Why You Should Read This Document

This industry brief provides an overview of the benefits and security challenges of cloud-based infrastructures for the financial services industry, with an introduction to Intel technologies that can help strengthen the financial cloud. This brief:

- Discusses how the cloud computing model can lower operational costs for financial institutions and increase the flexibility of computing infrastructures
- Examines legitimate security, regulatory, and compliance concerns that have slowed implementation of the cloud in financial institutions
- Describes how data encryption can help safeguard sensitive personal data as it moves in and out of the cloud
- Explains how hardware-based authentication can validate identity and access in the financial cloud to help ensure that only authorized users can enter
- Examines how service gateways provide API enforcement points at the network edge to reduce the risk of content-borne attacks against financial institutions
- Discusses how virtualized platforms can be made more secure with hardware roots of trust that help assure system integrity and provide a foundation for trusted computing across dynamic environments
Industry Brief

Securing the Cloud for Financial Institutions
3 Securing the Cloud for Financial Institutions

3 Benefits of Cloud Computing for Financial Services Institutions

5 Concerns with Cloud Computing Meeting Regulatory and Compliance Standards for Financial Institutions

6 Protecting the Financial Cloud with Comprehensive Security Approaches

9 Conclusion
Securing the Cloud for Financial Institutions

Cloud computing presents an increasingly popular model for businesses in the financial services industry. Banks, stock brokerages, money management firms, and other financial entities are attracted to the cost savings that cloud infrastructures can provide.

However, the technology infrastructures found in most financial institutions are multi-tiered and highly intricate, making cloud deployments challenging to engineers. The financial services industry also operates in a highly regulated environment and the shared resources model of cloud infrastructures heightens concerns over privacy, security, access and compliance.

Creating pervasive security defenses for these complex cloud environments remains a technical challenge, requiring the right hardware and software tools and a comprehensive security strategy. While cloud computing can help improve the performance of financial institutions, the financial cloud requires a highly secure and auditable computing platform to meet statutory and regulatory requirements that govern the handling of personal and financial information.

This paper describes the benefit of cloud computing environments for financial services organizations and examines the security and compliance considerations that financial entities must meet. It then discusses how cloud security is strengthened with Intel® technologies that make it easier for financial organizations to secure data, authenticate identities and access requests, and ensure trust and compliance across the cloud environment.

Benefits of Cloud Computing for Financial Services Institutions

The financial services industry is undergoing a period of enormous change and reform, facing new regulations that require increased reporting and auditable processes, and a growing need to squeeze cost from business operations.

Cloud computing can help address some of these challenges. The efficiencies and cost-savings made possible by cloud environments directly help lower operational expenses for financial organizations. Clouds can cut energy costs through reduced power consumption, and lower technology infrastructure expense in terms of capital investment in underlying infrastructure—and the human resources needed to manage the technology footprint.

Cloud computing also offers financial institutions greater IT flexibility and scalability. By outsourcing portions of their infrastructure to the cloud, firms have greater agility to adopt new technologies and plan for capacity management, with the ability to expand and contract infrastructure and resources as circumstances demand – a valuable option during times of high market volatility. In addition, the cloud can help improve information management, with centralized data storage for increased productivity and enhanced data sharing and collaboration.

However, not all clouds are created equal. Public cloud infrastructures are hosted computing resources that are shared among the general public, with services delivered from a centralized data center to many on-demand subscribers. Some small to mid-sized firms employ public clouds for utility compute purposes, attracted to the capital cost savings of public cloud for non-mission-critical computing such as administrative functions, enterprise email, and storage.

Private cloud infrastructures refer to hosted compute resources dedicated to a single organization or a designated set of users, usually with security maximized for data protection and compliance. For many firms, private clouds are used to support enterprise-wide
services such as front- and back-office applications, personnel, and other internal line-of-business functionalities.

As cloud security grows increasingly robust, financial institutions are embracing hybrid cloud models that integrate private and public clouds, with the addition of software-as-a-service (SaaS) applications for specialized, industry-specific uses. These include private cloud applications specific to trading, asset management, and market data that are deployed in third-party data centers. An example of this kind of cloud technology is NYSE Technologies’ Capital Markets Community Platform, which delivers a highly flexible, low-latency trading infrastructure and streamlines access to a wide variety of trading applications across a cloud-based platform.

Certain transactional applications specific to financial services firms have largely not made the move to the cloud. Business critical applications such as proprietary trading applications, risk and order management systems, and portfolio accounting services—often considered a firm’s most valuable intellectual property—are considered too critical and complex to place on even a private cloud infrastructure. In addition, applications that provide real-time logic and analytics for such activities as arbitrage trading require extremely low-latency networks to be effective, which the cloud’s shared resource model cannot dependably provide.

While cloud-based infrastructures may never be appropriate for all data processing applications in financial institutions, the potential for operational and capital cost savings represented by the cloud is too significant to ignore for banks, brokerages, and other financial organizations looking to trim expenses. As cloud security technologies mature, these organizations are employing a mix of cloud computing models to meet the security, compliance and performance requirements of varying types of workloads.
Concerns with Cloud Computing Meeting Regulatory and Compliance Standards for Financial Institutions

Financial institutions face strict privacy and data security mandates that compel them to protect their client's personal and financial data. Cloud infrastructures for financial institutions must meet the following regulatory standards, among many others.

**Sarbanes-Oxley Act.** Although the Sarbanes-Oxley Act of 2002 was largely established to provide a regulatory framework for financial reporting and accountability, some of its provisions have had an impact on IT security. In particular, regulations that require internal controls over financial reporting are commonly interpreted as mandating increased data security and access controls.

**Dodd-Frank Wall Street Reform and Consumer Protection Act.** The massive Dodd-Frank Act was signed into law in 2010. The 2,307-page legislation is intended to reform the United States financial regulatory system, increasing oversight and transparency into the activities of financial institutions. Many aspects of the legislation are still being interpreted and written into rules, and the full impact on IT organizations is not yet determined. However, the law requires extensive reporting to improve transparency across financial business units, with increased oversight into data management, risk analytics and data rationalization. Implementing consistent and auditable processes across vast stores of financial data will provide IT and security challenges.

Highly scalable cloud environments can help support some of these legislative goals, as the cloud can help improve information management, with centralized data storage and easier data sharing. However, legitimate security and compliance concerns remain, slowing cloud implementation in a number of financial usage models.

**Cloud Environments Present a Range of Security Challenges**

**Identity and access management.** Existing organizational identification and authentication frameworks may not extend into the cloud, and if these are based on unique username/password combinations for individual applications, they can represent a weak link in the security chain. In the cloud, identity management is key to maintaining security, visibility and control, and centralizing IT control of identities and access is critical.

**Data protection.** Data stored in the cloud typically resides in a multi-tenant environment, sharing virtualized server space with data from other customers of the cloud provider. Financial organizations that move sensitive and regulated data into the cloud must ensure that the data is controlled and secure. One of the inherent risks of multi-tenancy and shared compute resources within cloud infrastructures is the potential failure of isolation mechanisms that serve to separate memory, storage, and routing between tenants.

**Meeting federal regulations and compliance.** Federal laws, rules and standards call for a complex weaving together of security and privacy mandates, making compliance a potentially complicated issue for cloud computing. To comply with these strict data privacy laws, cloud infrastructures must be auditable for such features as encryption, security controls, and geo-location.

**Trust.** In cloud infrastructures, financial organizations relinquish direct control over many aspects of security, shifting an enormous burden of trust onto the cloud provider. The cloud provider's role is critical in performing incident response, including attack analysis, containment, data preservation, remediation and service continuity. For highly regulated financial organizations, deploying data management tools that provide visibility across the cloud to ensure agreed-to policies are being enforced is a requirement.

**Secured architecture.** For cybercriminals, virtualized cloud infrastructures offer an even larger potential attack surface than a traditional data center. Onslaughts using malware and rootkits can infect cloud system components such as hypervisors, BIOS, and operating systems and spread throughout the environment. Protecting a financial cloud from malware requires management of identities and APIs at the network edge to ensure that only authorized users can gain access, and the establishment of roots of trust to assure system integrity.

**Mobile access.** Using mobile devices to extend financial services beyond the office provides obvious benefits to staff and the public alike. However, accessing confidential data on unsecured mobile devices runs the risk of data theft or loss—and of regulatory noncompliance. The increasing numbers of mobile devices and mobile workers in the financial services industry are driving the need for device management solutions and regulated API environments that provide secure transmission of data and solutions across broadband networks, protecting devices from data breach and unauthorized access.
Protecting the Financial Cloud with Comprehensive Security Approaches

Today’s cloud technologies can significantly reduce the security risks previously associated with cloud environments. Intel hardware-enhanced security technologies provide tamper-resistant capabilities to better protect identities, data, and the cloud infrastructure. Solutions that use these capabilities can strengthen identity protection, encourage pervasive encryption to protect data, measure platform integrity, and enforce security policies to better meet compliance requirements and protect privacy.

Protecting data in motion and at rest. Protecting confidential and regulated data is a fundamental responsibility of financial organizations, and the best way to protect data, whether at rest or as it moves in and out of the cloud, is encryption, which makes data unusable if compromised. It also demands secure communication connections, which locks down browser access and encrypts content as it is transferred over the network and throughout the cloud.

However, data encryption based on Advanced Encryption Standard (AES) relies on compute-intensive algorithms that can impact the performance of the computing network, particularly when used pervasively to protect the massive volumes of information that pass to and from the cloud. Traditional encryption solutions can create computing logjams due to high performance overheads, making them less than optimal for protecting cloud data traffic.

Intel has worked to mitigate these performance penalties. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), built into Intel® Xeon® processors, Intel® Core™ vPro ™ processors, and select Intel® Core™ processors, enhances encryption performance by speeding up the execution of encryption algorithms by as much as 10 times. Intel AES-NI delivers faster, more affordable data protection, making pervasive encryption standard in cloud networks where it was not previously feasible.

The browser security protocols Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are used to assure safe communications over networks, including the Internet, and are widely used for secure web browsing (HTTPS), electronic mail, instant messaging, and voice over IP. These protocols are also critical for secure cloud computing, preventing undetected content tampering or “eavesdropping” on content as it’s transferred.

However, traditional SSL and TLS protocols involve two compute-intensive phases—session initiation and bulk-data transfer. Intel has made two contributions to the widely used, open-source protocol, OpenSSL* which greatly improve performance during these phases. One is a library function that accelerates session initiation and a second enables simultaneous execution of data encryption and authentication for bulk data. Any software that incorporates OpenSSL can automatically take advantage of these Intel advancements.

By accelerating data encryption, secure session initiations, and transfer of bulk data, financial organizations can better utilize network resources and implement pervasive data protection to and from the cloud without compromising compute performance.

---

**Financial Services IT Pros: What would increase your confidence in private cloud infrastructures?**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guaranteeing the cloud infrastructure is free of malware</td>
<td>58%</td>
</tr>
<tr>
<td>Creating data “boundaries” to physically restrict workloads</td>
<td>50%</td>
</tr>
<tr>
<td>Ensuring network packages have not been compromised</td>
<td>48%</td>
</tr>
<tr>
<td>Isolating virtual machines to avoid data mixing and contamination</td>
<td>43%</td>
</tr>
</tbody>
</table>

*Extended analysis of data from What’s Holding Back the Cloud: Intel’s survey on increasing IT professionals’ confidence in cloud security
More secure access in the cloud. Realizing cloud-computing advantages while meeting stringent requirements for data security and regulatory compliance requires hardening the underlying platform, including hardware, software and process methodologies. Securing both server and client platforms safeguards cloud infrastructures, and managing identities and access-control points at the network edge ensures that only authorized users can enter the cloud. With malware attacks now moving beyond software to target the platform, organizations face new risks from rootkit and other low-level exploits that can infect system components such as hypervisors and the BIOS to quickly spread throughout the cloud environment.

Protecting identity in the cloud. Protecting a cloud platform begins with managing who has access to it. Intel® Identity Protection Technology (Intel® IPT), found in Intel® Core™ vPro™ processors, builds tamper-resistant, hardware-based authentication that provides a simple way for financial organizations to validate that legitimate employees or authorized users are logging in from a trusted device. Intel IPT offers token generation built into the hardware, eliminating the need for (and cost of) a separate physical token. It also verifies transactions and protects against malware.

Establishing API security at the edge. Application programming interfaces (APIs) are the fundamental method to expose cloud applications to third parties and mobile services. To reduce the risk of content-born attacks on cloud-accessed applications and to protect edge-system infrastructures requires controlled, compliant API governance, particularly at the gateway layer where security policy enforcement and cloud service orchestration and integration take place. Intel® Expressway Service Gateway (Intel® ESG) is a software appliance that provides enforcement points at the network’s edge to authenticate API requests against an organization’s existing identity and access-management systems. Service gateways offer a centralized way for IT and developer teams to collaborate on cloud security policy and enforcement, and deliver standards-based security for consistent API-level controls across the organization.

Ensuring cloud infrastructures are more secure and auditable. Cloud computing, with its dynamic resources and dependence on virtualization, pushes the perimeter of the financial organization far beyond the traditional data center, and with the addition of hypervisors and multi-tenant environments, creates a much larger attack surface for malware and other exploits. The threats against this larger target involve not only malware assaults at the application level, but also attacks against lower-level components in the platform itself.

In addition, reduced visibility into cloud infrastructures also makes it difficult to verify that applications and data are secure and meet statutory and regulatory compliance.

Intel® Trusted Execution Technology (Intel® TXT), found in Intel® Xeon® processors, can help financial organizations reduce the security risks and compliance complications that derive from virtualized computing platforms. Intel TXT establishes a more secure platform based on a hardware root of trust at the level of the chipset and CPU. This root of trust helps assure system integrity, providing a solid foundation upon which to build secure virtual platforms and pools of trusted computing, substantially reducing the security risks of using a virtualized cloud infrastructure by restricting sensitive workloads to these trusted compute pools.

Intel TXT measures platform components such as the BIOS and hypervisor in their “known good” state. These trusted measurements are stored in hardware and compared to boot-time measurements made during subsequent launch sequences. If the measurements do not match, Intel TXT can block the launch of the platform, mitigating boot-level attacks.
Intel TXT Enables the Following Characteristics:

**Verified launch.** Using a hardware root of trust and cryptographic measurements, Intel TXT establishes a safe environment for launching virtual machines (VMs); it also interacts with governance, risk, and compliance tools to report on verified launch status of VMs to improve insight and visibility into the underlying infrastructure.

**Policy-based live migration.** For sensitive workloads, organizations can enforce policies such as the following: VMs shall only be migrated between hosts that have successfully undergone a verified launch.

**Protected execution.** For highly sensitive or protected information, Intel TXT enables applications to run in isolated environments on dedicated resources managed by the underlying platform.

**Protected input.** Through the use of cryptographic keys, Intel TXT protects communication between input devices (such as mice and keyboards) and execution environments to guard against the data being observed or otherwise compromised by unauthorized software processes.

**Data protection.** The risk of insecure or incomplete data deletion in shared cloud resources raises the security risk of data migration from virtual machines and reuse of cloud hardware. Intel TXT scrubs memory during environment shutdown to mitigate memory snooping or reset attacks.

**Auditable compliance.** For financial institutions, meeting regulations and compliance requires significant time, effort, and budget. Legislative mandates often demand security enforcement and can create audit requirements, with the need to understand, document, and report what’s happening in the cloud environment to verify that security policies are set, monitored, and certified. Increasingly, Intel TXT is being utilized by software solutions that manage governance, risk and compliance of virtualized infrastructures based on different security framework requirements.

Trusted compute pools are foundational for building trust across dynamic environments. When grouped together with similar policies, trusted compute pools of virtualized servers can be validated by external entities based on known, trustworthy signatures. Intel TXT can establish and verify adherence to data protection and control standards—enabling hardware-based reporting of platform trust both locally and remotely, enhancing the auditability of the cloud environment.

How Intel TXT protects a virtual server environment:

1. **Provisioning:** Known good values for BIOS and hypervisor provisioned into the TPM
   - If mismatched, policy action enforced, indicates **untrusted** status
   - If matched, policy action enforced, indicates **trusted** status

2. At power on, measured launch of BIOS, results match?
   - 3. Measured launch of hypervisor match?
      - If mismatched, policy action enforced, indicates **untrusted** status
      - If matched, policy action enforced, indicates **trusted** status

   If matched, policy action enforced, indicates **trusted** status

   If mismatched, policy action enforced, indicates **untrusted** status

   If matched, policy action enforced, indicates **trusted** status
Conclusion

Intel technologies help financial services organizations gain the benefits of cloud computing by building a comprehensive foundation for a secure virtual environment. Intel provides the tools to help manage the most important security challenges to the financial cloud—data and infrastructure protection and compliance—with technologies that promote pervasive data encryption, provide more secure data movement, and build higher assurance into compliance efforts.

Intel’s comprehensive set of security technologies and solutions cover end-to-end cloud deployment models, but these are only a part of Intel’s efforts to secure the cloud. Intel is working to develop best practices, standards, design principles, deployment considerations, and governance models to accelerate cloud adoption by financial entities. Intel® Cloud Builders provides proven security reference architectures in conjunction with Intel partners to ease deployment. The Intel® Cloud Finder program can help identify cloud service providers that meet your specific requirements.

Intel is also participating with partners and key industry alliances worldwide to accelerate cloud security standards and interoperable solutions by working with such industry organizations as:

- Open Data Center Alliance (ODCA)
- Cloud Security Alliance (CSA)
- Trusted Computing Group (TCG)

As financial organizations look to more securely integrate their data and business structures in the cloud, Intel continues to drive hardware-enhanced security technologies and software solutions that protect identities, data, and infrastructure in the cloud. These innovations will further increase confidence in the financial cloud by providing increasingly robust methodologies to better manage, monitor, and enforce security policies and enable automated auditing of cloud environments to meet compliance requirements.

For more information on cloud security, visit intel.com/cloudsecurity.

---

1 Intel® AES-NI requires a computer system with an Intel AES-NI–enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Xeon® processors, Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For availability, consult your reseller or system manufacturer. For more information, see http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard-aes-data-protection-aes-general-technology.html.

2 Source: Testing with Oracle Database Enterprise Edition 11.2.0.2 with Transparent Data Encryption (TDE) AES-256 shows as much as a 10x speedup when inserting 1 million rows 30 times into an empty table on the Intel Xeon processor X5680 (3.33 GHz, 36 MB RAM) using Intel IPP routines, compared with the Intel Xeon processor X5560 (2.93 GHz, 36 MB RAM) without Intel IPP.

3 Software and workloads used in performance tests may have been optimized for performance only on Intel® microprocessors. Performance tests, such as SYSmark® and MobileMark®, are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

4 No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd or 3rd gen Intel® Core™ processor, enabled chipset, firmware, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://www.intel.com/content/www/us/en/architecture-and-technology/identity-protection/identity-protection-technology-general.html.

5 No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.1. For more information, visit www.intel.com/go/inteltxt.