virtustream

Whitepaper

Virtustream: Choosing a Cloud Provider for Mission-Critical Applications is All About Trust

Organizations that want to modernize their businesses have learned it's a tough road to go alone. The transformational journey generally requires a move to cloud, which often includes migrating your core mission-critical systems. These core systems – manufacturing systems, ecommerce systems, ERP systems – drive your business and manage critical data.

These are not simple applications, and migrating them to a cloud environment is not to be taken lightly. These applications demand high, consistent, and assured performance protected by committed service levels, robust security, and an increasingly complex set of compliance requirements. Enterprise customers understand the risk associated with these applications, and need to work with providers that can earn their trust to advance their transformation programs.

Virtustream cloud operations, migration and management services, security and compliance programs, data privacy practices, and service quality are all designed to sustain the trust that has been built with leading organizations around the world.

This white paper will cover the five (5) tenets of Virtustream trust, including security, compliance, privacy, transparency, and service quality.

Security

Virtustream's security foundation is built on the CIA Triad model, protecting the Confidentiality, Integrity, and Availability of its assets. Virtustream's top-down approach, starting from the senior executive leadership, entails in-depth, extensive due diligence in all aspects of our defense-in-depth security posture. Virtustream's people, processes, and technologies strive for trust, transparency, dependability, scalability, accountability, auditability, innovation, and automation. This paradigm includes routers, firewalls, vulnerability scanners, intrusion detection, internal and external audits, risk management, governance, least privilege and need-to-know principles, identity and access management, extensive vetted and background checked technical personnel, comprehensive change management and incident response plans, firewall policy reviews, file integrity monitoring, audit log correlation and review, as well as mandatory security awareness training for all employees.

Virtustream's IAAS cloud services employ industry-leading security capabilities to ensure perimeter defense, network security, host security, system hardening, tenant isolation, secure development lifecycle, data privacy, and data protection while enforcing strict administrative, physical, and technical controls.

Key areas addressed by Virtustream security capabilities include:

Responsibility Model

Security is a shared responsibility between Virtustream and the customer. Virtustream's shared responsibility model clearly articulates which controls Virtustream implements and which controls a customer must implement to achieve compliance.

Virtustream Responsibility - Security of the Cloud

Virtustream is responsible for the security and protection of the infrastructure that runs all Virtustream cloud services. This infrastructure is composed of the hardware, software, operating system, networking, and facilities, and can include databases for certain applications. In a traditional cloud model, the customer remains responsible for the applications, user access, and databases. With Virtustream Managed Services, customers can opt to simplify operations further and shift security for the operating system and databases to Virtustream.

Virtustream Managed Security Services

For a truly enterprise-class experience, Virtustream can augment an organization's cloud services with Virtustream managed security services.

Some of the fully managed security services available at the virtual machine (VM) and network level include:

- Anti-Virus/Anti-Malware: Detects and blocks viruses, trojans, spyware, and other malicious activity
- Host-based Intrusion Detection System (hIDS) and Firewall (hFW): A bi-directional layer 4 stateful firewall along with a sophisticated IDS engine can prevent, detect, and block malicious traffic and behaviors such as reconnaissance scanning, denial of service attacks, or SMB exploits
- Network-based Intrusion Detection System: Detects network-level threats against hosted assets such as attacks that seek to take advantage of network vulnerabilities and unpatched systems using both vendor-supplied threat signatures and a behavioral baseline to assess unknown threats based on atypical network behavior and anomalies
- File Integrity Monitoring (FIM): Detects changes to registry values, registry keys, services, processes, installed software, ports, and files
- Transparent Data Encryption (TDE; data at rest): Provides encryption key build and management, along with data access policy management for the directory that houses the data portion of a database (e.g. SAP) in a tenant environment
- Vulnerability Scanning: Scans customer systems for vulnerabilities in their operating systems to produce a recurring vulnerability report. This report can be provided to either the customer or the Virtustream Application Managed Services (AMS) team. The report can then be used to schedule maintenance windows and system patches to ensure that the systems are kept up to date.

Customer Responsibility - Security in the Cloud

The customer is responsible for application updates and patches, including those for security, identity and access management, and network security.

Host and Network Security

Host and network security is important in IT operations, including when migrating mission-critical applications to the cloud. Virtustream offers a comprehensive set of host and network level security options that help protect data. Customer segregation is provided through Virtustream's isolation model, implemented for each customer. These customers are logically separated with Virtual Routing and Forwarding (VRF) and Virtual LANs (VLANs).

To access the cloud, Virtustream offers public networking, private networking, or a combination of both. Whether an IPSEC VPN tunnel mode or an MPLS direct connection, the entry point will be a virtual firewall which gives full control over IP address space and eliminates the potential for overlap with other tenants. Customers can utilize as many dedicated VLANs and IP address ranges as desired. Firewall rules can be defined on a VM-by-VM basis that Virtustream applies at the hypervisor level.

There is a great deal of granular control over how traffic gets routed within a virtual private cloud in the Virtustream data center. Virtustream's security services offer a variety of security tools available at either the perimeter or host-level. These options include perimeter firewall, host and network intrusion detection systems (IDS), host-level anti-virus/anti-malware, vulnerability scanning, file integrity monitoring, and first-response remediation services. Customers work with Virtustream professional services during the onboarding process to customize their general security, and can select additional Virtustream network managed security services options during onboarding or anytime afterwards.

Data Protection

Virtustream views data protection as a critical capability to ensure the data integrity, resiliency, and availability required for an organization's most important business applications and data in the Virtustream cloud.

Data Encryption

To help ensure data integrity, Virtustream employs encryption technologies in the cloud environment. As a result, data is secure at rest, in archive, and in transactional databases. In keeping with Virtustream's core competency in mission-critical applications, Virtustream offers an add-on encryption option with SAP to encrypt HANA workloads without negatively affecting the performance of the HANA databases.

Disaster Recovery

For high availability workloads, Virtustream provides embedded disaster recovery (DR) through the replication of data at geographically-dispersed data centers, with industry-leading recovery-point objective (RPO) and recovery-time objective (RTO) capabilities guaranteed through service-level agreements (SLAs). Data backup and recovery options are also available for those customers who do not require full disaster recovery capabilities.

Virtustream offers disaster recovery protection as well as data backup and recovery solutions with uptime SLAs from the IaaS layer up to the operating system, database, and SAP Basis level. In contrast, most public cloud services do not provide disaster recovery or data backup and recovery solutions as a standard component in their cloud services. This requires customers to either design, implement, and test the disaster recovery and data backup solutions themselves or hire a third-party contractor to do it.

Configuration, Hardening, and Vulnerability Management

Virtustream focuses on a number of key areas to ensure systems are secure, including consistency in infrastructure configurations, enhancements to meet industry and regulatory needs, and proactive measures to identify and remediate vulnerabilities. Many of the capabilities in these areas come standard with Virtustream cloud services, while other capabilities are offered as managed services to address specific customer needs.

Configuration

Ensuring consistency in system configurations is imperative to the integrity of Virtustream cloud services. Virtustream systems are continuously tested and audited, including by independent third parties, to verify they are secure.

Hardening

Virtustream hardens systems to meet industry-standard best practices, as well as various government standards defined by compliances, attestations, frameworks, and laws. System audits are completed regularly to ensure the infrastructure remains hardened per applicable guidance. Virtustream also works with customers to test and evaluate hardening practices, as well as providing them with artifacts, such as third-party audit reports, on-demand.

Vulnerability Management

Vulnerability management is vital to any security program. Virtustream has a number of experts across multiple departments responsible for identifying risks within the Virtustream cloud. In addition, vulnerability scanning is available for purchase as a managed service in a customer's network. Virtustream's diverse team of security analysts have experience across various government agencies, as well as major corporations.

Identity Management and Access Control

Virtustream believes identity management and strong access controls are critical to preserving the integrity of Virtustream cloud services for customers.

Identity Management

Virtustream Enterprise Cloud utilizes strong two-factor authentication as a standard authentication process for users to access the management portal. Users are authenticated via a user-selected PIN and a one-time password generated via software or a hardware token. This provides a high degree of confidence that access to the Virtustream management console is restricted to only authorized users whose identity has been verified. Virtustream supports software tokens on diverse platforms including iOS, Android, and desktop systems, and Virtustream's management portal console is secured with https.

Access Control

Access to Virtustream cloud services is controlled through a combination of user roles and firewall rules based on IP addresses. Role-based access control (RBAC) provides a way to give different types of users access only to the resources they need to perform their work. Default roles include Read Only, Resource Creator, System Administrator, Tenant Administrator, and User. Each role contains a set of default permissions. Only a few steps are required to create new roles to customize permissions that align with an organization's inner workings. For auditing purposes, all privileged users are monitoring and logged 24x7x365.

Additionally, the Virtustream xStream Cloud Management self-service portal lets customers designate specific source IP addresses that can access the enterprise-cloud portal. This effectively limits the IP addresses from which users can log into their xStream portal, further increasing security and reducing the chance of unauthorized access to the cloud.

Security Logging and Monitoring

Virtustream understands that security is of the utmost importance to enterprises and government organizations. Virtustream gathers and monitors security logs to ensure that threats to systems and data remain just that, threats, and don't become incidents.

The Virtustream Security Intelligence Operations Center (SIOC) uses centralized logging and security information and event management systems (SIEM). SIOC analysts monitor alerts, researchers investigate industry trends and threat intelligence, and tooling experts build alerting based on continuous monitoring and threat categorization. Virtustream also takes proactive action for those customers who have contracted with Virtustream to monitor their Virtustream hosted infrastructure. In keeping with best practices, Virtustream maintains logs in its centralized logging system for at least one year to comply with PCI DSS requirements.

For customers that have purchased the Virtustream "Log Management" managed service, Virtustream support staff will proactively monitor security threats which arise in an organization's environment hosted on the Virtustream cloud in real-time. The Virtustream SIOC has 24x7x365 on-call support and the tools needed to provide a comprehensive security and compliance posture via an extensive suite of reports.

Customers that use Virtustream Application Managed Services can leverage Virtustream to help create artifacts for audit, compliance, and continuous monitoring purposes. For reports, Virtustream can also design multiple common control profiles (CCPs).

Security Development Lifecycle (SDL)

At Virtustream, security has always been a top priority because Virtustream cloud services are purpose-built for mission-critical workloads. Virtustream employs a security development lifecycle (SDL) process to reduce the number of vulnerabilities and provide a highly trusted cloud platform. SDL is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost at every stage. As the threat landscape changes, Virtustream's SDL changes to keep pace with increased technological and attacker sophistication.

Policy, Governance, and Risk

Virtustream policy, governance, and risk practices encompass several critical areas of cloud service.

Information Security

Virtustream has implemented an Information Security Management System (ISMS) policy that is certified to the ISO 27001:2013 standard. Additionally, information security is delivered in the form of third-party auditing and certifications for rigorous international industry standards. Virtustream cloud services are certified to ISO 9001 for quality, ISO 22301 for business continuity, and ISO 27001 for information security, as well as ISO 27017 for cloud services security and ISO 27018 for protection of personally identifiable information (PII). In addition, Virtustream's cloud services are audited for attestations to SOC 1, SOC 2, SOC 3, and HIPAA/HITECH/HITRUST, and are certified to PCI DSS and CSA STAR. The public sector Virtustream Federal Cloud is certified to FedRAMP Moderate.*

**Note - Not all services have all certifications. Please contact Virtustream for more details.*

Business Continuity

The Virtustream Governance, Risk, and Compliance (GRC) team is dedicated to ensuring all functions that support Virtustream cloud services adhere to the policies and procedures established by executive management and meet the control requirements of the standards.

Throughout the year, the GRC team conducts internal audits, risk assessments, business impact analysis, tests business continuity plans, and reviews findings with senior management to continually improve the management system that governs Virtustream operations.

Risk

Virtustream follows the ISO 27001, FedRAMP, and other standards for risk assessment, risk treatment, and risk reporting. Risks that are identified throughout the IaaS during an assessment, audit, or vulnerability assessment are identified, tracked, and then either mitigated or remediated. Remediation of vulnerabilities within the IaaS management zone are addressed according to the PCI DSS standard.

Compliance

Virtustream is dedicated to providing the highest levels of compliance. A rigorous approach to information security management is core to the way Virtustream manages its facilities and operations. Cloud-delivered systems must be compliant with both regulatory standards (which encompasses global, regional, and industry-specific regulations) as well as obligations specified in service agreements. That's why all Virtustream services have the appropriate certifications and attestations, in addition to all technical data center personnel being government security cleared.

Privacy

Virtustream respects the privacy of its customers and is committed to protecting the personal information that customers share. The Virtustream Privacy Statement describes how information is collected, used, and disclosed from what is obtained from visitors to the Virtustream website, www.virtustream.com, and the services available through the website. The Privacy Statement describes practices that reflect Virtustream's activity as a data controller, including, but not limited to, how these practices impact European Union data protection rights like those set forth in the General Data Protection Regulation (GDPR), how visitors can access their personal information, and their choices about how Virtustream uses their personal information.

Transparency

Virtustream believes in transparency in communications to give customers confidence in its abilities and to gain and sustain customer trust. Virtustream provides organizations with visibility into its cloud practices to provide customers with a clear understanding about how customer data is handled, including how it is processed, stored, and secured and who has permissions to access it. Additionally, Virtustream makes proof available to provide evidence of claims and a forum for the sharing of information among peers and Virtustream leadership. As important, Virtustream abides by the Dell Technologies Code of Conduct, which provides the guiding principles for its culture and values.

Virtustream cloud services certifications, attestations, frameworks, standards, and laws addressed include:

Certifications/Attestations	Laws/Privacy/Regulations	Frameworks/Standards
• CJIS • CISPE • Dod SRG • FedRAMP • ISO 27001 • ISO 22301 • ISO 9001 • PCI DSS • SOC 1, Type 2 • SOC 2, Type 2 • SOC 3 • ASD (IRAP)	• HIPAA • HITECH • CUI • ITAR • EAR • GLBA • FISMA • GxP	• FIPS • DISA STIG • ISO 27000 • NIST 800-53 • NIST 800-171

Audit Reports

Virtustream cloud services meet many regional, global, and industry-specific requirements. Compliance and attestation audit reports completed by an authorized third-party certified public accounting (CPA) firm or assessment organization (3PAO) are available to customers upon request. Virtustream makes these reports available to substantiate and give evidence to its claims.

Customer Advisory Board

The Virtustream Customer Advisory Board (CAB) was established to provide senior leaders from customers and Virtustream an opportunity to participate in an open exchange of information. The CAB is intended to generate feedback and direction for Virtustream about how customers currently use and would like to use Virtustream's cloud services, and what enhancements customers would like to see to help enable greater business benefits and outcomes.

Code of Conduct

Virtustream adheres to a code of conduct followed by the entire Dell Technologies family of businesses. It's a shared belief that it's the culture and values that differentiates the Dell Technologies family of businesses in the marketplace just as much as the products, services, and innovations.

Service Quality

For organizations deploying mission-critical applications in the cloud, trust is not just about security and compliance. Trust involves the quality of service that Virtustream cloud services offer, including guaranteed availability levels, consistent high performance, reliability, professional and managed services, and unmatched customer service.

High Availability and Resiliency

Mission-critical applications should be available anywhere and anytime. Virtustream cloud services provide enterprise-class availability backed by service-level agreements (SLAs) that extend beyond the infrastructure layer.

Virtustream Enterprise Cloud provides up to 99.999% (five nines) availability at the IaaS layer and up to 99.9% (three nines) availability at the operating system, database, and Basis layer for certain production systems such as SAP. Because both Virtustream and Dell EMC are Dell Technologies businesses, customers get single-source support for Dell EMC storage and data protection. Hyper-scale cloud providers only guarantee 99.99% (four nines) availability at the IaaS layer and have no single-source support option when used with Dell EMC solutions.

Reliability

Embedded disaster recovery comes standard with Virtustream cloud services, which replicates compute and storage between primary and secondary geographically dispersed data centers.

Performance Assurance

Virtustream provides performance assurance for application response times backed by service-levels for Tier 1 storage response times as low as 1000 milliseconds (ms). The Virtustream patented MicroVM (μVM) resource allocation model guarantees required CPU, memory, storage, and network bandwidth. Proactive network, compute, memory, and storage optimizations always ensure right sizing of resources for applications.

Professional Services

Virtustream offers cloud planning, onboarding, and migration services to speed time to value when moving mission-critical applications to cloud. Virtustream Advisor provides an assessment of the enterprise application landscape, identifying all workloads and analyzing system configurations for optimum set up in the Virtustream cloud. Hyper-scale cloud providers do not offer advisory services; enterprise IT either has to do it themselves or outsource it to a third party.

Additionally, Virtustream onboarding and migration services reduce the risk for enterprises and minimize disruption in enterprise IT service. Virtustream takes responsibility for project planning, project management, documentation of all applications and workloads, move sequences, tests, mock cutover, and final cutover plan. Once system migration is initiated, data and application consistency is checked.

Once systems go live on Virtustream Enterprise Cloud, steady-state must be reached before handover to Virtustream Managed Services. Hyper-scale cloud providers do not offer onboarding and migration services; enterprise IT either has to do it themselves or outsource it to a third party.

Managed Services

With the move to cloud complete, Virtustream Managed Services provides a fully-managed white glove cloud service from the IaaS layer up to the operating system, database, and Basis layer, with proactive incident-event management, monitoring, alerts, troubleshooting, and other pre-scoped managed services round-the-cloud (24x7x365). Hyper-scale cloud providers don't offer any managed services; as part of separate engagement, enterprises have to select fragmented managed services through hyper-scalers' partner network.

Contact

For more information about Virtustream, please contact us at info@virtustream.com or visit us at www.virtustream.com. To learn more about the five tenets of Virtustream Trust, please visit our Trust Center.

About Virtustream

Virtustream, a Dell Technologies Business, is the enterprise-class cloud service and software provider trusted by enterprises worldwide to migrate and run their mission-critical applications in the cloud. For enterprises, service providers and government agencies, Virtustream's xStream® Management Platform and Infrastructure-as-a-Service (IaaS) meets the security, compliance, performance, efficiency and consumption-based billing requirements of complex production applications in the cloud - whether private, public or hybrid.

