

StoneGate in Finance Industry



Main Drivers for IT and Security Infrastructure in Finance

With both volumes and volatility growing, financial markets firms are adopting strategies to increase profitability and market share. For one, leading institutions are increasing the sophistication of their electronic trading systems. Also, they see the need to create infrastructures that shift costs from a fixed to a variable model to enable them to be responsive to fluctuating business demand.

The need to better monitor and control exposure, coupled with constraints arising from regulatory requirements, such as the Basel II Capital Accords, the Sarbanes-Oxley Act, and Section 501 of the Gramm-Leach-Bliley Act, have forced financial markets firms to review risk management and compliance policies, processes, and systems.

As banks turn more and more to technology to further their business, new risks brought about by technology are encountered and must be addressed. Primary is the risk of unauthorized intrusion into the financial institution's network, where information can be compromised and systems damaged or altered. Organizations take great effort to prevent such intrusions from occurring, developing protection and detection mechanisms to thwart break-ins.

Typical Challenges in the Industry

Financial markets firms seek to go for offshore operations and extend their global footprint in order to compensate diminishing margins. They move processes online (e.g., online advice, real-time inventory) and therefore try to increase efficiency and minimize fixed costs.

Regulatory uncertainty is threatening to drive up

Create a world of
confidence.



compliance costs and distract firms from focusing on revenue generation. In the U.S., pending regulation NMS and soft dollars are creating a need for increased automation and transparency, while Basel II and European integration are driving enterprise-wide infrastructure transformations in Europe.

Several financial standards impose security requirements on financial institutions

On January 17, 2001, the banking regulatory agencies adopted guidelines implementing Section 501 of the Gramm-Leach-Bliley Act (GLBA). The guidelines require financial institutions to establish a comprehensive and coordinated information security program, appropriate to the size of the bank and the complexity of its operations.

These guidelines require financial institutions to establish an information security program to:

- identify and assess the risks that may threaten customer information
- develop a written plan containing policies and procedures to manage and control these risks
- implement and test the plan
- adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security

NASD Rule 3510, 3520 and NYSE Rule 446 require members to create business continuity plans that are reasonably designed to enable members to meet their existing

obligations to their customers in the event of a significant business disruption. These obligations include granting customers access to their funds and securities during such an event. NASD and NYSE members also must address their existing relationships with other broker/dealers and counter-parties.

The Sarbanes-Oxley Act requires that appropriate internal controls be in place to contain and detect fraud (section 404). And it requires a company CFO and CEO to sign off on those controls as part of the periodic reporting process (Section 302).

In October 2001, the Basel Committee on Banking Supervision (BCBS) issued Customer due diligence for banks, subsequently reinforced by a General Guide to account for opening and customer identification (CDD) in February 2003. The CDD paper outlines four essential elements necessary for a sound know your customer (KYC) programme. These elements are:

- customer acceptance policy
- customer identification
- on-going monitoring of higher risk accounts
- risk management.

Similar to the approach to consolidated credit, market and operational risk, effective control of consolidated KYC risk requires banks to coordinate their risk management activities on a groupwide basis across the head office and all branches and subsidiaries.

Conduct business in
confidence.



Stonesoft solutions for Finance Industry

Reduces risk for business disruption

According to Infonetics Research study¹⁾ financial vertical firms faced on the average 1180 hours downtime during 2004. The number is a bit smaller if financial respondents were not involved in e-commerce. Downtime caused \$165 million in productivity loss and \$56 million revenue loss annually. Stonesoft products can remove 35% of those downtime costs. These downtime costs that are related to security products, network products and Internet service providers.

Financial institutions are typically highly distributed branch networks. Employees at financial companies are highly dependent on their network; not only does every second of downtime cost money in lost transactions, but most employees are rendered completely unproductive during downtime.

Stonesoft products have been designed for production critical environments where downtime is not allowed. Clustering of devices, multiple simultaneous Internet service providers and patented Multi-Link Virtual Private Network (VPN) connections have been proven to work in this demanding environment. For example, software upgrades can be done without any business disruption. In the event of the total destruction of a site the other operating sites can automatically recover lost communication links using Multi-Link features.

Reduces the total cost of ownership (TCO) for financial firm's multisite environment

Financial firms typically have a lot of branch networks and they have to be able to enforce security policy and manage security infrastructure cost effectively. StoneGate products provide centralized management of all components. If branch office equipment loses connection with central management due to administrator configuration mistake then branch office equipment will automatically revert to a previous known good version and clear the connectivity problem.

New remote office security equipment deployments can be done without specialized IT staff on the site. Software upgrades can be done remotely and they will rollback to a previous version if something went wrong during the upgrade process. Calculating three years running cost for multi-site environment will show significant reduction in total cost of ownership.

Efficient audit handling for regulatory compliance

An audit trail is a basic requirement for regulatory compliance. Stonesoft's StoneGate products provide clear audit trails for administrative actions. Internal and external auditors can receive clear and precise reports. These reports save a lot of evaluation time and can be used as part of a compliance report. Reports are based on StoneGate logs where auditors can find more detailed information about the specific event in case they want to take a closer look at details.

Stonesoft Case Studies for Finance Vertical

■ *First European Transfer Agency (FETA): Transferring Security Confidence Ahorro Corporacion: Banking on Reliable Security*

■ *StoneGate and Finance vertical*

¹⁾ The Cost of Enterprise Downtime: North American Vertical Markets 2005, January 2005

STONESOFT EXPERIENCE

Finance professionals rely on Stonesoft's StoneGate platform to provide integrated network security and business continuity through advanced firewall, VPN and IPS solutions. Stonesoft's unified platform is designed to provide the most secure, available, manageable and scalable solutions for players of all sizes in the government profession.

Stonesoft Corporation (HEX: SFT1V) is an innovative provider of integrated network security and business continuity. Stonesoft is a global company focused on enterprise level customers requiring advanced network security and always-on business connectivity with low TCO, best price-to-performance ratio, and highest ROI. StoneGate™ Security Platform unifies firewall, VPN and IPS, blending network security, end-to-end availability and award-winning load balancing into a unified and centrally managed system for distributed enterprises.

Founded in 1990, Stonesoft Corporation has corporate headquarters in Helsinki, Finland; Americas headquarters in Atlanta, Georgia; and Asia Pacific headquarters in Singapore. For more information, go to www.stonesoft.com.



THE STONEGATE PLATFORM

As the first highly available, load balancing network security solution of its kind, StoneGate sets a new standard for FW, VPN and IPS solutions. StoneGate provides a unified security platform with active-active clustering, load balancing and bandwidth aggregation for multiple Internet links and ability to transparently fail-over VPNs, all with the security and connectivity of an integrated FW/VPN.

- **Multi-Link Technology™** – Seamless fail-over between multiple ISPs and FW clusters for always-on connections
- **Increased Performance** – Analyzes and utilizes fastest possible connection through integrated intelligent load balancing between ISPs and FWs.
- **Multi-Layer Inspection™** – Combines the best aspects of application proxy firewalls with traditional packet filtering and stateful inspection technologies
- **Reduce Costs** – Eliminate network complexities and costs associated with multiple vendor solutions and travel time
- **Unified, Central Management** – Robust remote management, along with simple remote update, alert center management, reporting, diagram editor and hierarchy policy updates. Also integrates FW and VPN with StoneGate's IDS Plus solution into a unified platform.

StoneGate is available either as a software-based solution that capitalizes on existing hardware investments, or as Stonesoft's own integrated appliance eliminating complexity and costs associated with multiple-vendor solutions. All of Stonesoft's appliances include the standard enterprise level features with the only difference being the number of physical interfaces and performance level.

STONESOFT
www.stonesoft.com

Stonesoft Corporation (HEX: SFT1V)
is an innovative provider of integrated
network security and business continuity.

Corporate headquarters
Stonesoft Corp.
Itälahdenkatu 22 A
FIN-00210 Helsinki
Finland
tel. +358-9-476 711
fax. +358-9-4767 1234

Americas regional headquarters
Stonesoft Inc.
1050 Crown Pointe Parkway,
Suite 900
Atlanta, GA 30338, USA
tel. (770) 668-1125
fax. (770) 668-1131

Asia Pacific regional headquarters
Stonesoft Corp.
90 Cecil Street
#13-01 Carlton Building
Singapore 069531
tel. +65 6325 1390
fax. +65 6325 1399