WYSE

THE GLOBAL LEADER IN
CLOUD CLIENT COMPUTING

Enabling Financial Services Organizations to Innovate and Prosper Under Tighter Scrutiny

The Role of Virtualization and Cloud Client Computing in Advancing Financial Services

A white paper by Wyse Technology Inc.

Contents

Introduction

1

Introduction and Challenges

The challenges facing financial institutions around the globe are unprecedented. Many banking and investment firms continue to see huge disruptions in their business, from mergers and acquisitions to governmental intervention. Amid today's uncertain regulatory environment, financial services companies face new operational challenges that require the latest technology and market insight to remain competitive while seizing opportunities for growth.

The G20 is spearheading introduction of tougher and more globally co-ordinated regulation of the Financial Services industry. Key areas of focus include identification and management of systemic risks, transparency of trading and incentives, as well as new consumer protections to improve resolution and recovery. In the US and in Europe, major regulatory changes are being planned and implemented in response to the G20 priorities. In the US, the Dodd-Frank legislation provides the enabling framework through which rules for the most far-reaching changes to FS regulation since the 1930's are being implemented. In Europe, new 'super-regulators' for banks, insurers and asset managers are being created from what were previously 'committees' of national regulators.

Financial Service organizations face the challenge of mounting federal regulations as well as unique, varying regulations among the 50 states, and self-governing organization requirements. As a result of this complex regulatory environment, many financial services organizations today continue to address regulatory compliance in a highly reactive mode. Without the right tools in place, executives are often unaware of compliance problems until they are faced with a negative event, such as a data breach, whistle blower allegation or a consent decree. The obvious risks include penalties, fines, litigation and potential negative media coverage.

Financial Industry Regulation

In light of today's economic condition, regulatory agencies are becoming more aggressive as they pursue inspections of financial services institutions, hiring more inspectors and implementing tougher inspection criteria. It is imperative that financial services organizations be able to respond quickly and effectively to prove compliance with all applicable regulations and standards, thus reducing the risk of penalty and potential damage to the brand. Depending upon the type of financial institution, there are eight regulatory agencies in the United States who are responsible for enforcement of regulations. These federal regulators perform systematic assessments of business practices, as well as reviews of audit practices, management oversight, systems development and acquisition, and support and delivery systems for IT.

Federal regulators in the U.S. include the Board of Governors of the Federal Reserve System Bank; Commodity Futures Trading Commission Commodities; Department of the Treasury, Office of the Comptroller of the Currency (OCC), Department of the Treasury, Office of Thrift Supervision (OTS); Federal Deposit Insurance Corporation (FDIC) Banks they insure, not including Federal Reserve System members; and the Federal Trade Commission (FTC). They are responsible for enforcing several key pieces of regulatory legislation enacted to cover the financial services industry, including

The Gramm-Leach-Bliley Act: The Gramm-Leach-Bliley Act (GLBA) was signed into law in 1999, requiring financial institutions to insure the security and confidentiality of customer records and information. Title V is a very significant part of the GLBA because its purpose is to ensure that financial services providers respect the privacy of individual consumers to protect customer information against threats to security, confidentiality, and integrity. Providers must establish customer information security programs to safeguard this information.

Sarbanes Oxley: The Sarbanes-Oxley Act of 2002 was enacted primarily to address corporate governance, financial reporting and internal control issues. It came about due in large part to well publicized accounting scandals at Enron and WorldCom. It applies to all U.S. publicly traded companies, requiring IT departments to provide deep visibility into the companies' finances, controls, operations and processes.

USA Patriot Act: After the tragic set of events on September 11, 2001, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which contains strong measures to prevent, detect and prosecute terrorism and international money laundering. The Act is far-reaching in scope, covering a broad range of financial activities and institutions, and provides the groundwork for new filing and reporting obligations for financial institutions. All financial services companies are covered under this regulation, and those supervised by the federal financial institution regulators or SEC will receive onsite inspections.

Other regulatory requirements: Other recently enacted requirements include the California law, Civil Code 1798.82, in force since July, 2003. This law states that any person or business that deals with personal consumer information must disclose any unauthorized data access to the individuals affected as quickly as possible, and must remedy the cause of the breach. Similar laws have been adopted by 45 other states in the U.S. Responsibilities in this area are also affected by regulatory requirements in other countries. For example, the 1995 European Union (E.U.) Data Protection Directive 95/46/EC prohibits the export of any personal data from the E.U. to countries that do not meet its minimum standards for consumer privacy protection.

Financial organizations that take or process credit card payments are likely subject to the cardholder security programs enforced by the payments vendors such as Visa and MasterCard. Both the Visa Cardholder Information Security Program and the MasterCard Site Data Protection Program require security controls and practices ranging from security management, security assessment, access controls, operations, monitoring and logging, and more. Each program also requires card merchants to undertake or be subject to annual security assessments.

Increased Security Risks

Quantifying security risks and their associated costs can be very difficult. A company often doesn't know that a breach has taken place, particularly in the case of data loss. According to a 2010 McAfee Labs report titled "Security Takes the Offensive", data loss is accelerating at an alarming rate, as there were 222 million records lost in 2009 in the United States alone.[1]

In March 2011, the Ponemon Institute released the findings of a 2010 study which revealed that data breaches grew more costly for the fifth year in a row. The average organizational cost of a data breach increased to $7.2 million and cost companies an average of $214 per compromised record, markedly higher when compared to $204 in 2009. The study also found that for the second straight year, an organization's need to respond rapidly to data breaches drove the associated costs higher. The annual Ponemon report is based on the actual data breach experiences of 51 U.S. companies from 15 different industry sectors.[2] The report included other alarming statistics showing the steady rise of IT security-related events.

- Malicious or criminal attacks are the most expensive and are on the rise. In this year's study, 31 percent of all cases involved a malicious or criminal act, up seven points from 2009, and averaged $318 per record, up 43 percent from 2009.
- Negligence remains the most common threat. The number of breaches caused by negligence edged up one point to 41 percent and averaged $196 per record, up 27 percent from 2009. This steady trend reflects the ongoing challenge of ensuring employee and partner compliance with security policies.

[1] McAfee Labs report, "Security Takes the Offensive", 2010

[2] Ponemon Institute report, "Cost of a Data Breach", 2010

- Companies are more vigilant about preventing system failures. System failure dropped nine points to 27 percent in 2010. This trend indicates organizations may be more conscientious in ensuring their systems can prevent and mitigate breaches through new security technologies and compliance with security policies and regulations.
- Data breach costs have continued to rise. The average organizational cost of a data breach this year increased to $7.2 million, up seven percent from $6.8 million in 2009. Total breach costs have grown every year since 2006. Data breaches in 2010 cost companies an average of $214 per compromised record, up $10 (5 percent) from last year.

Risk Management and Control

At the heart of many of the regulatory and security pressures that financial institutions face is the need to better control and manage risk. Risk comes in many forms, including financial, legal and operational risks. Not only must institutions manage and control risks to avoid fines and sanctions from non-compliance with regulations, but also to avoid increased operational costs caused by having to fix problems that occur. Institutions are now taking a more holistic view of risk management across all of their technology systems.

Data security is a key risk for financial organizations owing to the vast amounts of customer information that is gathered and retained, and the sensitive nature of that information, such as transaction, debt, and personal records. Data is also produced across multiple communications channels, including

- internet and mobile banking channels
- in-person visits to branches and
- transaction records across the breadth of the financial institutions products and services

It becomes clear that security controls must be placed around critical information stores and communication tools to prohibit any information leaks.

Identity and Access Management

Respondents to a security study of financial services organizations by the international accounting and consulting firm, Deloitte, indicated that identity and access management along with data protection were their two top initiatives in 2010. According to the report, organizations state that their biggest threat is “non-intentional loss of sensitive information” due to uncontrolled and excessive access rights. Excessive access rights was the top internal/external audit finding in both 2009 and 2010.[3]

[3] Deloitte 2010 Financial Services Global Security Study

Information security, as demonstrated by the ability to holistically manage the confidentiality, integrity and availability of sensitive customer data, is required for all financial institutions. This is of such importance that governments have established legal and regulatory requirements related to information security and internal controls. Each of these requirements necessitates a comprehensive awareness of system and network activity to ensure that access to sensitive information is appropriate and unauthorized activities are identified and addressed. The result of non-compliance with these regulatory requirements can include serious consequences such as:

- Enforcement actions, including individual prison sentences
- Monetary fines, which could escalate well into six figures
- Loss of company reputation, should non-compliance become public

Cloud Clients for Security and Compliance

Proper data and endpoint security is a necessity in the financial services data environment. Cloud client solutions at end-points formerly occupied by PCs can increase data security, governance, and compliance through a centrally stored data base and managed infrastructure. Cloud clients can be configured to support the latest identity management and access control policies and best practices though the use of two-factor authentication. Cloud clients can also be centrally configured to restrict user access to specific resources, and access rights can be changed without having to service or modify the desktop in any way. By using cloud clients, end points and individual access can be completely locked down as needed by the IT administrator through centralized control of the virtual machines hosted by the servers.

All of the data in a cloud client/virtual server computing environment resides on the servers themselves...not at the cloud client end-points. Data is prevented from leaving the premises on USB memory sticks, CDs, or other portable media, for example, since no data resides on the cloud client desktop device. Storing all data in centralized data centers greatly improves security and can also help ensure compliance with data privacy regulations as required under the Gramm-Leach-Bliley Act and other federal and state regulations. Since all data resides in the data center, automatic information back-up can be deployed more easily across the IT infrastructure, ensuring business continuity and reducing the risk of loss through disaster, while also removing the uncertainty of relying on each user to archive the files stored on their personal device.

More Cloud Client Benefits

Research firm Gartner compared the Total Cost of Ownership (TCO) of personal computers versus what they term server-based computing (SBC). SBC is simply one implementation of cloud client computing. According to their findings, the "TCO of a SBC deployment used to deliver all applications to users is around 50% lower than that of an unmanaged desktop deployment, and 11% to 18% lower than that of a locked and well-managed PC deployment." In addition, the direct costs "of SBC are between 12% and 27% lower than those of traditional PCs."[4] The cloud client approach also delivers other benefits to financial services organizations.

Improved economic efficiencies for IT - Software and storage are hosted and supported on the centralized server infrastructure, so financial institutions don't buy software for each desktop or laptop device that only one person uses, invest in technologies that are quickly outdated, or spend hours and hours on technical support. On average, it costs more than twice as much to provision a PC vs. a cloud client. PCs typically incur significant annual maintenance costs associated with software maintenance and upgrades, hard drive failure, and troubleshooting, while cloud clients are essentially maintenance-free, and can be easily swapped out when necessary. The average lifespan of a cloud client is six to eight years, vs. the three to four year lifespan of a PC, thus extending the buying cycle and reducing costs over time. In addition, cloud clients provide a greener solution from an energy perspective, consuming 10% or less of the wattage (under 7 watts versus 100 or more) required to operate a PC.

Greater reliability – Cloud clients do not have moving parts such as disk drives and fans, and require no native OS to be loaded on the machine, since they are completely dependent upon the centralized servers. With no PC OS to corrupt, cloud clients, and more secure 'zero clients', reduce or eliminate virus or vulnerability issues. Unlike a PC, it is impossible for unauthorized users to "customize" the cloud client with outside software which could potentially disrupt the workstation and the network.

Simplified desktop environment and ease of use – Since information and computing resources are resident on centralized servers, cloud clients are not cluttered with multiple applications, and can be re-purposed to meet changes in operating systems and the application environment. A single cloud client can efficiently display any application and OS supported by the virtual server cluster.

Rapid deployment to meet business changes – The lower per-unit costs of cloud clients vs. PCs means that more cloud clients can be deployed rapidly, when and where needed, to address new service initiatives or manage expansions and mergers.

[4] Total Cost of Ownership Comparison of PCs With Server-Based Computing, August 2008, by Federica Troni, Mark A. Margevicius, Michael A. Silver.

Cloud Clients in Financial Services

Commerzbank North America (NY) recently embarked on a virtualization project that included moving to a cloud client virtual desktop model for all employees. Commerzbank North America is a subsidiary of Commerzbank AG, the second-largest German bank, founded in 1870 and headquartered in Frankfurt-am-Rhein. Commerzbank's North American headquarters in New York was established in 1971, and provides wholesale banking services for corporate and institutional customers and banks. A key challenge was data security; while cloud clients solved many data security issues by providing access to corporate data stored centrally in the data center, traditional security methods based on building access could still be circumvented. Commerzbank decided to adopt a virtual desktop infrastructure, and engaged Wyse and partners Leostream and IdentiPHI to create a smart card-based authentication system for virtual desktops to provide straightforward log in and "anywhere" access for end users, while maintaining strict adherence to industry security standards.

Commerzbank's decision to move toward a virtualized desktop infrastructure model for end user computing promised many of the benefits of centralization of computing resources: improved data security, more efficient administration of desktop computing resources and management of end users, and the flexibility to integrate a wide range of data center resources. But it was essential for Commerzbank to ensure that the virtual desktop model would also comply with the strict security standards of the banking industry. Most conventional desktops are protected only by a password, but office security also enhances this single-factor desktop security through access control systems, locked office doors, and/or security guards. All of which require a second factor – a key, an ID, or a swipecard – for the user to get to their desktop. The virtual desktop model allows users to access their desktops from any physical location within the firewall, effectively removing the second security factor provided by controlled access to a physical location.

The challenge for Commerzbank was to develop a virtualized desktop infrastructure that emulated the authentication provided by the combination of physical, location-based access and password-protected sign on to the desktop. This solution would need to give end users seamless and trouble-free log-in while providing the benefits of "anywhere" access to the desktop. In addition, the solution would need to adhere to industry security standards by emulating strong, two-factor authentication.

Wyse and its partners at Commerzbank implemented a virtualized desktop solution that met their security requirements and was equivalent to their old system of securing desktops through the combination of building access and desktop log on. This enables users to access applications and data via Wyse virtual desktops from any cloud client located behind the firewall while avoiding the cost, complexity, and limitations of using building security to secure computing resources.

Hiscox Insurance

International insurance group Hiscox has grown from being a single underwriter at Lloyd's of London to become a £1 billion turnover business listed on the London Stock Exchange. The insurer specializes in protecting people and businesses with unusual and often complicated insurance needs. The success of the business lies in how Hiscox has focused on specialist areas of expertise and strength. Their strategic decision to choose Wyse cloud client computing helps make their business responsive to customer requirements. Three years ago a decision was taken to review the information technology infrastructure. One of the top criteria was for systems that gave advisers and brokers the right information and tools wherever they worked in a rapidly growing network of offices in the UK, Europe and North America.

Hiscox decided to adopt an information infrastructure based on cloud clients with applications delivered from a central data center. Cloud clients could be configured with no data storage, thus enabling all customer data to be stored centrally and securely. Today, Hiscox uses Wyse cloud client computing and virtual desktops throughout its business. There are over 650 cloud clients deployed across each of 30 Hiscox locations worldwide.

The configuration of each cloud client is pared right down to the Wyse operating system for security purposes. No data can be stored on the cloud client desktop, eliminating any possibility of data being lost or stolen. The data centre is highly secure with a full array of security features, backup systems, and disaster recovery facilities. Using virtual desktop software, the virtual server infrastructure presents a desktop image to each cloud client with potential access to around 230 applications including specialist brokerage and claims management software.

Hiscox has made the Wyse V10L cloud client the mainstay of its virtual desktop infrastructure. The Wyse V10L can be optimized for the VDI environments that Hiscox operates. Its Wyse firmware and high speed network interfaces deliver the responsiveness that end users expect. It also supports the running of multiple applications and dual screens - the latter being an important factor for end users working with specialist financial applications.

Managing the clients is also a lot easier for the Hiscox IT team. The Wyse Device Manager allows the team to detect any under-performing or malfunctioning units early. The ability to swap out units without any time-consuming re-configuration reduces the maintenance overhead considerably. The ease of deployment is critical for Hiscox's ability to be responsive to industry change and growth. The installed base of Wyse cloud clients is extremely "green" – highly energy efficient and automatically shuts down when not in use. Hiscox is enjoying the benefits of cloud computing on a large international scale. Total cost of ownership has been optimized, and the secure but flexible infrastructure is supporting the business at every level and in all of its regional and international markets.

Summary

2

These examples illustrate the value of deploying cloud clients and a Virtualized Desktop Infrastructure in demanding financial services environments. Not only does the cloud client computing platform from Wyse Technology deliver better VDI with clear and compelling operational benefits to financial services organizations, it also enables efficient, confident adoption of the complex regulatory mandates and security requirements that financial services organizations are being required to implement around the world. Wyse Technology continues to deliver ground-breaking software and hardware solutions in virtual computing environments which enhance data security, support regulatory compliance requirements, reduce IT overhead, and ensure greater operational reliability to meet the demanding requirements of the financial services industry around the globe.

Wyse Technology is the global leader in Virtual Desktop Infrastructure and Cloud Client Computing. The Wyse portfolio includes industry-leading thin, zero and cloud PC client solutions with advanced management, desktop virtualization and cloud software supporting desktops, laptops and next generation mobile devices. Cloud client computing replaces the outdated computing model of the unsecure, unreliable, energy-intensive and expensive PC, all while delivering lower TCO and a superior user experience. Wyse has shipped more than 20 million units and has over 200 million people interacting with their products each day, enabling the leading private, public, hybrid and government cloud implementations worldwide. Wyse partners with industry-leading IT vendors, including Citrix®, IBM®, Microsoft®, and VMware® as well as globally-recognized distribution and service partners. Wyse is headquartered in San Jose, California, U.S.A., with offices worldwide.

WYSE

THE GLOBAL LEADER IN
CLOUD CLIENT COMPUTING

wyse.com

A white paper by Wyse Technology Inc.