StratusCore Inc. Internal Security Provisions

Version 2.1 (Abridged)

Table of Contents

Introduction

Organizations have looked to the cloud for cost savings, or to augment private data center capacity. However, organizations are now looking to the cloud primarily for security, realizing that providers can invest more in people and processes to deliver secure infrastructure.

Having built a hybrid cloud platform, StratusCore has invested in a deep understanding of the security implications of cloud computing. Our cloud services and infrastructure security follows the Federal Information Security Management Act (FISMA) and Federal Risk and Authorization Management Program (FedRAMP) to deliver better security than many traditional solutions. We make security a priority to protect our own operations, and because StratusCore runs on the same infrastructure that we make available to our customers, your organization can directly benefit from these protections.

Security is a strategic focus at StratusCore. Protection of data is among our primary design criteria. Security drives our organizational structure, training priorities and hiring processes. It shapes our data centers and the technology they house. It's central to our everyday operations and disaster planning, including how we address threats. It's prioritized in the way we handle customer data. And it's the cornerstone of our account controls, our compliance audits and the certifications we offer our customers.

This paper outlines StratusCore's approach to security and compliance for the StratusCore platform, our suite of public-cloud products and services. Our platform includes offerings in compute, 3D-accelerated virtual workstations, transfer, storage, networking and big data.

This white paper reviews the organizational and technical controls StratusCore has built to protect your content while using StratusCore's suite of content creation services. Details on compliance and how you can meet regulatory requirements are covered in the appendix.

StratusCore Security Culture

StratusCore has created a vibrant and inclusive security culture for all its employees. The influence of this culture is apparent during the hiring process, employee on-boarding, and ongoing training. Our security culture is highly visible in company-wide events, where we work to reinforce awareness.

Employee background checks

Before hiring a new staff member, StratusCore will verify the individual's education and previous employment, and perform internal and external reference checks. Where local labor law or statutory regulations permit, StratusCore may also conduct criminal, credit, immigration, and security checks. The extent of these background checks is dependent on the desired position.

Employee security training

All StratusCore employees undergo security training as part of the orientation process. All staff also receive ongoing security training throughout their StratusCore careers. During orientation, new employees agree to our Code of Conduct, which highlights our commitment to keep customer information safe and secure. Depending on the employee's job role, she or he may be required to receive additional training on specific aspects of security .

Our security team

StratusCore employs a team of security and privacy professionals. These experts are part of our software engineering and operations division. This team is tasked with maintaining the company's defense systems, developing security-review processes, building security infrastructure and implementing StratusCore's security policies. StratusCore's dedicated security team actively scans for security threats using commercial and custom tools, penetration tests, quality assurance (QA) measures and software security reviews.

Our privacy team

The StratusCore privacy team operates separately from the product development and security organizations. It participates in every StratusCore product launch by reviewing design documentation and performing code reviews to ensure that privacy requirements are followed.

Internal audit and compliance specialists

StratusCore has an internal audit team that reviews compliance with security laws and regulations. As new auditing standards are created, the internal audit team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties.

Operational Security

Operational security is an integral part of StratusCore's infrastructure.

Vulnerability management

StratusCore administrates a vulnerability management process that actively scans for security threats using a combination of commercially available and purpose-built in-house tools; intensive automated and manual penetration efforts; quality assurance processes; software security reviews; and external audits. The vulnerability management team is responsible for tracking and following up on vulnerabilities.

Malware prevention

An effective malware attack can lead to account compromise, data theft, and possibly additional access to a network. StratusCore takes these threats to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware.

Monitoring

StratusCore's security monitoring program is focused on information gathered from internal network traffic, employee actions on systems and outside knowledge of vulnerabilities. At many points across our global network, internal traffic is inspected for suspicious behavior, such as the presence of traffic that might indicate bot-net connections.

Automated network analysis helps determine when an unknown threat may exist. Threats are escalated to StratusCore security staff. Network analysis is supplemented by automated analysis of system logs. StratusCore makes use of multiple anti-virus engines, servers and workstations to help identify malware that may be missed by anti-virus signatures.

Incident management

We have a rigorous incident management process for any security event that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action; and procedures for notification, escalation, mitigation, and documentation. StratusCore's security incident management program is structured around the NIST guidance on handling incidents (NIST SP 800–61).

In preparation for an event, key staff are trained in forensics and handling evidence, including the use of third-party and proprietary tools. Testing of incident response plans is performed for key areas, such as systems that store sensitive customer information. These tests take into consideration a variety of scenarios, including insider threats and software vulnerabilities.

Security and Technology Core

StratusCore's platform runs on a technology infrastructure that is conceived, designed and built to operate securely. StratusCore is an innovator in hardware, software, network and system management technologies. We custom-designed our servers, virtual images, proprietary operating system, and geographically distributed data centers. Using the principles of "defense in depth," we've created an IT infrastructure that is more secure and easier to manage than more traditional technologies.

Data centers

StratusCore's focus on security and protection of data is among our primary design criteria. Physical security at StratusCore data centers features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, and strong authentication. Data center floors feature laser-beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders.

Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of StratusCore's employees will ever set foot in one of our data centers.

Powering our data centers

To keep things running 24/7 and ensure uninterrupted services, StratusCore's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel-engine backup generators can provide enough emergency electrical power to run each data center at full capacity.

Cooling systems maintain a constant operating temperature for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment help prevent damage to hardware. Heat, fire, and smoke detectors trigger audible and visible alarms in the affected zone, at security operations consoles, and at remote monitoring desks.

Custom server images and software

Our production servers run a custom-designed operating system (OS) based on a stripped-down Linux version that has been hardened using the Security Technical Implementation Guide (STIG). StratusCore's servers and our server OS are designed for the sole purpose of providing StratusCore services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on customer demand.

This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications. If a modification is found that differs from the standard StratusCore image, the system is automatically returned to its official state. These automated, self-healing mechanisms are designed to enable StratusCore to monitor and remediate destabilizing events, receive notifications about incidents, and slow down potential compromise on the network.

Hardware tracking and disposal

StratusCore meticulously tracks the location and status of all equipment within our data centers from acquisition to installation to retirement to destruction. Bar codes and asset tags facilitate asset management. StratusCore has implemented video surveillance to help make sure no equipment leaves the data center floor without authorization. If a component fails to pass a performance test at any point during its life-cycle, it is removed from inventory and retired. StratusCore hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect content at rest.

When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no content in accordance with DoD 5520.22-m (7-pass).

Global Network

StratusCore's IP data network consists of diverse transport mediums. This allows us to deliver highly available and low-latency services across the globe.

In other cloud services and on-premises solutions, customer content must make several journeys between devices, known as "hops," across the public Internet. The number of hops depends on the distance between the customer's ISP and the solution's data center. Each additional hop introduces a new opportunity for content to be attacked or intercepted. In contrast, because it's linked to most ISPs in the world, StratusCore's global network offers materially enhanced security of content in transit by limiting hops across the public Internet.

"Defense in depth" describes the multiple layers of defense that protect StratusCore's network from external attacks. Only authorized services and protocols that meet our security requirements can traverse this defense structure; anything else is automatically dropped. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation.

Securing content in transit

Content is most vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing content in transit is a high priority for StratusCore. Content traveling between a customer's device and StratusCore is encrypted using HTTPS/TLS (Transport Layer Security).

StratusCore has also upgraded all our RSA certificates to at least 4096-bit keys, making our encryption in transit for platform and all other StratusCore services even stronger. Perfect forward secrecy (PFS) minimizes the impact of a compromised key, or a cryptographic breakthrough.

A low-latency, highly available solution

StratusCore designs the components of our platform to be highly redundant. This redundancy applies to our server design, how we store data, network and Internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design. This approach creates a solution that is not dependent on a single server, data center, or network connection. StratusCore's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages.

Service availability

Some of StratusCore's services may not be available in some jurisdictions. Often these interruptions are temporary due to network outages, but others are permanent due to government-mandated blocks.

Data Usage

Our philosophy

Our data-usage philosophy is simple: platform customers own their content, not StratusCore. The content that customers put into our systems is theirs. We do not scan it for advertisements nor sell it to third parties. We offer our customers a detailed data processing amendment that describes our commitment to protecting customer data. It states that StratusCore will not process data for any purpose other than to fulfill our contractual obligations.

Furthermore, if customers delete their data, we commit to deleting it from our systems within seven days. Finally, we provide tools that make it easy for customers to take their data with them if they choose to stop using our services, without penalty or additional cost imposed by StratusCore.

Access Control

Administrative access

To keep content private and secure, StratusCore logically isolates each customer's platform content from that of other customers and users, even when it's stored on the same physical server. Only a small group of StratusCore employees have access to customer content. For StratusCore employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. StratusCore employees are only granted a limited set of default permissions to access company resources, such as employee email and StratusCore's internal employee portal.

An employee's authorization settings are used to control access to all resources, including data and systems for platform products. Support services are only provided to authorized customer administrators whose identities have been verified in several ways. StratusCore access is monitored and audited by our dedicated security, privacy, and internal audit teams.

Delegated customer administrators

Within customer facilities and partner networks, administrative roles and privileges for StratusCore platform are configured and controlled by the owner. This means that individual team members can manage certain services or perform specific administrative functions without gaining access to all settings and data.

Law enforcement data requests

The customer, as the data owner, is primarily responsible for responding to law enforcement data requests. However, like other technology and communications companies, StratusCore may receive direct requests from governments and courts around the world about how a person has used the company's services. We take measures to protect customers' privacy and limit excessive requests while also meeting our legal obligations.

Respect for the privacy and security of content you store with StratusCore remains our priority as we comply with these legal requests. When we receive such a request, our team reviews the request to make sure it satisfies legal requirements and StratusCore's policies. Generally speaking, before we comply, the request must be made in writing, signed by an authorized official of the requesting agency and issued under an appropriate law.

If we believe a request is overly broad, we'll seek to narrow it, and we push back often and when necessary. We believe the public deserves to know the full extent to which governments request user information from StratusCore. It is StratusCore's policy to notify customers about requests for their data unless specifically prohibited by law or court order.

Third-party suppliers and vendors

StratusCore directly conducts virtually all content-processing activities to provide our services. However, StratusCore may engage some third-party suppliers and vendors to provide services related to our platform, including customer and technical support.

Prior to on-boarding third-party suppliers and vendors, StratusCore assesses the security and privacy practices of third-party entities. These reviews ensure that suppliers and vendors provide a level of

security and privacy appropriate to their access to data and the scope of the services they are engaged to provide.

Once StratusCore has assessed the risks presented by the third-party entity, we require the supplier or vendor to contractually commit to appropriate security, confidentiality, and privacy terms.

Conclusion

The protection of customer content is a primary design consideration for all StratusCore's infrastructure, products and personnel operations. We believe that StratusCore can offer a level of protection that very few public-cloud providers or private-enterprise IT teams can match. Because protecting content is core to StratusCore's business, we can make extensive investments in security, resources and expertise at a scale that others cannot.

Content protection is more than just security. StratusCore's strong contractual commitments make sure you maintain control over your content and how it is processed. Customers have absolute assurance that their content is never used for advertising or any purpose other than to deliver platform services.

Looking toward the future is as important as reviewing existing investments in architecture, resources and training. StratusCore will continue to invest in our platform to allow you to benefit from our services in a secure and transparent manner.

Appendix

Applicable Regulations

StratusCore aligns to the following regulations:

- Computer Fraud and Abuse Act
  [PL 99-474, 18 USC 1030]
- E-Authentication Guidance for Federal Agencies
  [OMB M-04-04]
- Federal Information Security Management Act (FISMA) of 2002
  [Title III, PL 107-347]
- Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
  [OMB M-01-05]
- Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection
  [HSPD-7]
- Internal Control Systems
  [OMB Circular A-123]
- Management of Federal Information Resources
  [OMB Circular A-130]
- Management's Responsibility for Internal Control
  [OMB Circular A-123, Revised 12/21/2004]
- Protection of Sensitive Agency Information
  [OMB M-06-16]
- Security of Federal Automated Information Systems
  [OMB Circular A-130, Appendix III]

Applicable Standards and Guidance

StratusCore aligns to the following standards and guidance as prescribed by FedRAMP:

- A NIST Definition of Cloud Computing
  [NIST SP 800-145]
- Computer Security Incident Handling Guide
  [NIST SP 800—61, Revision 1]
- Contingency Planning Guide for Federal Information Systems
  [NIST SP 800-34, Revision 1]
- Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
  [NIST SP 800-27, Revision A]
- Guide for Assessing the Security Controls in Federal Information Systems
  [NIST SP 800-53A]
- Guide for Developing Security Plans for Federal Information Systems
  [NIST SP 800-18, Revision 1]
- Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  [NIST SP 800-37, Revision 1]
- Guide for Mapping Types of Information and Information Systems to Security Categories [NISP SP 800-60, Revision 1]

- Guide for Security-Focused Configuration Management of Information Systems
  [NIST SP 800-128]
- Information Security Continuous Monitoring for Federal Information Systems and Organizations
  [NIST SP 800-137]
- Managing Information Security Risk
  [NIST SP 800-39]
- Minimum Security Requirements for Federal Information and Information Systems
  [FIPS Publication 200]
- Personal Identity Verification (PIV) of Federal Employees and Contractors
  [FIPS Publication 201-1]
- Recommended Security Controls for Federal Information Systems
  [NIST SP 800-53, Revision 4]
- Risk Management Guide for Information Technology Systems
  [NIST SP 800-30, Revision 1]
- Security Considerations in the System Development Life Cycle
  [NIST SP 800-64, Revision 2]
- Security Requirements for Cryptographic Modules
  [FIPS Publication 140-2]
- Advanced Encryption Standard
  [FIPS Publication 197]
- Standards for Security Categorization of Federal Information and Information Systems [FIPS Publication 199]
- Technical Guide to Information Security Testing and Assessment
  [NIST SP 800-115]