GRANICUS SECURITY

govMeetings: Legistar, Media Manager and Video

GRANICUS OVERVIEW

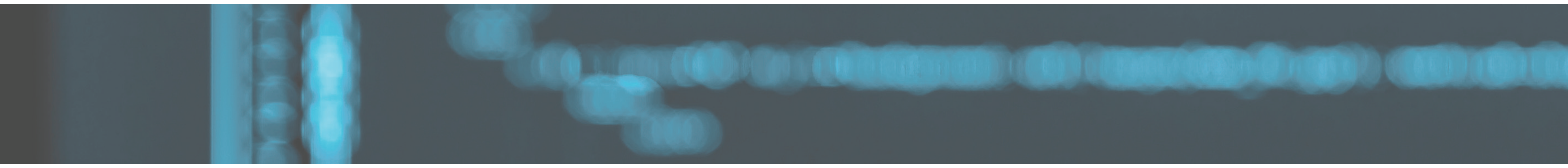
Granicus partners with 4,200 government agencies to deliver seamless digital experiences for millions of citizens. Government agencies use Granicus to communicate with people, manage meeting agendas, minutes and recordings, digitize records, and deliver citizen-first websites and digital services. These critical services drive Granicus to prioritize security and privacy of data. Therefore we adhere to best practices set in place by top government security organizations such as the National Institute of Standards & Technology (NIST) and our data centers meet SOC 1 & SOC (SSAE 16) requirements. Everyday, we monitor and protect your information because, in short, your data and system security is our top priority.

Data Center Security

With Software-as-a-Service based solutions a robust and secure data center implementation is a necessity, not an option. Granicus Data Centers are designed for reliability and redundancy. Our data centers are guided by a “defense-in-depth” security strategy to ensure reliable access of government data. With a 99.9% uptime, we are confident that customer data is consistently available.

Data Center Requirements

- ✓ Secure - SSAE-16 Accreditation
- ✓ Reliable Network – 7 ISP’s
- ✓ Data Availability: 99.9% Uptime
- ✓ Off-site Backups
- ✓ Encrypted data at rest



Granicus Server Locations

Primary Data Center in Ashburn, VA. Off-site backups at AWS US East - 1.

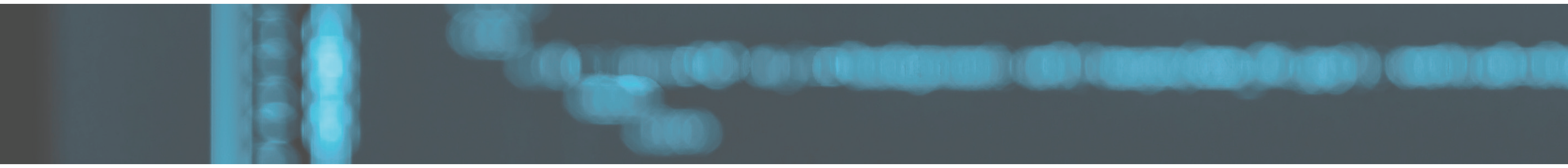
Architecture & Data Center Redundancy

The Granicus Primary Data Center is architected with redundant systems to avoid any single point of failure to ensure that disruptions have minimal to no impact on the availability of Granicus applications.

Robust Security Layers

Granicus provides a series of protective security layers. These layers add additional deterrents and protection against potential hacks providing the best possible environment for your data and instances of the Granicus applications.

- ✓ Hosting facilities that meet or exceed Uptime Institute's Tier III standards that are engineered to ensure application and data availability and security
- ✓ Edge-to-edge security, visibility, and carrier-class threat management and remediation. We utilize industry-leading tools to compare real-time network traffic and flag any anomalies such as: Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, worms or botnets.
- ✓ Network issues: traffic and routing instability, equipment failures, or misconfigurations
- ✓ Hardened, stateful inspection firewall technology
- ✓ An Intrusion Detection System (IDS) utilizing signature-, protocol-, and anomaly-based inspection methods
- ✓ 24/7/365 firewall, VPN, and IDS support and maintenance



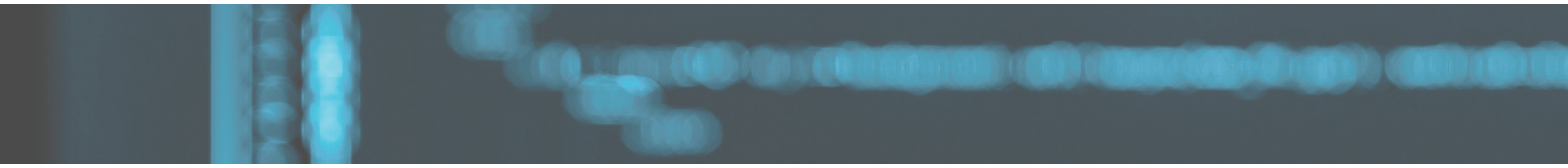
DATA SECURITY

Data Encryption

Granicus uses FIPS 140-2 validated cryptography standards created by NIST and required for all Federal Government agencies. We therefore encrypt all data - both in motion and at rest, at the highest level of Department of Defense (DOD) standard. Additionally, Granicus solutions access data across the Internet from secure and encrypted TLS 1.2 SSL connections, ensuring the protection of in-motion data.

Network Access Controls

Access to Granicus servers requires the use of a VPN connection paired with multi-factor authentication requiring a YubiKey. A YubiKey is a key-sized device that plugs into your computer's USB slot, so that even if credentials are hacked, the physical security of YubiKeys ensures the system is still immune from replay-attacks, man-in-the-middle attacks, and a host of other threats.



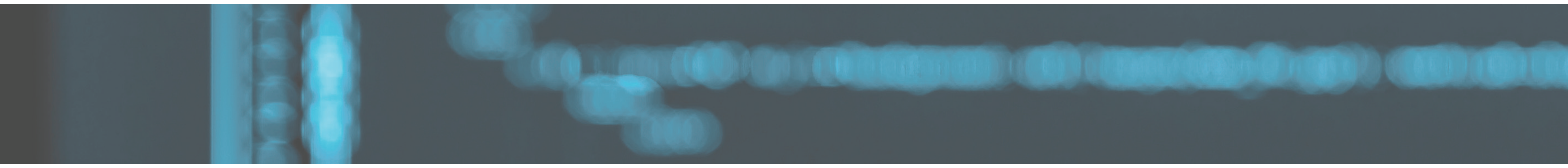
PHYSICAL SECURITY

Granicus solutions are hosted in dedicated spaces at Tier III Certified data centers certified by the Uptime Institute. The data centers are also SOC 1 & SOC 2 (SSAE 16) certified, requiring five concentric security rings and constant monitoring of common and restricted areas. Security protocols required by these top certifications include:

- 24/7 armed security guards
- Card access, biometric fingerprint and iris scan identification systems throughout the facility
- “Mantrap” entry
- CCTV and recorders
- Perimeter fencing
- Motion detection hand geometry readers
- Redundant HVAC units to provide consistent temperature and humidity
- Environmental hazard sensors, including smoke detectors and floor water detectors
- Raised flooring to protect equipment from water damage
- Fire detection and suppression systems
- Redundant (N+1) UPS power subsystem with instantaneous failover

Redundancy – High Availability Architecture

Every component in the SaaS infrastructure is redundant. There are at least two of each hardware component that process the flow and storage of data. All network devices, including firewalls, load balancers, and switches are fully redundant and highly-available. All internet traffic is balanced across 7 ISP’s for high availability and to ensure connectivity.



SECURITY MONITORING

Security Scanning

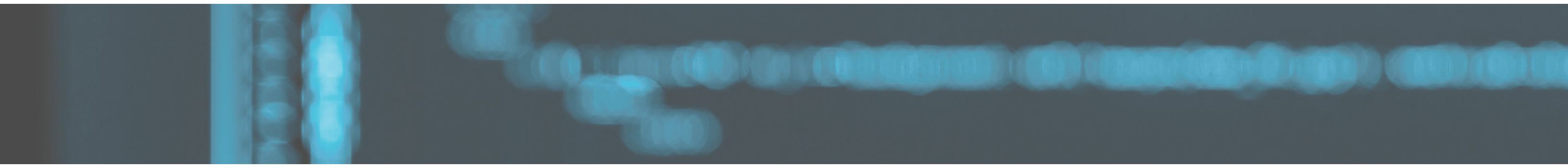
Because there's new security vulnerabilities being exposed every single day, Granicus takes a proactive approach to address them by scanning the application, host, and database layers every 30 days with updated security vulnerability reports.

Centralized Logging

Logs provide deep insights into application activity, including potential hack attempts. With centralized logging of all activities and changes across application host infrastructure, Granicus is able to aggregate the data to proactively monitor activity to discover potential threats.

Automated Virtual Server Management

Granicus servers are configured based on the Center of Internet Security's (CIS) best practices. The automated management of these servers means that our servers will rewrite settings back to the standard configuration every 30 minutes.



GRANICUS SUPPORT RESPONSE

SECURITY LEVEL	Description	Examples	Initial Customer Response Time
LEVEL 1	**Emergency** Incident represents a total outage; the product is unavailable or not accessible for use	• govDelivery's admin.govdelivery.com is down or all sending is significantly delayed • govMeetings web server is running but the application is non-functional or SQL-server errors that are not related to hardware • govAccess website is unreachable by public users	Within one (1) hour of notification by the customer of occurrence
LEVEL 2	**Severely Impaired** Incident occurs when a major feature of the product is not working and there is no workaround available, or the workaround is not acceptable and impacts the primary usability of the product	• govDelivery's PageWatch sending is delayed by more than 20-30 minutes, sudden and significant deliverability issues or intermittent errors or low performance issues for some or many customers • site operational but govMeetings modular functionality is non-operational • Customer's auto-sender via the Civica website isn't working but emails can be sent manually • govAccess error, where there is no means of circumvention, that renders an essential component of the content management tool non-functioning that did not occur at the time of the website launch and usually requires debugging of programming code	Within four (4) hours of notification by the customer of occurrence
LEVEL 3	**Impaired** Incident occurs when a primary feature of the product is not working as expected and an acceptable workaround is available – does not impact the basic usability of the product	• govDelivery system not connecting to social media, single customer app/feature help, or database requests • govMeetings system files won't upload, or text not rendering • govAccess website works but there are problems with presentation	Within one (1) business day of notification by the customer of occurance

Resolution time will be based on the service or support request and regular follow-ups will be communicated with the customer on final resolution. Granicus shall use commercially reasonable efforts to resolve errors affecting non-essential components of Granicus Solutions, or errors that can be reasonably circumvented but errors that require debugging of programming code may need to be corrected during the next regular update cycle.