

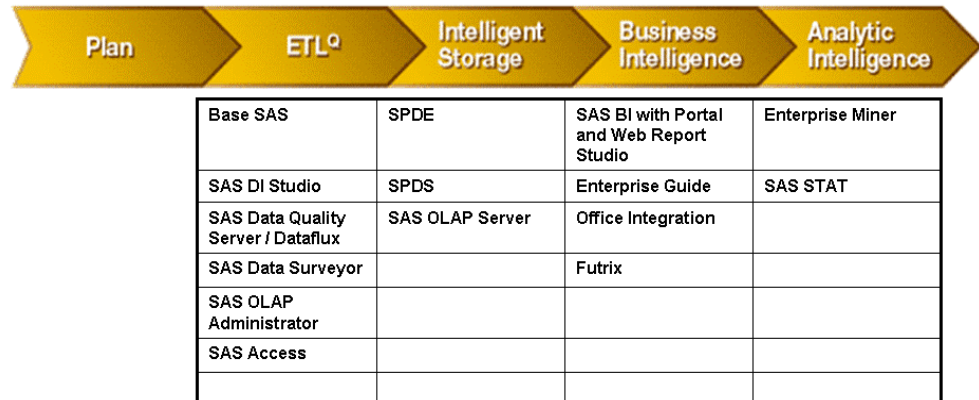
Enterprise Security Model in SAS Environment

WHITE PAPER

Enterprise Security Model in SAS Environment

Emerging internet threats coupled with strict compliance requirements of banks, financial institutions, medical service providers, insurance companies, and retailers is making mandatory to incorporate and integrate strategic security technologies in the IT landscape. This document presents a 360 degree view towards the four-tiered security model to address operational and compliance needs in the mission critical SAS environment. Gone are those days where SAS would run in an isolated workstation or server environment for statistical analysis. SAS has broadened the product offering to encompass the enterprise with array of products running in n-tier architecture. Below snapshot of some of the key solutions in SAS value chain (Please note Futrix is not a SAS technology but has tight integration with business intelligence platform suite).

Strategic Framework for Delivering Enterprise Intelligence



Security Model

This paper focuses on an integrated four pronged framework for protection of mission critical systems hosting credit sensitive data with security enveloped from the physical, network, server (OS), and database level.

Physical Security.

At Intellidyn safeguarding the client and bureau data is of utmost importance. Keeping the operational efficiency with stringent compliance guidelines of bureau and customers we have selected tier 1 co-location data center facility of AT&T in New Jersey. This highly secured environment will host mission critical

Intellidyn systems running 24*7 enterprise applications for array of modules in the above SAS Value chain.

Adequate perimeter controls are in place to control access to the data center by use of security personnel, access card, biometric scans, and video cameras.

The access to the data center facility at AT&T is strictly enforced. The access to the facility is only for selected IT staff and selected senior management. The facility has a security personnel stationed inside a locked environment to monitor and control access to the data center after verification of credentials (updated access list for each customer). This control is enabled for 24*7*365 days.

Logs are maintained for customer and visitor access and are required to wear visitor badge during their stay in the data center. Ticketing system tracks the visitor/maintenance engineer access and escorted to the client cage during the maintenance window. Ticket needs to be opened for access with complete information of the maintenance engineer/visitor, time, date, and duration of access.

The data center has been designed according to the best practices guidelines with raised floor, isolated client cages with locking cabinets, air conditioning, and fire suppression system. Conventional smoke and heat sensors are cross-zoned throughout the center on the ceiling and below the raised flooring. Fire extinguishers are located on the center floor for human intervention. Pre-Action Dry-Pipe Fire Suppression System is installed in the data center. Adequate controls to monitor temperature and humidity in the data center

The customer cages have redundant power grids to meet the high availability needs. The first tier of protection in case of outage is UPS. The second tier of protection is Generator for back-up power with capacity of 52 hours of fuel onsite. Both UPS and Generator sets are configured in N+2 configuration for redundancy.

All activities in the data center are monitored using CCTV and is recorded in two locations (NJ and San Diego). The tapes are kept for a period of 90 days. All exterior doors, entrance points, and loading dock, and delivery docks are

monitored and recorded. All interior activity associated with rack cages/client cages, environmental components, and personnel locations are monitored and recorded.

Network Security.

The Internet is the world's largest network *of networks*. A network is a physical and logical collection of computing resources (Servers, workstations, and network devices) managed by an administrator. While the Internet has transformed and greatly improved the way we do business, this vast network and its associated technologies have opened the door to an increasing number of security threats from which corporations must take proactive measures to protect.

The primary means for most companies for securing their private networks against unauthorized public access is to configure security devices on the perimeter to control and monitor the internet traffic configured according to the policies. *Stateful* packet filtering firewall (Cisco PIX and Fortinet) is used as an access control device, performing perimeter security by determining which packets are allowed or denied into the network. It monitors all traffic entering and leaving the private network and alerts IT staff to any attempts to circumvent security or patterns of inappropriate use based on certain criteria like high-volume packet inspection, internal address masking and hazardous content detection. In nutshell well configured *stateful* packet filtering firewall can provide effective defense against unauthorized access by external users addressing issues like IP spoofing (forged packets) where one hosts claim to have a trusted IP address of the impersonating host, port-scanning, and IP session hijacking where an attacker takes over the user's session.

NAT (network address translation) is often a service that is provided by firewall. NAT is a means to support multiple internal "IP" devices with a single advertised IP address. The nature of NAT allows network administrators to obscure the visibility of clients on a given LAN.

With proliferation of array of network devices the immediate threat is to control access to these devices according to the policies and changing default password and modifying them to meet your password policies to prevent unauthorized access to your network devices. Users are given privileges

according to their job description and duties and activities are monitored and logs updated. Integrated web-filtering, intrusion detection, and tiered anti-virus solution is deployed at strategic gateway devices to insure data integrity and security is not compromised.

VPN is employed to provide the ability for two offices, mobile workers or remote users to communicate with each other in such a way that it looks like they're directly connected over a private leased line. The session between them, although routed over the public Internet, is private (because the link is encrypted), and the link is convenient, because each can see each others' internal resources without showing them off to the entire world. Microsoft PPTP, SSL VPN, and IPSEC technologies are employed to address the remote connectivity by mobile workers and securing two end points.

CERT and CSRC mailings are also subscribed to be abreast of newer threats and solutions.

Server Security.

Keeping in tune with our strategy of setting up a defense in depth security scheme for the servers forming the cluster farm servers for hosting mission critical business applications with high uptime it is imperative to install and configure these servers with foresight and encapsulating the necessary security layers. These secure servers are isolated on network with controlled connectivity and access based on Physical and Network security practices defined above.

Selection of Operating environment is made keeping into the consideration of hardware and software compatibility requirements. The OS which forms the core of this high compute environment is installed and configured to meet the requirements and best industry practices. Upon installation all the necessary security patches and application fixes are updated and unnecessary services are disabled. The console access is restricted and console servers are employed. Open source technology like OpenSSH is employed which encrypts all traffic to eliminate eavesdropping, session hijacking, and other network level attacks. Secure shell (ssh, sftp, and scp) are replacement to vulnerable services like telnet, ftp, rlogin, rsh which are disabled because of inherent limitation as password and data is transmitted across the wire un-encrypted.

Another technology which is highly recommended to encrypt data before transporting using electronic or media is PGP (Pretty Good Privacy). PGP supports message authentication and integrity checking. The latter is used to detect whether a message has been altered since it was completed (the *message integrity* property), and the former to determine whether it was actually sent by the person/entity claimed to be the sender.

TCP wrapper technology further provides firewall like capabilities for host to allow or disallow connections from different network devices. Root login to servers directly is not permitted on any Intellidyn servers, and the dangerous `r` commands are disallowed. The guest and unneeded accounts are either disabled or removed. Passwords are configured with creative use of alphanumeric characters and steps are made to insure users meet the guideline set in password policy. Logging is configured to send system messages to a centralized logging server, and events are monitored for kernel, system, and user errors.

Some of the key features for this highly secured and available computing architecture are that mission critical devices are configured in a cluster and there is no single point of failure. These servers are not visible to the world and access is provided to a few selected Intellidyn users and access privileges are granted based on their job description. Enterprise backup and recovery system is configured and master/media servers are defined with adequate security features like user logins and encryption. Combination of disk based and tape library based backup are employed to meet the faster recovery and compliance features.

Database Security.

The access of mission-critical systems and databases to Intellidyn employees over the public internet present new challenges to traditional notion of enterprise security. Data access must now be controlled at a very fine level of granularity, often to the level of individual customers or users. The SAS SPDS (Scalable Performance Data Server) addresses these requirements by providing highly granular, server-enforced access control and flexible privilege models. Users can be strongly authenticated, even remotely, and data is protected in transit by network encryption.

Each master input tables and customer specific data warehouse, data and information marts reside in separate domain which is a logical container for holding tables created for different campaigns and projects. The shelf life of the data is determined by the contractual agreement between customer and CSI at Intellidyn. Each domain has access control to provide access to users based on groups configured by the administrator. The granular level controls are further configured to provide access to user based on their credentials to the columns within the tables (Both row and column level security is enforced). This ensures that database users are only authorized to perform those specific operations required by their job functions.

The database users are configured with permissions to access separately from the users profile created at the Operating system level as defined above in the Server security section. Passwords are configured within the SPDS environment by use of alpha-numeric characters and steps are made to insure users meet the guideline set in password policy. Basically, this is server within a server with its own users, permissions, access control, and logs to track user access.

There is no one solution which fits all the organizations as each site has its compliance and data security needs with its customers and data-vendors. Technology eco-environment is fast changing and the above model allows the flexibility to enhance/upgrade components within each tier independently without impacting the whole grid after adequate tests have been carried out in the staging environment.

175 Derby Street | Hingham, MA 02043 | Ph.866.773.5756 | Fax.781.749.5545