

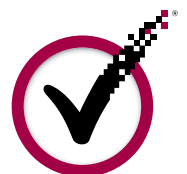
WHITE PAPER

THE TRUSTED FRONT DOOR TO THE CLOUD



CONTENTS

- 1 EXECUTIVE SUMMARY
- 1 ORGANIZATIONS CONSIDER THE CLOUD—BUT CAN THEY TRUST IT?
- 1 TRUST COMES FIRST
- 2 THE TRUSTED FRONT DOOR: WHAT IT LOOKS LIKE
- 3 CONCLUSION: INDUSTRY LEADERS WORK TO CREATE A BLUEPRINT FOR TRUST
- 3 ABOUT VERISIGN





THE TRUSTED FRONT DOOR TO THE CLOUD

EXECUTIVE SUMMARY

Cloud computing offers organizations new options for scalable, cost-effective, and flexible IT, but to gain the full benefits of cloud-based services, enterprises have to trust the security, policies, and processes of those new services. To extend their IT security beyond their own perimeters, enterprises must first establish a trusted front door to the cloud: one that provides security assurance, governance, control, and reliable performance.

ORGANIZATIONS CONSIDER THE CLOUD— BUT CAN THEY TRUST IT?

Organizations are increasingly turning to cloud computing. Analysts put the size of this market at \$42 billion,¹ with the Software-as-a-Service (SaaS) market alone growing to \$16 billion by 2013.² Some organizations are pulled towards cloud computing by the obvious benefits it offers; others are pushed to adopt it because their competitors are already gaining an advantage through it. For many organizations, both these forces are at play.

Virtually every CIO short list of solutions should include a cloud-based option, because cloud computing enables enterprises to improve the quality and flexibility of the IT they rely on to run their businesses. Cloud-based application, platform, and infrastructure offerings can extend the capabilities of data centers, while making more efficient use of resources and decreasing the total cost of ownership of IT functions. The pay-as-you-go model of cloud-based services enables organizations to start small and expand rapidly, without sacrificing quality of service or requiring huge up-front investments in infrastructure.

Cloud computing is the most significant trend in IT now and probably will be for the next few years. Yet the industry is in its infancy: platforms are incomplete and security measures are still evolving. IT managers can't ignore the cloud—but they can't fully trust it, either.

TRUST COMES FIRST

While enterprises acknowledge the potential benefits of cloud computing, they are reluctant to move all critical processing or data into the cloud. The cloud isn't inherently more or less secure than an organization's existing environment, but it's different—particularly in its dependence on third parties.

Organizations are right to demand assurance that service providers will secure their critical assets before they embrace cloud computing. Enterprises should know, though, that security in the cloud isn't as simple as an all-or-nothing choice: they may have to make trade-offs between openness and security, control and availability, flexibility and risk management, and process and enforcement.

Before an organization can rely on SaaS and cloud services for computing power, storage, and mission-critical business applications, it needs to know that its own policies still apply to resources in the cloud, and be able to audit cloud policy enforcement. Trust also requires service-level agreements (SLAs) that guarantee availability, reliability and business continuity. And the organization should insist that cloud providers address the new possibilities for data leakage, including multi-tenancy and access by the cloud operator.

When enterprises move from using just one cloud-based service to using several from different providers, they must manage all these issues across multiple operators, each with different infrastructures, operational policies, and security skills. This complexity of trust requirements drives the need for a trusted front door to the cloud.

1. "The Internet Industry Is on a Cloud—Whatever That May Mean," Wall Street Journal, March 26, 2009.

2. "Gartner says Worldwide SaaS Revenue to Grow 22 Percent in 2009," Gartner Newsroom Press Release, May 7, 2009.





THE TRUSTED FRONT DOOR: WHAT IT LOOKS LIKE

A trusted front door is a security and trust brokering service that can encourage administrators, employees, and business partners to adopt cloud-based applications and processes by offering a single, convenient point of entry to multiple cloud services. It can improve upon the organization's original security, while making security seem simpler than before. To the enterprise, the trusted front door presents one API that complies with open standards. On the cloud side, it supports multiple interfaces to facilitate business partners' integration. Neither side needs to see how the trusted front door shields both the enterprise and its cloud providers from the prohibitive complexity and cost of implementing the strong security practices necessary to secure cloud users, applications, and data.

For most organizations, turning to a recognized and dependable service provider (or "trust provider") for security and trust brokering services is the best way to create that secure front door to the cloud. In choosing trusted front door providers, organizations should evaluate how well they address the key issues of assurance, governance, control, and reliable performance—and establish metrics to help ensure they get what they are paying for in each of these areas.

Security Assurance Opens and Closes the Door

Trust providers should deliver assurance through stringent user authentication and authorization, with additional consideration given to high-privilege or high-risk users and the challenges of remote access use cases. In all cases, providers must demonstrate that they will deny access to unauthorized users according to the enterprise's access policy. Although it will mostly rely on existing processes and resources, a trusted front door can improve security by dynamically inserting additional layers of security such as multi-factor authentication.

Organizations should consider whether a trusted front door provider offers the ability to check trust of user devices such as laptops and smart phones. Threats based on malware have been affecting consumers for several years, and recent corporate attacks have demonstrated that end-point protection does not make enterprise user devices immune to external attacks. A trust provider should protect and monitor user devices to assess whether they should be allowed to access sensitive cloud resources.

Because a trusted front door could impose security best practices on cloud providers, the industry could converge on a cloud security standard similar to the PCI standard for the credit card industry. A provider may then require that SaaS and Platform-as-a-Service providers be certified according to these standards. In the meantime, a trust provider may offer security certification services and vulnerability assessments on its own.

Governance Puts the Enterprise Back in Control

While cloud applications offer benefits over on-premise alternatives, they can also disrupt organizations' models for governing and managing users, applications, and business processes. Organizations should assess any SaaS or cloud-service provider's security governance processes and capabilities for sufficiency, maturity, and consistency with their own information security management practices.

For many enterprises the trusted front door will integrate with corporate directories and meta-repositories to support consistent governance, authentication, and authorization beyond the perimeter. Others may choose a simpler policy enforcement methodology that relies on automated user provisioning and de-provisioning.

To traditional identity and access management platforms, the trusted front door to the cloud resembles an access request switch/router, also acting as a policy enforcement proxy on the outside. As an identity broker and authorization proxy, the trusted front door should avoid credential leakage by leveraging bootstrap credentials and authentication from a trusted source within the organization, such as enterprise domain controllers or external identity provider services such as Google or PayPal. Trust providers will therefore adhere to standards such as SAML, OPENID, OAUTH, and XACML to avoid later lock-in.

Controls Are Key to Compliance

Trust providers must offer not just assurance, governance, and reliable performance, but also full tracking, auditing, and reporting on their effectiveness in providing those services. For every single access event, providers should be able to monitor and report who accessed what, how, when, and from where.





The trusted front door represents a unique opportunity to consolidate access event logs, simplifying audit trails and compliance reports. Auditors can more readily check compliance with laws, regulations, and rules—such as SOX, HIPAA, PCI DSS—across all cloud resources and all users.

Reliable Performance Drives Business Continuity
Organizations must feel confident that their trust provider will deliver access to cloud-based resources in full accordance with SLAs. Organizations also must investigate whether the trust provider complies with industry best practices for connectivity, redundancy, fail-over, disaster recovery, and protection from DDoS attacks.

Cloud provider partners and organizations need to discuss and agree both on SLA reliability standards and on the process of monitoring and reporting against all SLAs. A trusted provider service might offer consolidated SLA monitoring and reporting across all the cloud services an enterprise relies upon. This could increase visibility and reduce the operational complexity of managing multiple independent clouds.

CONCLUSION: INDUSTRY LEADERS WORK TO CREATE A BLUEPRINT FOR TRUST

The challenge of ensuring both tight security and flexibility across multiple users and cloud resources is unprecedented, requiring specialized expertise that most organizations don't have, and don't have time to develop. Instead, service providers of a new kind are rising to meet this challenge of creating a trusted front door, re-integrating best-of-breed applications, data, and users in new ways both to preserve the flexibility of the on-demand model and to enable organizations to extend access policies and security controls into the cloud. By opting to use such a service provider, organizations can buy into best practices for dependable security in a complex IT environment.

The Cloud Security Alliance brings together top service providers including VeriSign and other leading organizations to help establish best practices and common standards for creating trusted front doors to cloud-based assets, and, in the longer term, for opening channels between online resources so that organizations can create their own cloud-based IT ecosystems. Just as the emergence of e-commerce

led to common access protocols (SSL), common policy framework (Web trust), and common compliance standards (PCI), the rise of cloud computing is going to lead to common protocols, frameworks, and standards for securing cloud services. By bringing together innovative service providers and technology leaders, the Cloud Security Alliance is creating a blueprint for trust that can expand and adapt to match the growth and development of cloud computing.

ABOUT VERISIGN

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.VeriSign.com for more information.

