Information Security Whitepaper

Introduction to Medidata's Information Security Program

Information Security is critically important to the safe execution of drug trials. Medidata has built a mature, validated information security program based on the widely recognized NIST 800-53 and CoBIT security frameworks. The integrity of the Medidata's information security program is evaluated and confirmed by multiple annual independent external assessments, including NIST 800-53/FISMA audits, SOC-1 Type II and SOC-2 Type II (with additional controls) audits, and ISO 27001:2013, 27018:2019 and 27701:2019 assessments.

Our information security program is the foundation of our industry-leading unified, intelligent platform that supports your end-to-end clinical development. Medidata's secure clinical cloud computing solutions deliver high availability, integrity, confidentiality, reliability and flexibility to enable our wide range of product offerings.

With the acquisition by Dassault Systemès, Medidata is ideally positioned to take advantage of the global scale that Dassault provides while continuing to deliver secure, stable and scalable infrastructure.

Trust and Transparency

Medidata's information security program, along with our Data Privacy and Quality functions, ensure that Medidata has created a secure, stable, and scalable cloud platform, robust data governance processes, and an inspection-ready quality management system — which, when you put them all together, are critical enablers for success in clinical trial execution. Visit https://www.medidata.com/en/trust-and-transparency/ to learn more.

"Information Security is crucial to the protection of patient privacy and in some cases their very life; when I became a clinical trial patient, the protection of my healthcare data became personal. I can tell you that as a security professional who understands the cyber threats, as well as a trial patient, Medidata is the only firm I want storing and processing my information."

Glenn Watt, Medidata Chief Information Security Officer (2007-2018)

This Whitepaper provides an introduction to understanding the focus, investment and expertise that Medidata brings to the forefront, in order to protect the data entrusted to us.

Program Overview

Effective Information Security is a program, not a checklist. Using a “Security-by-Design” and “Privacy-by-Design” philosophy, integrity in our systems is built in at the ground floor.

Medidata has a team of dedicated Information Security professionals, with over 350 years of accumulated Information Security experience in practicing InfoSec in the Life Science, Research, Technology and Defense industries.

Reporting directly to the Chief Information Officer, our InfoSec team is responsible for the full and independent management of the InfoSec program, which is based on the CobIT, ISO and Service Organization standards. This program is audited four times a year by independent third-party auditors including PricewaterHouseCoopers, Apex CyberTek and DQS.

Transparency is part and parcel to trust and to that end we provide a customer portal at http://www.medidata.com/trust which has the results of our third-party assessments, quarterly penetration test results, and quarterly vulnerability scan summaries across the entire environment. We also have an annual “Red and Blue” team engineering test which has the penetration testers working alongside the response team, in order to maximize learnings.

Infrastructure vulnerability scans, peer code reviews, static source code analysis, dynamic scanning of URL’s are all performed at least monthly or during any significant change in the environment. Additionally, prior to any product being released for General Availability, every product is scanned for vulnerabilities.

The core of the environment is hosted within Amazon Web Services (AWS) data centers, in the US-East, US-West, Frankfurt, Ireland and Paris for truly global coverage using a homogenous support and security model. We use Amazon’s security features including tight security groups, rigid network access control lists, CloudFront, AWS Shield and Advanced Shield, CloudTrail, Macie as well as the organic security built into all Amazon’s products.

We have our private cloud-based operation in Houston, Texas with an alternate processing site in Frankfurt, Germany in order to protect the systems in the event of a regional disaster.

In order to support the People’s Republics specific needs, we have a completely separate database instance in the AWS Ningxia, which has compliant security controls.

In order to provide 24x7x365 support, we use a Managed Security Service Provider, who is empowered to act to protect against any and all threats, regardless of the time of day.

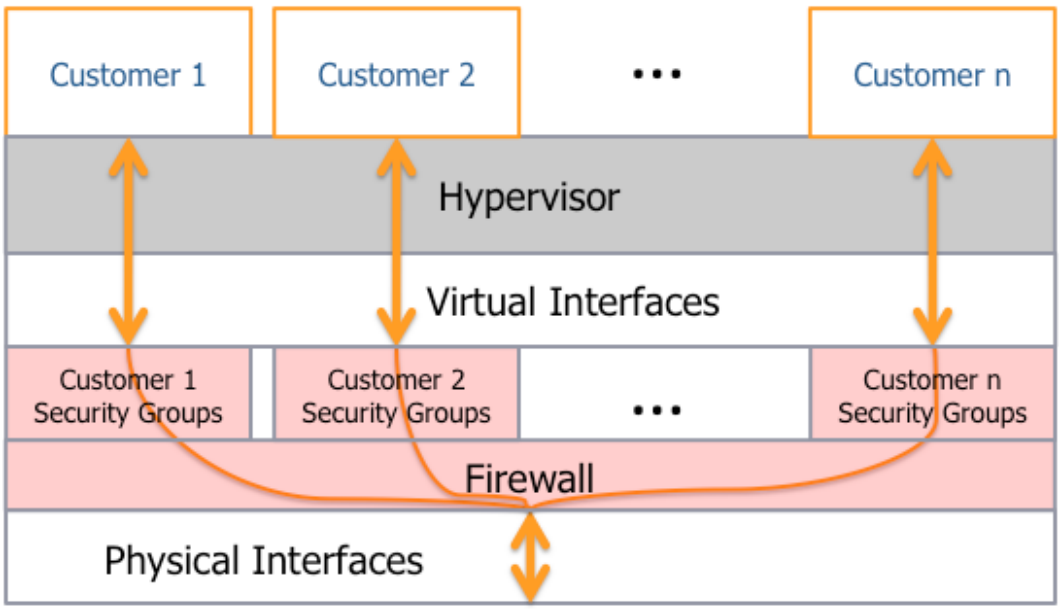
We are proud of the trust that our customers and their patients have provided to us, and we earn that trust every single day.

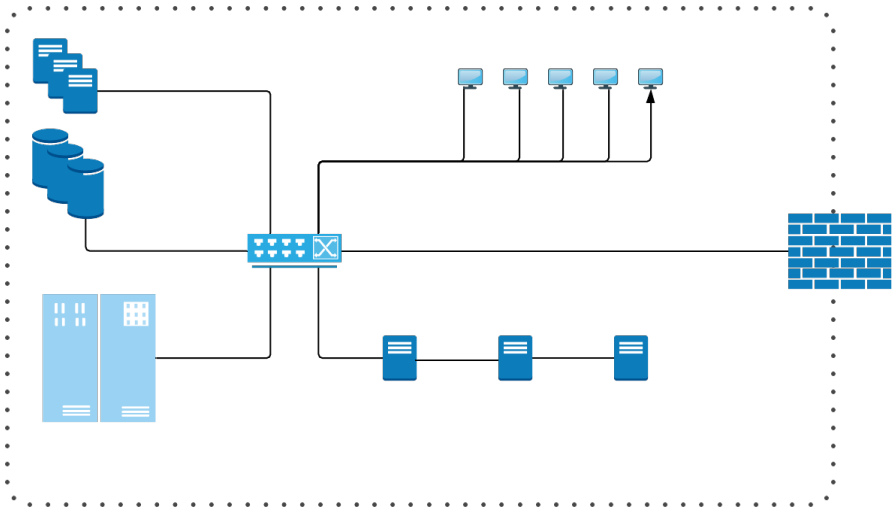
Cloud vs On-Premise Security

Security in the cloud is not managed the way it is in a legacy premise-based environment. The concept of bastion perimeter is more nebulous; without a single network connection to the outside world, you have to harden everything.

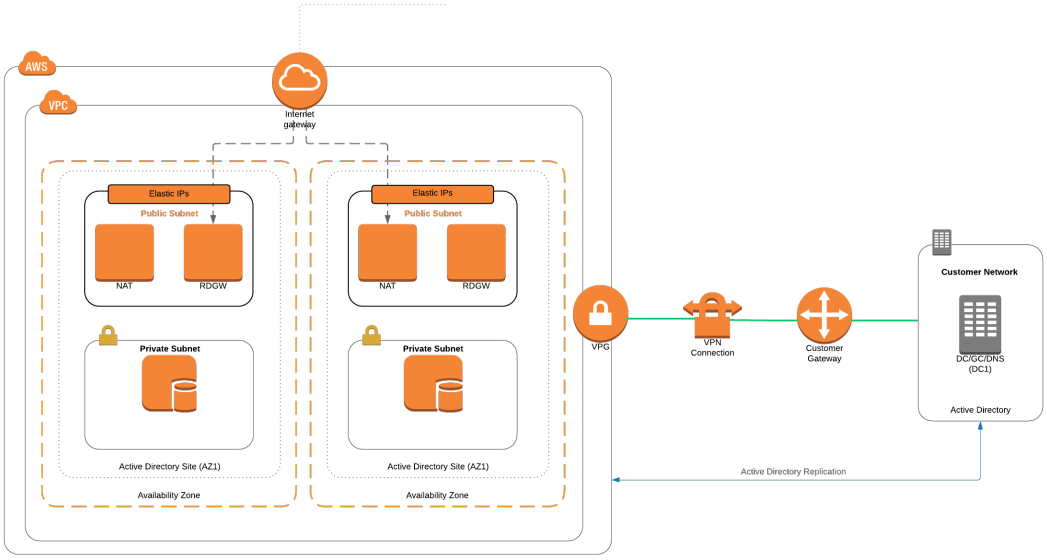
Cloud Security has matured beyond traditional data center security; rather than relying on a set of controls at the perimeter, controls and technology permeate the entire infrastructure and application layers. Where you had a perimeter firewall, you now have security groups, Network Access Control Lists (NACL), File Integrity Monitoring, Malware Protections, Log Inspection, Web Reputation checking and Web Application firewall layers on each and every host.

The hypervisor segregation allows for completely independent hosts and databases but converged to allow to take advantage of the advanced security features such as anti-beaconing monitoring, cloud access security brokers and web application firewalls.





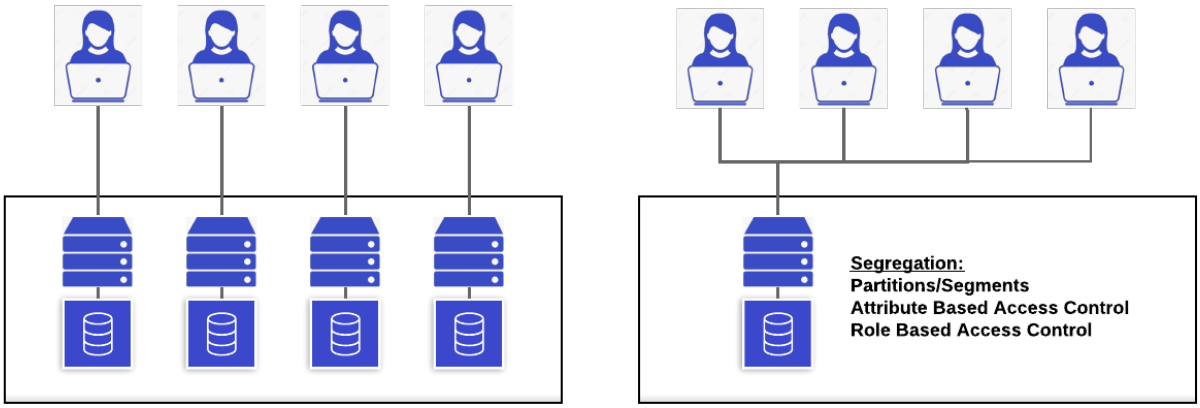
In a legacy premise-based environment, security services are enabled at the network perimeter, and where technology exists, installed on the hosts. With this configuration, consistency and speed of deployment is problematic. Maintenance of technical debt and consistent practice is difficult to perform, and once a malefactor is inside the perimeter, it is hard to track and stop.



In a cloud environment, security permeates the fabric of the infrastructure; with security control at every single layer, consistently applied, and centrally managed. This allows bringing new services to bear simultaneously across the entire environment, quickly and accurately. With detailed instrumentation, a malicious actor can be caught and contained, before there is a security event. Updates to any layer can be done in a matter of minutes and is much easier to manage and report against.

Tenancy

Tenancy refers to application architecture describing the relationship between the customer accessing the software and how those instances of that application are separated.



The first case is **Single Instance Single Tenant ("SIST")** - where there is one application, one database per tenant. Everything is dedicated to that customer. This means increased direct cost (more hardware), indirect cost (management) and is increasingly difficult to secure. In order to secure the environment, you have to apply "the control" or "the patch" or "the setting" to each instance perfectly, in order to have the homogenous barrier to malicious activity. Upgrades need to be carefully planned and coordinated and can take months to execute. It's also expensive.

In a **Multiple Instance Single Tenant ("MIST")**, each instance of a set of applications accessed by one tenant. Therefore, each tenant accesses a set of application instances, with the entire environment dedicated to them. The practical security differences are fundamentally not that different than **SIST**, but in this case, there is more than one instance of a particular application per customer. There's a lot of duplication of infrastructure, and underutilization is common. It's also more difficult to secure, for the same reasons as **SIST**.

In a **Single Instance Multi-Tenant ("SIMT")** environment, a single instance of an application operates and is accessed by a number of tenants. With **SIMT** applications, all customers use the same application while the customer data remains in logically separate databases, with different types of access control. **SIMT** applications are architected and designed such that customers cannot access data and configuration information that belongs to other customers. Segregation is achieved using a combination of techniques and tools, including Attribute Based Access Control (**ABAC**) and Role-Based Access Control (**RBAC**); leveraging these controls provide strong separation of customer data.

SIMT applications inherently carry less risk to the customer than **MIST** applications primarily because of the consistency of controls applied, and speed of response for changes and controls.

An upgrade or patch is applied to a single point and applied uniformly which provides a seamless barrier to malicious activity.

If developed using the same standards as **MIST** applications, customers adopting **SIMT** products realize immediate benefit from ongoing product enhancements — including enhancements driven by regulatory changes. **SIMT** application upgrades are fast, consistent and highly effective.

From a security perspective, it is far more effective to provide a seamless and holistic environment to manage, with a minimal attack service and better consistency of controls. In a commercial setting, it's also far less expensive to operate and maintain.

Governance and Management

The best information security programs are consistently supported from the top, starting with the board, and permeating through the entire leadership of an organization. The executives have the right background and pedigree to ask the right questions and provide proper direction with respect to the Information Security program and how it meets the organization's needs.

Medidata adopted an ISO 27000 standard Information Security Management System (ISMS), which drives a three-year strategy. Using NIST 800-53 as the set of governing principles, the guidance provided to the InfoSec team comes straight from the board of directors, maintaining independence from operational matters for maximum objectivity. The evolution of the ISMS includes the addition of the adjunct Privacy Information Management System (PIMS), which mutually one another.

Our NIST 800-37 based Enterprise Risk Management system goes beyond InfoSec, and helps manage risk in the Human Resources, Operations, Privacy and other areas of the business.

With respect to the InfoSec team, it consists of collective of experience of over three hundred and fifty years in Life Sciences, Technology and Information Security. There is tenure in the National Security Agency, the United States and Royal Navy as well as other heavily secured organizations.

Eight of our team members have the Certified Information Systems Security Professional (CISSP) certification, which is the pinnacle of InfoSec certifications, with four more targeted for 2020. We also have certified Incident Handlers, Forensics examiners, AWS Architects, CISA/CISM/CRISC, ISO Auditors, PCI ISA's and many more.

From top down, Medidata/Dassault Systemès Information Security team, has complete management support and guidance from the top, which allows the team to bring to bear centuries of experience, skills and techniques to the job.

Technical Controls

Technical controls are key success criteria in protecting patient data. Medidata makes significant investments in technologies, coupled with our “best-in-breed” security techniques and practices, provides a secure, stable and scalable architecture.

We categorize these controls into the following groups:

- Policy, Physical Security and Training
- Data Protection
- Endpoint Security
- Network Security
- Defect and Vulnerability Management
- Identity Management
- Monitoring
- Independent Testing and Review

The holistic design provides for defense-in-depth, which allows for a control to fail, while maintaining the confidentiality, integrity and availability of data within the systems.

Policy, Physical Security and Training

Policy

Policy is the guide to behavior, and without it, employee, contractor and vendor responsibilities would be unclear and imprecise. Our policies are based on commonly accepted frameworks including CobIT, ISO 27000 and HITRUST. All activity is monitored closely, and enforcement is strict and consistent. Every employee and contractor, at hire, and annually on the entire policy hierarchy, to ensure that the duty and responsibilities are clear and understandable.

Physical Security

All our data and systems are housed in TIA Level 3+ data centers in order to provide state-of-the-art protections at the front door. All data centers are unmarked with unpublished addresses, cameras with digital recorders, 24x7 uniformed guards, biometrics, mandatory photo-id smart cards, environmental sensors and more. Our corporate sites are similar, with tight access control uniformly applied throughout the entire environment.

Training

Education is something that is central to an effective Information Security program; without it, the technical controls cannot be brought to bear to protect patient data and other sensitive information.

Each and every employee is trained in an all-day “New Hire” program, which is the first exposure a Medidatian has to the company’s Information Security practice and is performed by one of the InfoSec leaders. This session is intended not only to sensitize the new hire to their responsibilities, but also emphasize the role of an employee in providing protections against insider risk, ransomware, social engineering, proper use of assets and other related items.

Developers get an extra Secure Code training, annually, which includes OWASP Top-10 and SANS Top-25 in order to minimize the risk of weak secure-coding practice.

If the role has access to sensitive information, or is a “control role”, additional training on their obligations and responsibilities is also held which can include high authority ID management, PII management, Data Governance policies and more.

All of the online training is conducted via a Learning Management System, and employees and contractors are held accountable for timely completion. This includes KnowBe4, a leading InfoSec training platform.

We refresh the education often – usually several times a year- in order to ensure that we make the internal community aware of the most recent and relevant risks.

Data Protection

Data Protection from the core where the data is stored, through the entire private cloud infrastructure. These data protections start at encryption, both where the data is stored at rest and while it is transmitted. Our philosophy of “Encrypt Everywhere”, which provides the most flexibility and safety, using the Advanced Encryption Standard algorithm, using 256-bit keys providing military grade protection across the entire environment.

Encryption-at-Rest

Encryption is enabled at the storage unit level and is effected through the use of hardware. For the EDC data stores, the Hitachi Storage Area Network uses 256-bit Advanced Encryption Standard (AES) keys, using a proprietary key management system. For our multi-tenant systems, we also use AES-256, but use Amazon’s KMS Product.

Encryption-in-Flight

All data transmission, whether internal or external, is encrypted using Transport Layer Security (TLS) version 1.2. We are evaluating TLS version 1.3; although it is not fully implemented across the industry, Medidata is ready to move to the new protocols, as soon as they are proven to be robust and secure.

We also manage our ciphers used in transmission tightly, such as AES_256_GCM and ECDHE_RSA with P-256 for proper key exchange.

Over the next twelve months, we will look to future proof (quantum protect) our ciphers. The current full list is:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
- TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048)
- Null compressors
- Client cipher preference

Data Loss Prevention

Movement of data is monitored real-time, using Data Loss Prevention tools and techniques. Starting with AWS's Macie offering, we also put proprietary tools in place to monitor data as it is stored and processed. Any suspicious movement of data alerts our InfoSec team automatically, and the data movement is locked down and investigated promptly.

Any data movement is governed by our ISO 27018 tested Data Governance program, directly supervised by our Chief Privacy Officer, as well as heads of Information Security and Global Compliance and Strategy to ensure that data protections remain intact.

Identity and Access Management

Perfect identity management is tough; very few organizations are able to achieve it with precision. In order to solve this problem, Medidata has implemented a “HRIS-As-A-Master” program, which automates provisioning and deprovisioning, reducing errors and omissions to an absolute minimum. Additionally, we audit the entire landscape every quarter, with those audits being reviewed by external organizations for maximum consistency.

Identity Management Standards

For our customer facing systems, the password requirements are:

- Eight-character password length
- Contains at least one uppercase letter, one lowercase letter and one number character
- Moderate strength (e.g., no “ILoveCats”)
- Must confirm to Electronic Records Electronic Signatures (ERES) requirements for signature
- Rotated every 90 days; 120 day forced rotation
- Cannot be one of the last ten passwords

Where possible, we encourage the adoption of MultiFactor Authentication (MFA) and are likely to mandate it in the near future.

Authorization is separated from authentication, because of the nature of how access is provisioned. iMedidata provides authentication into the environment; authorization grants access to the studies themselves. In order to ensure tight coupling to the supported organization, the Medidata customers manage~~d~~ access to the studies, as they are closer to the sites, and to promote maximum flexibility and response.

Password length is eight characters, with three types of complexity – upper vs lower case, symbol, number and alphabetic characters. We rotate passwords every 90 days.

Because we support 50,000+ sites worldwide, this is the commonly accepted baseline which allows varying technologies to access the Medidata platform.

MultiFactor Authentication.

Passwords, even if complex and rotated regularly, are not enough, so we offer Multi Factor Authentication (MFA). This allows either an SMS text message, Authy Authenticator or a voice call to provide additional certainty on the identity of the end user using a one-time token.

We are moving closer to a mandatory MFA across all accounts, as soon as the more remote sites are capable of supporting it. We expect as we get closer to the end of 2022, we will shift the majority of end users to use this key security service.

Endpoint Security

Each server has protections over and above at-rest encryption. Each and every host has the Trend Micro suite of tools installed and is fully integrated into Security Incident and Event Monitoring (SIEM) tool, so that systems are dynamically monitored, and any potential issues are responded to promptly; 24 hours a day, 7 days a week, 365 days a year.

Trend Micro - Malware

Trend Micro has emerged as a leader in the platform-based malware tooling space; providing not only signature based anti-malware software, but also logic that looks for new zero-day type virus, trojans and other malicious code. This is installed on each and every host in the Medidata environment and is monitored centrally by our Security Operations Center.

Trend Micro – Log Inspection

The Trend Micro Deep Security Log Inspection module provides the ability to collect and analyze operating systems and application logs for security events, which in turn feeds the Medidata Security Incident and Event Monitoring systems. Log Inspection rules optimize the identification of important security events buried in multiple log entries. These events can be forwarded to a SIEM system or centralized logging server for correlation, reporting, and archiving. The Deep Security Agent will also forward the event information to the Deep Security Manager console, which is managed by our Security Operations Center.

Trend Micro – Intrusion Prevention

Intrusion Prevention Systems (IPS) are suited to detect and stop attacks that originate over the network, including those focused on application and operating system vulnerabilities.

These systems monitor the entire environment for malicious activity or policy violations. Any intrusion activity or violation is collected centrally using a security information and event management system, and responded to by our Level 1, and if necessary, Level 2.

Trend Micro – Firewall

This host-based firewall complements the Palo Alto firewalls at the perimeter of the private cloud; and also, the AWS security group and network access control lists. These firewalls can block or allow certain types of network traffic by creating a barrier between the client and the network. Additionally, the firewall will identify patterns in network packets that may indicate an attack on clients. Installed on each and every host, they are integrated into the Security Incident and Event Monitoring systems.

System Hardening

Out of the box system configurations are often insecure; excess services, additional processes and extra posts are commonly default in operating systems, web services, database management systems and other components. Using CIS (Center for Internet Security) benchmarks, the most generally recognized secure system baseline available, we harden all our host and network components to Level 1 of that standard, before they are placed into services, by the use of our automated deployment practices.

System Lifecycle Management

Typically, when a component such as an operating system or Java™ is at the end of life, security support such as patching stops. Therefore, it's critical to retire those system before that point. Medidata's policies is to never have an end of life system or component in service; and aggressively manages updates in order to maintain that posture. Independent quarterly assessment ensures oversight on this; and that systems are upgraded well in advance of their retirement dates.

Update Management

The usual industry standard for applying patches supplied by Original Equipment Manufacturers (OEMs) is thirty days. This means that there is a significant window for malicious activity taking advantage of known and publish security defects. At Medidata, we target patching as soon as possible, with the internal target of seven days. Often, it is even less than that for urgent security issues. This maximizes a solid and well defended front against a hostile environment.

Network Security

Data protections must be more than simply encrypting; at Medidata, data is monitored as it flows through the environment. Each packet is monitored, inspected and tracked as traffic flows through the cloud environment. All network devices feed the Security Incident and Event Monitoring System, which in turn is monitored by our Security Operations Center for 7x24x365 response.

Firewalls

Enterprise class Palo Alto firewalls are installed at every network external endpoint in our corporate environment and private cloud. For AWS we use a combination of Security Groups, Network Access Control Lists (NACLs) and Web Application Firewalls (WAF). From an inbound perspective, we only allow ports 80 and 443. 80 is solely for the purpose of redirecting to the secure port for ease of our user community.

Intrusion Prevention and Detection

In addition to the host based systems mentioned above, Palo Alto's Intrusion Detection and Prevention Systems (IDS/IPS) is a network security technology built for detecting vulnerability exploits against a target application or computer; they also have the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies.

The IDS monitors traffic and reports its results to the Security Incident and Event Monitor (SIEM) and the Security Operations Center (SOC) for rapid response to emergent threats.

Malware

Palo Alto also brings unique malware prevention capabilities across the network, endpoint and cloud. The stream-based engine blocks malware in-line, stopping attacks before they can succeed, without impacting performance, providing high-efficacy malware prevention through multiple techniques, including:

- Consistent protection and enforcement across all deployment scenarios.
- Signatures based on payload, not hash, or other easily changed attributes.
- In-line, stream-based detection and prevention of malware hidden within compressed files, web content or other common file types.
- Near real-time updates from the WildFire® threat analysis service, ensuring protection against zero-day malware.

Anti-DDOS

Medidata, like other organizations, saw a significant increase in Distributed Denial of Service (DDOS) attacks in recent months, so in order to proactively defend against this emergent threat, we added additional anti-DDOS components, over and above the protective features in the Palo Alto firewalls and AWS Shield services. Using F5 Silverline, we are able to silence the botnets before they impact the services that we provide; and using AWS's Advanced Shield, we are protected from the most ambitious and aggressive botnet attacks.

Mail Filtering

Over 40% of the mail sent in the world is malware, spam and other unwanted mail. Medidata processes over 16 million email messages a month, so even 99.999% effectiveness implies that some of this will get through. In order to protect against that, Medidata uses Proofpoint for mail filtering, spearfishing attack prevention and secure email messaging, reducing this threat to an absolute minimum.

Defect and Vulnerability Management

A security vulnerability is a special class of defect; in that it not only can affect the stability of an environment, but the confidentiality and integrity of the data and the systems that process that data. Our multi-layered program is iterative, comprehensive and aggressive and designed to minimize attack surface, security vulnerabilities and risk to customer data.

Vulnerability Scans

We scan everything, internal and external, across the entire Medidata environment, every month, using Rapid7 Insight Vulnerability Manager. The results are populated into our ticketing system, evaluated for risk, priority and put into the backlog for remediation. Critical vulnerabilities – those with no compensating controls that pose significant risk – are resolved as soon as possible; with an emergency release if necessary. Vulnerabilities rated “high” are fixed within 30 days, “medium” within 180 days and “low” annually.

These scans are credentialed; in order to get in as deep as possible to scour for bugs, misconfigurations and other defects.

We also scan every application release prior to General Availability, in order to ensure that no software is released with security weaknesses.

Static Source Code Scans

Static source code scanning is the practice of analyzing software code prior to compilation and deployment.

Static source scans for the entire code base is done monthly, and prior to product release, using BurpSuite Enterprise, WhiteHat or Brakeman. These scans are also credentialed for maximum effectiveness of the tools.

We also put the source code scanning tools directly in the hands of developers. The earlier in a cycle that a defect can be fixed, the less risk and cost is incurred.

Dynamic Scanning

Dynamic code analysis, or scanning of compiled/deployed code, is capable of exposing a subtle flaw or vulnerability too complicated for static analysis alone to reveal and can also be the more expedient method of testing.

At Medidata, we feel that both dynamic and static scanning provides a holistic and more complete testing regime in order to maximize the number of findings in the most scenarios, and therefore reducing overall risk.

Free and Open Source Software

Managing Free and Open Source software licenses is critical; we have over 8000 open source packages, and in order to effectively manage that, we use FOSSA. This tool allows us to determine the proper licensing model in order to prevent risks associated with inappropriate deployment of open source software.

Threat Intelligence

Medidata uses a variety of tools and practices with respect to Threat Intelligence. Our Managed Security Service Provider (MSSP) alerts Medidata to emergent threats; but we also ingest feeds from a number of data sources, so that new attacks are stopped before they impact our systems. We also use Cisco StealthWatch which provides comprehensive visibility into the network traffic and provides advanced threat detection and accelerated threat response using advanced behavioral analytics.

Penetration Testing

Due to the shared nature of the environment, we cannot allow customer penetration or vulnerability testing of our environment.

Because our customers expect comfort around how we protect their data, we provide full transparency into our Information Security Penetration Testing program; posting the detail tests and their results online for perusal by our customer's security experts. To date, no penetration test has succeeded in gaining access to patient data.

Every 90 days (adjusted to correspond to release cycle), we bring a different world class penetration testing entity to attempt to gain access to our environment, testing our monitoring and alert and in general confirm the integrity of the boundaries of data protection. Coalfire, Optiv, BlackHills, Direct Defense as well as others all participate in this program.

Red/Blue/Purple Teams

Once a year, we bring two teams, one offensive, and one working with the defensive team to truly wring out the environment. The mandate is simple – get in, however you can. This provides objectivity and assurance that patient data is protected.

Techniques can be as traditional as using fingerprinting and vulnerability assessment tools, or more esoteric techniques such Bluetooth hacking via drones outside a building.

This is a complex, invasive and expensive exercise; but the old maxim of "the more you sweat in peace, the less you bleed in war" means that this investment of time and energy is worthwhile in ensuring that the protections are intact against the most aggressive threats.

Monitoring

Security Incident and Event Monitor

Medidata is a cloud provider, and we like to “practice what we preach”. Where practical, we use cloud services to support the environment, and a key service is SUMOLogic, a system which is tied to every processing and network device in the organization. Subsuming over 3 billion security events a month, SUMOLogic processes each activity, login, logout, failed password attempt, API calls and many others to look for attempts to gain or deny access to the environment.

Managed Security Service Provider

Leveraging SUMOLogic, our third-party Managed Security Service Provider “Smartronix “provides 24-hour, 365 day a year monitoring of our systems, and is empowered to disable any external threat, while escalating internally for prompt notification. Using threat intelligence provided by a number of external services, they are proactive in blocking the problems, before they become problems.

Smartronix, a Department of Defense support organization provides around the clock monitoring of all 20,000+ systems in the Medidata universe. With Security Operations Centers around the world, complete global coverage and around the clock response ensures proper support. This service is also supported by an additional in-house Network and Security operations center which manages the internal aspect of our NIST 800-53 compliant Incident Response program.

Real-time Configuration Management

Medidata uses Amazon Trusted Advisor in order to provide best practice to the AWS configuration. In order to enhance that, Medidata leverages Palo Alto Prismacloud, formerly known as Redlock. Prismacloud provides real-time measurement to standards such as NIST 800-53, FedRamp, PCI DSS, HIPAA and other baselines. This allows for assurance that the configuration and management of the hosted systems are properly managed, and as secure as they possibly can be.

Independent Testing and Review

Security is only as good as an objective observer says it is. So, in addition our customer and regulator assessments, we use multiple independent entities which we regularly rotate, to prevent complacency and ensure we bring objectivity, cutting edge techniques and emergent technologies to bear in order to ensure that the intellectual property of our customers and their patients are properly protected.

SOC-1

Medidata published its first SOC1 Type 1 report for our "Medidata Payments" application in 2017, and the first Type 2 in 2018. SOC-1 Type 2 reports are examination engagements performed by a service auditor (CPA) in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, *Reporting on Controls at a Service Organization,* to report on the suitability of the design of the controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements.

SOC-2+

Medidata publishes a Service Organization Controls 2 (SOC 2) report. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 2 report attests that Medidata data center control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. Our commitment to the SOC 2 report is ongoing, and we plan to continue our process of periodic audits.

In addition, Medidata obtains the SOC2_ with both the information security and privacy trust principles, reinforcing the governance program with a homogenous set of controls around quality, privacy and information security.

PCI DSS Service Provider

The Payment Card Industry Data Security Standard (PCI/DSS) was created to standardize controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually by our trained and certified Internal Security Assessor (ISA). We also apply it to any financial processing related information that is used as part of our Payments offering.

ISO/IEC 27001:2013

ISO 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely recognized international security standard in which Medidata clients showed significant interest.

Certification in the standard requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet our information security needs on an ongoing basis

The key to certification under this standard is the effective management of a rigorous security program. The Information Security Management System (ISMS) required under this standard defines how we continually manage security in a holistic, comprehensive way. The ISO 27001:2013 certification is specifically focused on the Medidata ISMS and measures how our internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms we are operating in alignment with the comprehensive ISO 27001:2013 certification standard.

ISO/IEC 27018:2019

ISO/IEC 27018:2018 is a security management standard that specifies security management best practices and comprehensive security controls in the context of Privacy Information in a cloud environment. This is a widely recognized international security standard in which Medidata clients also show significant interest.

This standard complements ISO/IEC 27001:2013 and other security frameworks in order to maintain effective management of a privacy related information. Like ISO/IEC 27001:2013, ISO/IEC 27018:2014 certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms we are operating in alignment with the comprehensive ISO 27018:2014 certification standard.

ISO/IEC 27701:2019

ISO/IEC 27701:2019 is a privacy extension for an existing Information Security Management System; including the adoption of a Privacy Information Management Systems (PIMS). This is a widely recognized international security standard which is as close to a GDPR certification that can be currently obtained.

These standard complements ISO/IEC 27001:2013 and other security frameworks in order to maintain effective management of a privacy related information. Like ISO/IEC 27001:2013, ISO/IEC 27701:2019 certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms we are operating in alignment with the comprehensive ISO 27701:2019 certification standard.

FISMA

Medidata enables U.S. government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). FISMA requires federal agencies to develop, document, and implement an information security system for its data and infrastructure based on the NIST (National Institute of Standards and Technology Special Publication) 800-53, Revision 4 standard. FISMA requires Medidata to implement and operate an extensive set of security configurations and controls. This includes documenting the management, operational and technical processes used to secure the physical and virtual infrastructure, as well as the third-party audit of the established processes and controls. Medidata is evaluated every year to maintain our FISMA compliance for Software as a Service and has been awarded an Authority to Operate by a number of US Government agencies.

Privacy Shield

The EU-U.S. Privacy Shield imposes strong obligations on U.S. companies to protect Europeans' personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbor framework invalid. The Privacy Shield requires the U.S. to monitor and enforce more robustly and cooperate more with European Data Protection Authorities. It includes, for the first time, written commitments and assurance regarding access to data by public authorities.

What will it mean in practice?

- For Medidata Solutions
    - Self-certify annually that we meet the requirements.
    - Display a privacy policy on our website.
    - Reply promptly to any complaints.
    - (If handling human resources data) Cooperate and comply with European Data Protection Authorities.
- For European Clients of Medidata Solutions
    - More transparency about transfers of personal data to the U.S. and stronger protection of personal data.
    - Easier and cheaper redress possibilities in case of complaints —directly or with the help of your local Data Protection Authority.

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, Medidata Private Cloud VPN endpoints and TLS-terminating load balancers in Medidata (U.S.) operate using FIPS 140-2 validated algorithms. Operating in FIPS-140-2 compliance mode does require comparable capabilities at the user browser side of the connection. While we do not employ FIPS 140-2 certified hardware, we do use the comparable make and model with fully approved FIPS 140-2 software.

HIPAA

For our Commercial Imaging and Quantum products, Medidata enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure Medidata environment to process, maintain, and store protected health information.

We feel that the Medidata security practice is world-class, comprised of the best people, processes and technology. We take our responsibilities seriously and earn our customers and their patients trust each and every day.

We are proud of what we do and are happy to show it. So, in addition to this document, we post vulnerability summaries, penetration tests results, certifications, audits and other security related matters at https://www.medidata.com/trust so that our customers and their sites can have a level of comfort in that the protections are what the patient expects.

For any questions or clarifications, feel free to reach out to security@medidata.com.