Satmetrix NPX: Safe and Reliable

Focus on Security and Usability Makes Satmetrix Software Safe and Easy for Every Organization to Use

Security and reliability are top-level concerns for any business considering a new software solution or service. Before getting into the finer points of features and capabilities, every business must be certain that their data will be kept safe and that the system will be up and available whenever it is needed.

At Satmetrix, we share those same concerns and have hardcoded security and reliability into every aspect of our organization and operating procedures.

It starts with a redundant, three-tiered network architecture infrastructure that we entrust to only the world's best and most secure data center providers. It continues with multiple policies and processes that cover everything from account access and new development to data retirement and disaster recovery. And it ends with dedicated staff, whose diligent monitoring safeguard each of our systems from security threats and network failures.

Together they form a system of controls and processes that ensure that your customers' experience information and programs are safe and available to you at all times.

Make Security and Reliability a Part of Your Program

To ensure security, we deploy a three-tiered network architecture infrastructure, in which all applications are housed in state-of-the-art data centers and overseen by Satmetrix information technology experts. Protecting it at the top is a firewall that manages all IP addresses, making it difficult for intruders to go deeper into the network. And connection via only required ports restricts outside access. At the bottom and most secure level sits the database. In between are systems specifically designed to minimize threats from the latest malware, or damage from component failure. Together, it can withstand just about anything that humans or nature can throw at it.

Keep Your Customer Surveys Secure

Satmatrix takes extraordinary measures to ensure only those authorized receive access to your customer surveys, information and reports. Encryption tokens and authentication protocols guarantee the integrity and security of every survey and response. And access to reporting is conducted via an encrypted data exchange and can only be gained through a rigorous SSL authentication process that must be renewed before each session.

In practice, that means individuals can only gain access to surveys via an email invitation containing a URL link or by clicking on an embedded link on a website. On click, the link instantly takes participants to the survey where they can enter responses.

Survey feedback is returned over the Internet using name-value pairs that are not meaningful. For clients interested, an additional level of security of survey data entry, Secure Socket Layer (SSL) can be built into this process.

Only those with permission can gain access a given survey system. Those typically include:

•   Individuals who have been invited to complete a survey.

•   Employees of the client company who have been approved to view survey results.

•   Satmetrix employees who build and service the system.

Control Access to Your System

Your customer information is your responsibility, so we leave who has access to that information completely in your control. To that end, Satmetrix application account administration is managed by your company's designated contact, NOT by a Satmetrix employee. While many clients retain account logins for their Satmetrixaccount team, you can, if you want, remove all report access for Satmetrix employees.

For additional security and control, all authorized development and monitoring are done via Virtual Private Network (VPN) connection that uses 128-bit encryption. And as a rule, Satmetrix employees are never given broad access to the survey system at large. Instead, individual account access is authorized on an as-needed basis.

In addition, the Satmetrix database stores all passwords in a hashed form, and enforces strong password rules that include but are not limited to minimum lengths, complexity, and expiration. In the event of forgotten passwords, users are directed to a secure reset password page and process that requires verification before completion. Satmetrix will never email passwords to users.

Start with a Secure, Top-Tier Data Center

When you get right to it, your data is only as secure and reliable as the data centers that house it. To put all questions aside, Satmetrix only uses state-of-the-art data centers managed by leading top-tier service providers, located in the EU or the United States. All data centers are overseen by a Satmetrix information technology expert and must adhere to our rigorous standards for uptime, maintaining a precision environment, access control and physical security, and conditioned power.

The following measures ensure the physical security and integrity of all data centers:

Security Protocols

All centers are protected by keycard and biometric scanning protocols and around-the-clock interior and exterior surveillance. Access to the production areas is strictly limited to authorized data center personnel, who are subject to multiple and thorough background security checks before hire.

Environmental Protocols

The physical environment itself is maintained by a N+1 redundant HVAC (Heating Ventilation Air Conditioning) system, where the air is re-circulated every 90 seconds to remove dust and contaminants. Each center is also protected by advanced fire suppression systems and powered by an Uninterruptible Power Supply (UPS) for all servers.

Make Sure You're Always On and Available

A customer experience program is not worth much without uninterrupted access to accurate and up-to-date data and intelligence. Because uptime is so key to our service, we've put multiple measures in place to ensure our listening and reporting systems are always on and available. Those include:

Redundant Infrastructure

The infrastructure, on which Satmetrix applications are hosted, leverages redundancy and failover in order to ensure that no single fault can cause the service interruption to end users. All hardware devices including network, storage, firewall and load balancers are clustered. The storage cluster is configured with RAID for disk level protection and redundant firewalls in an Active/Passive cluster to provide a two-tier security perimeter. In addition, redundant load balancers are set up to distribute the workload of the web server cluster.

Ongoing Monitoring and Backups

We use state-of-the-art diagnostic tools to monitor network and system performance, and warn of possible failures and risk. Full weekly and daily incremental backups, which are stored in an encrypted and secure offsite data center. A thorough disaster and recovery plan. And a globally distributed workforce that stands ready to mitigate risks from business downtime.

Don't Take Our Word for It

While our word is important, independent third-party validation ensures we are keeping it. With that in mind, we regularly submit to and pass rigorous audits to meet the security, privacy, and availability standards of the global industry and governmental organizations that regulate our business. The validation can be found in the following reports and certifications:

SSAE16

All Satmetrix data centers run in Class A data centers with an annually renewed SSAE16 certification. The SSAE16 certification process not only reviews the data center policies to ensure they are effective but also checks that the data center is following its policies effectively.

ISO27001 Certified Data Centers

All data centers (but not Satmetrix directly) are ISO27001 certified by an external auditing organization accredited by the International Standards Organization. A third-party security firm reviews the Satmetrix policies, procedures, and network architecture annually based on ISO27001 requirements. In conjunction with this review, the third-party security firm also conducts penetration tests on Satmetrix production systems.

TRUSTe

TRUSTe has reviewed Satmetrix' privacy policy and practices for compliance with TRUSTe's program requirements (including transparency, accountability and choice) regarding the collection and use of personal information and has awarded TRUSTe's Privacy Seal to Satmetrix.

US and European Safe Harbor Frameworks

Satmetrix also complies with the US-EU Safe Harbor framework and the US-Swiss Safe Harbor framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland.

Additional certifications include:

- Payment Card Industry (PCI) Data Security Standard (DSS) Level 1 Service Provider
- Content Protection and Security (CPS) Standard
- SAS-70 Type II

Copies of the associated reports may be obtained upon request.

Secure Everything

Unfortunately, threats to the network go beyond the virtual environment, and you need to be just as vigilant in the physical world as you are outside of it. At Satmetrix, we take the physical security of our infrastructure and data centers as seriously as anything else. To protect what goes on inside our data centers, we only use reputable service providers that employ a variety of methods to prevent unauthorized entry (including 24/7 CCTV surveillance), maintain optimal environmental conditions and safeguard against fire and electrical interruption. To guard against virtual threats, we use a firewall detection and intrusion application called Alert Logic, periodically scan the network using Nessus, and perform security audits and penetration tests to ascertain and mitigate threats. We also deploy multiple controls – such as encryption and timed screen lockouts-- to secure our office network and equipment from any unauthorized intrusions or access.

Make Everyone Accountable

While technology is certainly important, the ultimate responsibility for the security of your information is with the people that manage it. At Satmetrix, we have put in place a combination of comprehensive policies and procedures that makes every employee responsible for the security of our clients' customer data and information. Those include everything from the following security policies that make understanding and adherence a condition of employment to audits and reviews that hold everyone accountable for upholding them.

Comprehensive Security Policy

As a condition of employment, all Satmetrix employees must read and agree to a comprehensive security policy that strictly prohibits them from, among other things, divulging client-specific data to other clients or third parties and using anything but company issued computers to work on company data and files.

Corporate Security Practices

The Satmetrix corporate network and technology is built and managed by internal IT staff from company headquarters in Redwood City, CA. The IT staff is charged with staying abreast of new developments in security products, procedures, and practices and applying them to Satmetrix's technology. Because a portion of the staff frequently travels to visit clients, the network has been specifically designed to accommodate the needs of mobile professionals for secure access.

Security Audits

Satmetrix performs periodic security audits that include measures, such as reviews of security controls, network vulnerability and penetration testing. These are used to evaluate and document the possible vulnerabilities and implement mitigation measures to eliminate potential threats to the system.

Secure Your Data Transfers

Transferring data can leave it vulnerable to threats. To ensure your files are transferred safely, we support Pretty Good Privacy (PGP) and provide a public key to any client that wishes to encrypt their files before sending them over to Satmetrix. We also support SFTP and recommend encryption before transferring files via ordinary email or FTP.

Satmetrix NPX
Best Practices Built Right In

Learn more about how our industry-defining customer experience management software can transform your business. Satmetrix NPX, the CEM software for customer-first companies, has a best-practice library built right in. Get the tools you need to manage a world-class customer experience program.

Request a Demo