implemented can identify potential cybersecurity exposures in advance, so the risk can be avoided or mitigated.
- **Data breaches and incident handling.** The IT security team needs to understand the provider's breach notification procedures and incorporate them into the incident response plan. Additionally, the IT security team needs to have a clear communications plan with the provider to coordinate incident handling should a breach occur.

A collaborative engagement between IT and the business units is essential to fulfill these functions and to protect against unassessed, unmitigated risk. Early and ongoing involvement by IT enables SaaS and hybrid cloud solutions to be onboarded with appropriate measures to protect the business against cybersecurity missteps.

Risk Mitigation for Hybrid Cloud and SaaS Solutions

A key role for IT in the adoption of SaaS and hybrid cloud solutions is to guide how they fit into the organization's broader security posture. For example, threat modeling should assess the threats and corresponding protection requirements across all the datasets that are exposed to public services.

Appropriate controls can then be applied, including governance of the specific services that are permissible for use, as well as protections for the data itself. The following list provides some guiding examples of controls that can help optimize protections for data, processes and the broader organization:

- **SaaS solution and hybrid cloud whitelisting.** Security organizations should provide governance of which SaaS and hybrid cloud solutions are allowed, and then monitor the environment to enforce those restrictions. For example, SaaS offerings and cloud services can be disallowed by default, and those that are approved can be required to verify adherence to standardized sets of requirements.

- **User training and cultural conditioning.** Forward-looking IT organizations help foster a business culture where business units and end users are aware of the risks inherent to these services, as well as the mitigation measures available. End users should receive training to help them avoid unsafe use of SaaS and hybrid cloud services, including understanding the danger and recognizing the signs of social engineering.
- **Threat monitoring, detection and response.** Actual or potential threat indicators such as unauthorized solutions in use, unusual patterns of data access and possibly compromised security credentials must be continually monitored for and reported on, with automated responses put in place where applicable to block or interrupt non-compliant or dangerous actions.
- **Data-usage assessments.** Sensitivity levels should be applied to data, and the business value of exposures based on that data should be weighed against the associated risk. As a rudimentary example, organizations should consider whether to allow mission-critical, regulated or otherwise sensitive data to be exposed to public repositories or SaaS-based marketing automation platforms.
- **Data-loss prevention.** Detecting leaks where data is being exfiltrated in unauthorized ways is critical, including those cases where a non-malicious insider is responsible. A combination of measures is typically called for to cover data at rest, data in use and data in motion across various services, endpoints and networks. Hard controls can also be placed on how specific users are allowed to transfer data.

The complexity of these controls and other measures can be daunting for a mainstream IT security organization that must divide its resources between routine, proactive and reactive tasks on any given day. To heighten their security postures across their full technology and business environments, an increasing share of businesses have chosen to outsource some or all of the security responsibility, drawing on focused expertise of third-party security services. Avertium is a leading provider of managed security services.

Improve Security Posture with Managed Security

In a world of proliferating threats, increasing complexity and scarce cybersecurity skills, internal teams often struggle to protect the business. Floods of alerts overwhelm mitigation measures, false positives are rampant, and many incidents are not investigated as a matter of necessity. Adequately incorporating modalities such as SaaS and hybrid cloud into the security posture can be a stumbling block.

In response to challenges such as these, many businesses have chosen to optimize and augment the value of their existing cybersecurity investments with managed services from an external provider. That market segment is growing at more than 15% per year, offering a range of capabilities that include the following:

- **24/7 event monitoring and scanning** to hunt for threats, evaluate anomalies and sift through the sea of alerts to return meaningful incident reporting
- **Rapid response and remediation** working with internal security teams, including forensic analysis to better understand and learn from attempted or actual breaches
- **Long-range hardening and protection measures** such as architectural changes, SIEM tuning and improved integration of analytics and intelligence feeds

Avertium provides managed security services that integrate with and extend your own internal security efforts, for greater reach and an enriched security posture. Learn more.

Conclusion

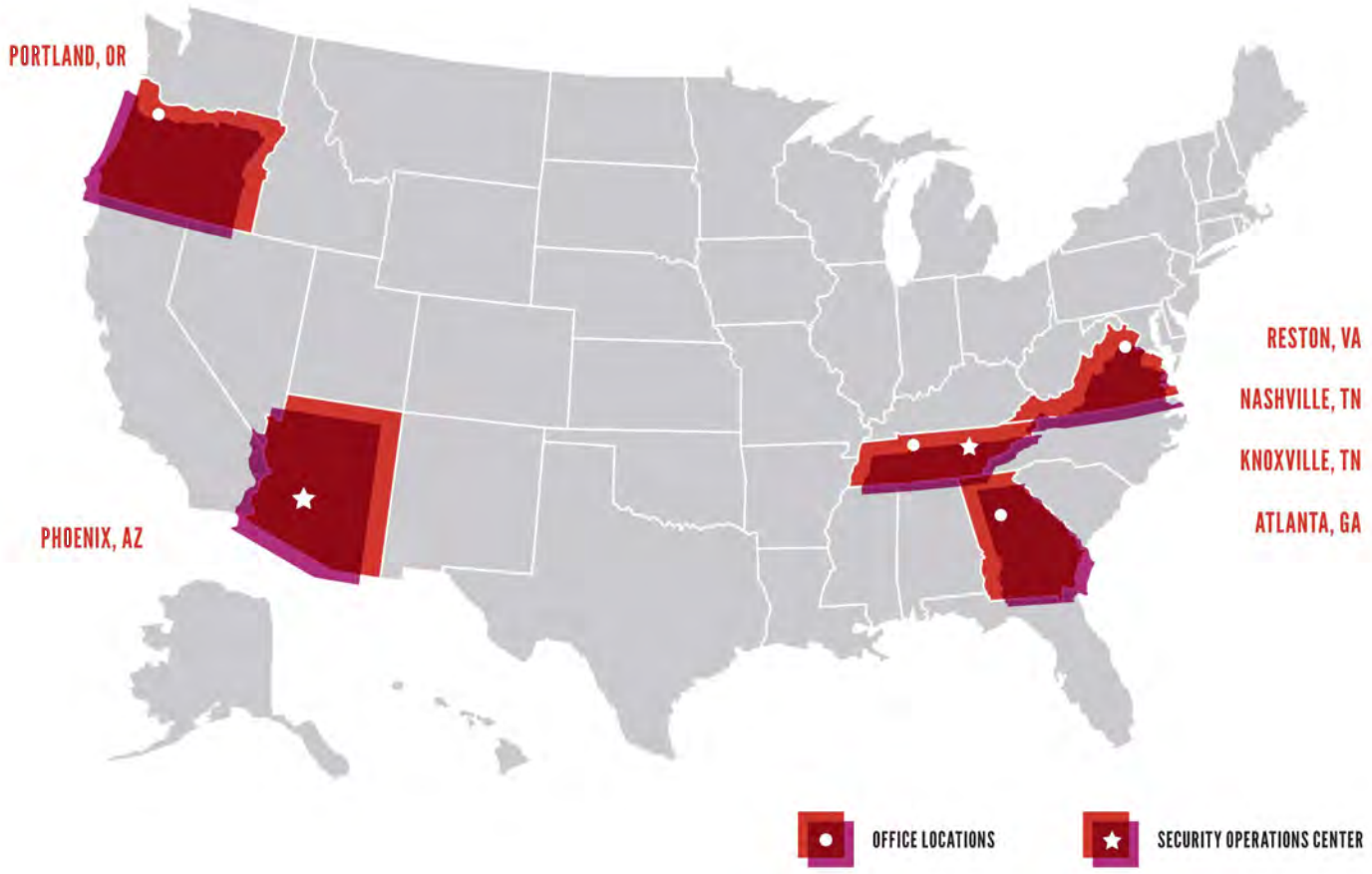
Businesses considering SaaS and hybrid cloud services stand to gain substantial functionality and benefit with minimal implementation complexity or financial commitment. They rightly expect that the associated security measures needed should not burden them as they pursue more intelligent operations with these cloud-native business models, but they may underestimate or misunderstand the role and responsibility of internal IT regarding data security.

To protect the business and ensure a show-no-weakness approach to cybersecurity, SaaS and hybrid cloud need to be brought under internal IT control so they can exist within a coherent security posture for security-in-depth.

Managed security by Avertium is a logical step toward providing this structure as well as the expertise and services to ensure that digital transformation with SaaS and hybrid cloud can coexist with the need to protect the business. Expert help can make this possible while maintaining simplicity and agility, so you can focus on your business.

Take the next step toward a more secure future. Reach out to start the conversation.

NATIONWIDE COVERAGE
LOCAL DELIVERY



ABOUT AVERTIUM

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 1,200 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

+1 (877)-707-7997
hello@avertium.com
www.avertium.com