White Paper

Cloud-Based Data Security

SaaS-built Galileo collects and analyzes customized performance data efficiently, on-demand, via a secure Internet connection.

GALILEO Performance Explorer®

About Galileo

Created by the ATS Group, Galileo improves IT utilization and capacity planning with convenient cloud-based performance monitoring. Evaluate hundreds of charts and metrics. Galileo delivers analytical perspectives of server and storage hardware and virtualization environments—to ensure optimal performance of physical and virtual servers and storage. Built on a SaaS architecture, Galileo installs in minutes without onsite data or hardware requirements. Automatic collection of real-time data and quick, easy, graphical reporting via an intuitive web interface offers access to custom dashboards with full drilldown into data details.

Table of Contents

Executive Summary

Software as a Service (SaaS) delivery models have had a profound impact to how businesses can more-efficiently communicate, collaborate, and achieve tasks—while delivering more data, to more places, from more access methods (e.g., tablets, smartphones, desktops). Businesses can now rapidly access data in the cloud that once resided solely behind a corporate firewall and required users to be in the office or use complex Virtual Private Network (VPN) systems. As cloud computing evolves, businesses will continue to demand more access to data. The role of the SaaS provider is to protect your data at the highest level of security.

This paper addresses the security measures of Galileo Performance Explorer® that provides a secure environment for your data. Galileo uses a multi-layered and multi-faceted approach to data security, designed to protect your data in transit and while at rest in the cloud.

The Problem

Security Threats are Vast

Compromised data often results in the loss of trust with your current and future customers. It could also mean the loss of trade secrets, identity theft, or even worse, the downfall of your entire business. Security threats have moved from what were primarily network based attacks to sophisticated website and application vulnerability profiling and eventual exploitation of those vulnerabilities. Worse yet, underground communities and massive “botnets” are being utilized to launch large scale denial of service attacks against providers—crippling infrastructure for hours and even weeks—leaving customers unable to access their data.

No single solution exists today to identify, prevent, or mitigate these security issues. Instead, SaaS providers of cloud-based tools must employ a multi faceted approach to security for both the physical and logical architectures of the solution for their end users. Technology can assist in the prevention of these attacks, however, the rigidity of policies and procedures are often the most critical pieces to security.

The Solution

Protect Data at the Source

One obvious solution to protecting offsite data is to minimize or eliminate the transmission of sensitive information deemed to pose security threats to your organization. That means that data security and integrity must start at the source. Galileo employs several methods to ensure that your data is scrubbed of sensitive information before the data even leaves your organization. So, even if your performance data is compromised in transit, it could never be used to uniquely identify your company, your customers, or open the door to potential hacking.

Galileo: Agent Data Security

Galileo uses a customer-side agent to collect performance metrics for each managed server. In most cases, the Galileo software gathers information from 'Operating System-native' utilities coupled with Galileo-written utilities and scripts. In order for data to be collected and forwarded to the Galileo infrastructure, the agent must first be registered and authenticated. The registration process uses machine-based authentication using a Certificate Authority (CA), signed and managed by the ATS Group. This authentication guarantees that data will be securely transmitted from your organization to the cloud using SSL. It also prevents unauthorized data transmission by non-registered agents.

Data transmission is unidirectional and outbound only, and at no time is data ever transmitted inbound to a customer server. The outbound data from the agent contains both relevant performance metrics as well as information to help identify the client to the Galileo servers. Server information such as IP addresses, host names, server model, and server serial number are included in the data transmission along with system performance metrics. For customers concerned with protecting this system-specific data, the Galileo agent can be optionally configured to either scramble or, in some cases, completely remove these metrics prior to the data being transmitted.

The agent communication process is similar in nature to devices that utilize "call home" capabilities, a process that allows system availability and performance metrics to be automatically transmitted to a third-party vendor at an offsite location. In fact, you may already have devices in your data center today leveraging this type of communication under similar security measures.

It should be noted, Galileo does not transmit nor store any Personally Identifiable Information (PII), such as Payment Card Industry (PCI) data, user id's or associated user names, social security numbers, phone numbers, addresses, biometric records, or birthdates; rather, all captured data transmitted is specifically related to IT data center performance on systems utilizing native OS and Galileo-developed tools. The Galileo client agent does not have visibility into databases, or other structures either on disk or in memory that would allow it to glean such information.

While we don't specifically capture financial information, Galileo is nevertheless hosted on systems owned and operated by Galileo/ATS in a secured colocation space that is accredited by the Statement on Standards for Attestation Engagements 16 (SSAE 16) as set forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The Colocation is further accredited by the Service Organization 2 (SOC 2) Type II examination bodies that set standardized security benchmark controls regarding data center testing and operational effectiveness, and are considered among the strictest standards for hosted and processed data, as defined by the AICPA.

We strive to adhere to some of the strictest current data transmission security regulations and standards set forth by both governmental and industry-specific regulatory bodies.

For example, the Federal Information Processing Standard (FIPS) 140-2 dictates very specific regulations when it comes to cryptographic components. Whenever applicable, Galileo utilizes FIPS 140-2 compliant SSL encryption modules on all systems receiving data from our customers. We are actively continuing to fine tune Galileo's security posture to ensure the strictest security of our customers' data - now and in the future. Our security evolves based on the current state of the industry, and we strive to be at the forefront of these efforts. We take great pride in utilizing proper methodologies and practices to ensure that we're protecting your data and our infrastructure.

Our developers and engineers practice secure development methodologies; our systems are continually audited for vulnerabilities and potential exposures as well as employ staff that focus the majority of their work days to keeping Galileo secure from internal and external threats using processes and procedures gleaned from decades working with Fortune 500 companies, the energy sector, telecommunications, and government entities who demand top-notch security.

Security Highlights

Agent Data Collection

Agent registration ensures authenticated access

Performance and machine metrics only

Optional scrambling or removal of sensitive data

Data Transfer

Outbound SSL communications (HTTPS) only

Communication is machine-authenticated

Secured by a certificate signed by the ATS CA

Web Portal Access

SSL communications (HTTPS)

User-authenticated web portal

Secured by a certificate signed by a trusted 3rd party Certificate Authority

Physical Security

24/7 operations center

Badge and biometric security access

Secure server cabinet

Internet firewall

Galileo: Web Portal Access

The Galileo web portal provides an initiative user interface that enables administrators and managers to view the performance data collected from their servers. Users access the web portal from a standard web browser over an HTTPS connection and secured by a certificate signed by a trusted third party CA. In addition, the web portal requires password-protected user authentication to prevent access to the data by anyone not authorized to access the portal. Users have access only to performance data related to their servers.

Galileo: Physical Security

Physical security consists of the measures in place to protect direct, physical access to the power, HVAC, network, and server infrastructure that operate web based applications. Our main data center must undergo stringent analysis for the presence, implementation, and ongoing administration of physical security infrastructure. Galileo operates its cloud infrastructure in a facility that has been audited by industry-leading compliance firms. As such, our facility has demonstrated control and accounting measures in place for physical security and maintains strict security policies and practices.

The physical location and design of this facility assists in the prevention and mitigation of both natural and man made assaults. The facility was selected based on a natural disaster scenario risk assessment, as well as flood plain screenings and evaluations. To further enhance the security of the infrastructure, no identifiable markings, or signage is visible from the exterior. All power and cooling systems are secured behind gated fences and are limited to authorized personnel. Each facility is equipped with solid block exterior perimeters and ramming bollards to mitigate potential damage to the infrastructure from exterior sources.

Security personnel control access to and from, including the monitoring of individuals within the facility. Access to our facility is limited to specific individuals for the purposes of maintaining and managing the infrastructure. Under no circumstances are unauthorized individuals granted privileges to enter.

The Galileo data center utilizes state of the art biometric scanning equipment for access to sensitive and restricted areas. These systems permit only authorized individuals into these areas, and log and report all access for historical reference and review purposes. Galileo's facility operates high resolution, continuous surveillance security cameras which monitor the movement of individuals throughout the facilities. These cameras are monitored by security personnel and also record all feeds to DVR systems which are maintained for historical reference and review purposes. Galileo's physical infrastructure equipment is always segregated from the collocation population with individually locked racks. These racks require physical key access which is only provided to individuals authorized to access these areas.

Galileo: System Security

Galileo operates primarily on the Linux® Operating System. Each system deployed for use in our production facilities is imaged to contain only necessary software required to operate Galileo. This practice, known as host hardening, reduces the likelihood of host exploits by limiting the software, processes, and open ports enabled on each system. Periodically, these systems undergo an evaluation of software, patches, and recommended updates to ensure proper function and to patch any security threats. Access to these processing systems is limited by Galileo's security policies and is granted only to those which require it for purposes of administration and maintenance of the system.

Galileo: Security Policies

Internal security policies developed by the ATS Group for Galileo specifically addresses physical, network, system, and data security.

These policies include, but are not limited to:

- Access Control (Physical, System, Network, and Hardcopy)
- Centralized Desktop and Laptop Antivirus & Malware Protection
- Desktop/Laptop security policies which enforce rules surrounding:
  - Software Installation and Usage
  - Network Accessibility
  - Periodic Password Resets
  - Credential Failure Lockout
  - Idle Screen Locking
- Employee Background Checks and Drug Screening
- Employee "Customer Data Confidentiality Agreements"

Conclusion

As businesses move sensitive data to the cloud, SaaS providers are faced with the growing challenges associated with keeping this data safe. Data breach, network intrusion, or denial of service threats are constantly evolving and require experienced security professionals. Galileo's multi faceted approach to security, backed by stringent security policies, industry leading threat protection, and mitigation solution deployments help keep your data private and safe.

GALILEO Performance Explorer®

07.08.15