

white paper

Ensuring the **safety** of customer data



The Host Analytics Approach to Security, Privacy, and Availability

Host Analytics is the leading provider of on-demand corporate performance management (CPM). Its solutions help financial departments and executives improve their budgeting, forecasting, financial consolidations, dashboarding, scorecarding, and reporting and analysis.

Host Analytics is highly focused on the safety, privacy, and availability of its customers' data. While security is important to any SaaS provider, it is particularly critical to Host Analytics as customers are entrusting it with their financial data. In particular, companies must be satisfied that the solution meets the following criteria:

Security. Is data being kept safe from malicious users or intent?

Privacy. Is the customer the only entity that can access its data?

Availability. Does Host Analytics have the appropriate architecture to assure application uptime?

This white paper describes the processes and technologies that Host Analytics has put in place to safeguard its customers' data. Procedures are based on ISO standards and span all aspects of Host Analytics business practices, including security policies, organizational structure and human resources, physical environment and asset management, communications and operations management, information systems management, and security incident management.

The Host Analytics application is architected based on the .NET framework with redundancy in all critical components to provide high levels of uptime. Business continuity and disaster recovery plans ensure continued operations in the face of natural disaster or major incident. Host Analytics performs regular SAS 70 Type II and other security audits, providing the foundation for customers to maintain compliance with critical regulatory requirements.

This attention to security and privacy has paid off for Host Analytics' customers. In over ten years since Host Analytics first began offering SaaS services, Host Analytics has enjoyed an exemplary security record without a single major security breach. The focus on uptime has also yielded customer benefits, with current application availability levels of 99.99%, significantly higher than its SLA target of 99.5%.

Host Analytics Security and Safety Controls

The approach Host Analytics employs to ensure the safety of its customer data can be subdivided into ten areas: security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition and maintenance, information security incident management, and business continuity management. These areas are depicted in Figure 1 and each is described in further detail below.

Figure 1 - Host Analytics Information Security Hierarchy

INFORMATION SECURITY	
COMPLIANCE AND AUDIT	
ISO STANDARDS	
SECURITY POLICY	SECURITY ORGANIZATIONAL STRUCTURE
ASSET MANAGEMENT	HUMAN RESOURCES SECURITY
PHYSICAL / ENVIRONMENTAL SECURITY	COMMUNICATIONS AND OPERATIONS MANAGEMENT
ACCESS CONTROL	INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE
INFORMATION SECURITY ASSET MANAGEMENT	BUSINESS CONTINUITY MANAGEMENT

Source: Host Analytics, 2011

Security Policy

Host Analytics takes a holistic approach to security policy and risk management. The goal of the policy is to protect the company's employees, assets, information, and integrity—and by extension those of its customers—from potential threats. The policy is guided by ISO standards and conforms to Host Analytics' basic core values, code of conduct, and set of business ethics, which includes professionalism and respect for employees and stakeholders.

Organizational Structure for Information Security

Providing the right framework to achieve appropriate information security starts with the Host Analytics organizational structure itself. Host Analytics has a security team headed by a Director of Security that reports into the Host Analytics CIO/VP of Operations. The security staff possesses relevant security certifications and has decades of experience in information and network security. Focus and support from the CEO down ensures that all Host Analytics personnel understand their roles and responsibilities and are empowered to make the right decisions regarding the safety of customer data.

Host Analytics backs up this internal organization with carefully chosen external parties who bring expertise in specific areas of security, including vulnerability management, application code review, intrusion detection, and network analysis. Explicit policies are in place to guard against sharing sensitive information with third parties and external service providers.

Asset Management

All physical assets are assigned to a designated member of Host Analytics' management team, who is responsible for protecting and maintaining that asset during its life. An inventory of equipment and software, along with classifications of each asset reflecting its importance to Host Analytics' mission allows effective protection of Host Analytics' assets. All assets are disposed of securely at the end of their operating life.

Host Analytics maintains documentation outlining responsibilities and procedures for management and operation of all information processing equipment. Practices ensure consistent, secure configuration of all equipment operated by Host Analytics.

Human Resources Security

Even companies with the best technical controls can be vulnerable without adequate focus on personnel and their role in ensuring security. To address this, Host Analytics has policies in place to ensure integrity and ethical values among Host Analytics staff. These include publishing clear guidelines for employee practices, following formal hiring practices including a background check for all applications, and provisioning on-the-job training and other employee education efforts. Confidentiality and non-disclosure agreements are in place with all employees.

Clear lines of accountability are also important to human resource (HR) security. Host Analytics realizes that the control environment is influenced by the extent to which individuals have clear lines of responsibility and will be held accountable for their actions. The Host Analytics management team encourages individuals and teams to use initiative when addressing problems and holds all staff accountable for maintaining the highest security standards.

Physical and Environmental Security

Host Analytics maintains its primary data center in a state-of-the-art colocation facility in St. Louis, Missouri operated by one of the premier providers of managed infrastructure, hosting, colocation and private cloud services. This award-winning hosting provider is an authorized VMware Hosting Service Provider and Microsoft Gold Partner, and its facility maintains a wide range of security characteristics, including architectural design and facilities, power distribution and backup power supply, environmental controls, and high secure monitoring. It enjoys interconnectivity with multiple Tier 1 global service providers, providing direct access to providers that serve over 90% of the world's Internet networks.

Power Distribution and Backup Power. Multiple levels of power redundancy provide the highest levels of availability. Flywheel CPS (Continuous Power Supplies) and battery backup prevent power spikes or brownouts. Redundant backup diesel generators provide sufficient power to ensure the facility remains running in the event of public utility power failure.

Environmental Controls. Heating, venting, and air conditioning systems in a raised-floor architecture provide appropriate and consistent airflow, temperature, and humidity levels. The systems are fully redundant and monitored 24 hours a day, seven days a week. Water-cooled package chillers are arranged in redundant configuration and backed up by the generator.

Physical Security. Visitors to the hosting center must provide appropriate identification and cameras monitor activity throughout the facility including equipment areas, corridors and mechanical, shipping and receiving areas. Motion detectors and alarms are located throughout the data center, and silent alarms automatically notify security and law enforcement personnel in the event of a security breach.

Hazard Mitigation. The hosting center is equipped with state-of-the-art equipment designed to detect, suppress, and recover from fire, floods, and earthquakes. To provide fire detection and suppression the facility operates a Very Early Smoke Detection Alarm (VESDA) system and a Dry Pipe System. The VESDA system samples the air and provides early detection alarms to provide notification in the event of a fire. Dual alarm (heat and/or smoke) activation is necessary for water pressurization of the Dry Pipe System to minimize the chance of false alarms.

Flood control starts with the fact that the facility is built above sea level with no basements. The center contains tightly sealed conduits, moisture barriers on exterior walls, dedicated pump rooms, drainage and evacuation systems, and moisture detection sensors.

To address earthquake risk the building is located in a moderate seismic zone in the U.S. Midwest, with structural systems that meet or exceed design requirements of the local building code. All equipment and nonstructural components including cabinets are anchored and braced in accordance with the requirements of the 1997 Uniform Building Code.

Communications and Operations Management

Communications and operations management covers a number of areas pertinent to security, including network controls, protection against malicious code, backup and restore, monitoring and audit logging, and data transfer and integration.

Network Controls. Host Analytics uses a variety of network security appliances including firewalls, switches, and Intrusion Detection Systems (IDSes) to safeguard the integrity of its network. All critical network components are deployed in a redundant configuration to ensure maximum uptime. Host Analytics backs these up with network security management policies and procedures that document the appropriate response to be taken in various circumstances to ensure the integrity of the network is upheld. The Host Analytics network topology is shown in Figure 2.

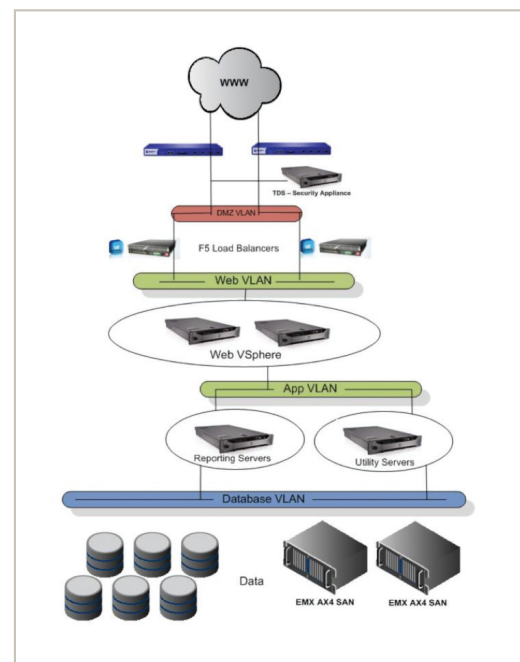
Protection against Malicious Code. Host Analytics follows accepted information technology best practices to safeguard against malicious code. This includes keeping operating systems up to date with the latest patches and security updates. To minimize the threat of viruses and other malware, Host Analytics constantly runs anti-virus software in memory where it can scan files every time they are accessed. All data introduced into the Host Analytics environment is scanned prior to introduction, including data from email, CDs and DVDs, Internet, and thumb drives.

Backup and Restore. As part of its core offerings, Host Analytics provides backup and restore services with alternate site backup replication. This is designed to increase data availability and protect customers' information from accidental loss or destruction. Host Analytics runs full data backups weekly and incremental data backups hourly, with all backed-up data stored on disk. This data is available for rapid reimplementation if the original data becomes compromised.

Monitoring and Audit Logging. Host Analytics uses a variety of third-party services to monitor and enhance application performance. These include services that simulate the user experience from locations around the globe, perform log management, monitor server performance to detect and enable resolution of any performance issues, and source code profiling to examine each transaction and identify poorly performing code. Host Analytics contracts with third party service firms to provide protection against denial of service attacks for its Internet presence.

Data Transfer and Integration. Host Analytics offers a number of methods to transfer data from customer's organizations to Host Analytics facilities. The standard Host Analytics user interface encrypts data via a Secure Socket Layer (SSL) connection or through secure FTP with PGP encryption. Deeper-level integrations are performed using an enterprise integration engine, database connectors, or web services and are protected using encrypted data transmissions. Host Analytics employs content monitoring and filtering to detect inappropriate data flows, with user access within the Host Analytics application restricted by user type.

Figure 2 - Host Analytics Data Center Network Architecture



Source: Host Analytics, 2011

Security of System Files. Only authorized Host Analytics personnel have access to system files and program source code. System libraries are kept separate from production systems, and physical access to equipment is controlled by biometric entry systems. Access to system files and program source code is controlled by system passwords and change management procedures control all changes and installation of software to minimize risk of corruption. Operating systems and virtual machine instances are hardened to provide additional protection against unwarranted intrusion.

Access Control

Access controls cover user access rights, management, and control. It covers best practices both on the Host Analytics side and on the customer side.

User Access Management. Host Analytics requires unique user names and passwords that must be entered each time a user logs on. Users must select strong passwords that conform to specific requirements and must make regular password changes. For users with higher security requirements, Host Analytics supports two-factor authentication.

The Host Analytics application uses a role-based security model with all requests validated against the role-based model. User sessions are timed out if the application is left inactive for more than 20 minutes. Username and password rules are configurable by the customer's administrators through the Host Analytics application.

Single Sign-On (SSO). Host Analytics supports SSO for customers who prefer to perform authentication on their intranet and then be redirected to the Host Analytics site. The trust mechanism can be based on encryption, time stamps, and/or username and password. The primary protocol is standard HTTPS, although if customers have unique sign on requirements those can be supported as well.

User Responsibilities. Host Analytics understands that the responsibility for ensuring good security does not end at the edge of its network, and that the customer plays an important role. It has published a set of responsibilities for customers, which includes maintaining and removing personnel from their organization who no longer require access, keeping software not provided by Host Analytics up to date, keeping access control lists (ACLs) up to date, and ensuring the integrity of physical locations and equipment used to transmit data to Host Analytics.

Information Systems Acquisition, Development, and Maintenance

This area includes cryptographic controls, security of applications and system files, and technical vulnerability management. To ensure high levels of cryptographic controls, Host Analytics uses SSL to protect sensitive information. When a user points a Web browser to the Host Analytics domain, a SSL handshake authenticates both the client and the server, and encrypts the session with a unique session key.

To ensure application-level security, the Host Analytics application is hardened to guard against the loss, misuse, and unauthorized alteration of data. Advanced security methods relying on firewalls and other technologies in the Host Analytics environment keep out unwanted intruders. Usernames and passwords are required each time a user accesses the application.

Technical vulnerability management is used to scan the environment for potential areas that could be exploited. Operator logs and fault logging are used to ensure information system problems are identified. System monitoring is used to check the effectiveness of controls adopted and to verify conformity to Host Analytics information security policies and standards. Host Analytics contracts 3rd party independent security specialists to scan for internal and external vulnerabilities. Scans are run routinely to ensure the infrastructure is vulnerability-free. Any security issues discovered are reported to information security staff and IT management, entered into Host Analytics' ticketing system for follow-up investigation, and tracked to resolution.

Information Security Incident Management

Host Analytics implements formal event reporting and escalation procedures for handling information security incidents. Employees, contractors, and third party users are provided annual security awareness training sessions that describe how to report and respond to different types of events. Alerts are monitored from the operating system and application, and real-time notification of security incidents are entered into the Host Analytics ticketing system and the appropriate Host

Analytics personnel are notified to address the incident. The resolution is then documented, allowing all problems to be tracked to completion.

Business Continuity Management

Host Analytics performs cross-functional assessments to identify risks that could affect its ability to meet its customer commitments. Assessments include identification of specific risks, their likelihood and impact, and controls required and in place. Host Analytics uses these assessments to establish mitigation and business continuity plans, the foundation of which is the business drivers.

Business continuity management plans specify practices to minimize the impact of an incident such as a natural disaster, accident, or deliberate action. They provide actions and responses to maintain or restore operations and ensure availability of information following critical interruptions. These plans cover the Host Analytics application and customer data, and emphasize people, processes and procedures to define who, how, and when backup personnel will take over to carry out key business functions.

A core component of the business continuity plan is Host Analytics' disaster recovery plan. Host Analytics mirrors all customer data at a geographically distant backup data center by performing live replication of all virtual machines and shipping live database logs via secure VPN. In the event of a catastrophic event at the primary datacenter, Host Analytics simply changes the DNS and spins up the new virtual machine, meaning customers can be back up and running in a span of hours or less. Customers who desire additional recovery options can also export their data to CSV format via the user interface and store that data in an alternate location.

Compliance and Audit

Compliance is particularly important to many Host Analytics customers given the nature of the data they are entrusting. Host Analytics follows a risk-perspective methodology, continuously assessing all elements of risk from corporate business risk to specific security threats. These risks are evaluated and categorized, and mitigation plans are identified and put into place. Host Analytics performs this process on an ongoing basis.

Host Analytics guides all aspects of its information security program by the International ISO 27002 standard, and performs regular SAS 70 Type II. These standards provide guidelines in terms of access controls, change management, disaster recovery, and protection of the data center designed to ensure the security, privacy, and availability of customer data. Finally, Host Analytics provides the foundation for customers to maintain their own compliance with Sarbanes Oxley, PCI, HIPAA and other standards.

Host Analytics sponsors security audits performed by third party firms on a regular basis, and performs regular self-assessments. These include ongoing third party secure code reviews, vulnerability scanning, and network penetration testing. Audits are performed with the assistance of automated security assessment tools.

Availability and Scalability

Host Analytics has built its application to ensure high availability and scalability. This begins with the application architecture.

Application Architecture

The Host Analytics application was developed on the Microsoft 2008 platform and subscribes to the .NET specification. It is based on a high-availability VMware architecture with a fully redundant network backbone. The application is written in C# and dynamically produces every page and sends it to the user's desktop encrypted using SSL. No static HTML pages or content is delivered by the application unless required by the customer.

The application is housed in the primary datacenter with a second, geographically distant, datacenter as a backup. Data is stored using AES-256 encryption. Data is backed up hourly, and stored backups use 228-bit encryption for their protection.

To ensure maximum uptime, every component in the Host Analytics infrastructure is redundant. There are at least two of each hardware and networking component that processes the flow and storage of data. Host Analytics load-balances at every tier in the infrastructure, from the network to the database servers. Database servers are mirrored for failover and application server clusters are enabled to ensure that servers can fail without interrupting the user experience.

Scalability

Host Analytics provides scalability by performing load forecasting and building in excess capacity. Excess capacity is available at all times via fully configured servers operating in standby mode. When peak loads increase, new servers are brought on line to ensure that substantial reserve capacity is maintained at all times.

Privacy

Personally Identifiable Information

When companies talk about privacy it's often in regard to personally identifiable information (PII), information such as social security numbers, name and address, and date of birth, which when used in combination could replicate an individual's identity online. Host Analytics has measures in place to ensure PII does not fall into the wrong hands, based on the security procedures and technologies described previously in this paper. In addition, customers can access their PII and update it at will, and Host Analytics does not disclose PII without the customer's consent. Further, Host Analytics has a third party arbitration process in place to resolve conflicts around whether PII was inappropriately exposed.

Separation of Customer Data

Many Software-as-a-Service vendors providing shared web access via multi-tenant application architecture have one set of database tables in a normalized database shared by many customers. This is not the case with Host Analytics. Host Analytics customers share the network security infrastructure, web servers, application servers and database instance; however each customer has its own set of database tables and its own partition in the database containing its own unique database schema with no logical communication allowed between customer database instances. Each customer instance can be completely exported out of the database without affecting any other customer.

Conclusion

Host Analytics takes its responsibility to security, privacy, and availability seriously. With customers entrusting it with their financial data, Host Analytics is committed to maintaining the appropriate standards of security. Host Analytics has put into place a tiered, multi-level approach to safeguarding customer data. Based on the ISO standards and subject to regular SAS 70 Type II audits, this approach touches all aspects of Host Analytics' business operations, from organizational structure and human resource policies, to physical and environmental security, access controls, information systems operations and maintenance, and incident management.

Business continuity and disaster recovery plans ensure continuity of operations, while the application architecture ensures application uptime. Security and audit measures allow customers to meet compliance requirements. Attention to the safety of customer data has paid off, as Host Analytics has not experienced a single major security breach in the more than ten years it has offered its SaaS services, and its focus on availability has allowed it to deliver 99.99% uptime for its customers.

hostanalytics

decide

Host Analytics Headquarters:
Host Analytics, Inc.
900 Island Drive, Suite 203
Redwood City, CA 94065 USA

Phone: 650 249 7100
Fax: 866 896 1738
Toll Free: 866 391 HOST (4678)
Email: info@hostanalytics.com

www.hostanalytics.com