virtustream
A Dell Technologies Business

WHITE PAPER
VIRTUSTREAM ENTERPRISE CLOUD

Combatting Ransomware: Cloud Data Security, Backup and Restoration

Virtustream incorporates multiple layers of security controls in our enterprise cloud infrastructure to protect your data from ransomware attacks. In addition to protecting the infrastructure, combatting ransomware requires secure and reliable backup and restore capabilities for your business-critical workloads that are inaccessible to a malicious attacker.

Ransomware is a top concern for organizations, with the growing frequency and sophistication of attacks and debilitating effects on businesses. One of the most serious outcomes occurs when ransomware encrypts all assets, propagating across systems through lateral movement to backup software and storage targets. If backup data is impacted, recovery from a ransomware attack becomes even more challenging.

This white paper details the backup procedures for each tenant within the Virtustream Enterprise Cloud as well as information about internal management access to each backup network.

Virtustream Enterprise Cloud Architecture

Virtustream Enterprise Cloud architecture has security controls in place to deter ransomware and other cyberthreats. Our backup infrastructure layers consist of the internal backup network where firewalls, backup application servers and data storage systems reside. Communication within the backup network is over an RFC-6598 Layer 2 data link to eliminate routing as well as provide a highly efficient isolated transport for backup data only.

The highly-restrictive control plane has firewall access controls toward the management of the environment. It also has firewall access controls towards the services infrastructure and ultimately into the backup system.

Separate independent internal backup networks reside within the customer network while being controlled and managed by the data protection operations team which has sole access to each environment. Each network resides behind individual firewalls allowing access for only specific functions that are uniquely related to backup.

The backup application server operating environment has tightly integrated resources to support the backup infrastructure, encompassing the enterprise-class backup application and deduplication backup data target appliance specifically designed for backups and isolation. The data protection advisor server offers enterprise monitoring, reporting and analytics tools which provide details around success and failure dashboards.

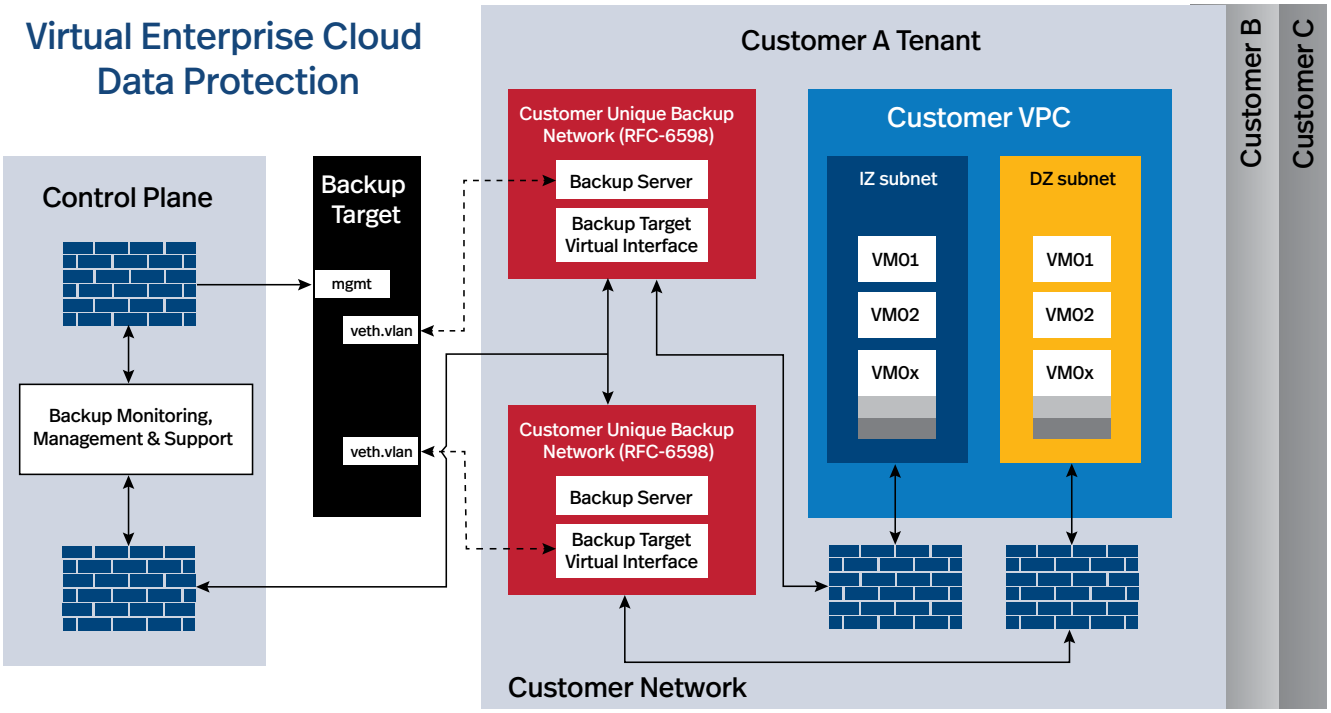

Figure 1: Virtustream Enterprise Cloud High-level Architecture

A VMware virtual machine (VM) emulates a physical server that resides in a shared hypervisor environment where power, CPU, RAM, disk and I/O are provided as resources that run as independent systems on an operating system (OS) of your choice. The customer environment includes the VMs and storage allotted to each customer in a multi-tenant cloud.

Trust Boundaries

Virtustream ensures the infrastructure that supports our managed services and customer environments is isolated to protect against attacks moving across cloud or customer locations. To achieve this separation, multiple trust boundaries between customer and Virtustream networks are established.

Network isolation through the implementation of firewalls reduces the attack surface by segregating computing assets in a networked environment to prevent lateral movement. Virtustream Enterprise Cloud infrastructure utilizes this strategy to isolate customer systems, backup servers and backup targets. Wherever possible, data flows are restricted to one-way communication from backup servers to source servers, also known as a pull model. This model limits the ability for a compromised system to reach backup servers.

In addition, each layer of the backup infrastructure uses different authentication realms to manage users and determine user identity. If a threat gains authentication credentials for one of the backup layers, it cannot use them to enter other layers. Access to a single authentication realm, such as Active Directory, will not compromise another layer of the infrastructure.

Once a user is authenticated, multiple levels of authorization are required to access the backup solution components. Secure, isolated storage of cryptographic customer controls ensure sensitive information such as encryption keys, access tokens and user credentials are not shared between customers or stored within the dedicated backup infrastructure outside the security controls of the backup application itself. If a customer is compromised, this setup keeps threats away from other Virtustream customers.

Non-routable, non-internet facing IP addresses are used to restrict communication to only computers on the same internal network. Moreover, attack tools are not commonly available for the proprietary protocols used by our networking and storage layers.

Secure Backup Infrastructure

Virtustream incorporates a tenant-specific backup network securely designed to isolate the backup infrastructure for each tenant residing within the enterprise cloud. Communication within the backup infrastructure is initiated from the backup application and only agent-to-agent, limiting the scope of activities the backup client can execute.

All backup resources reside behind an extra layer of security firewalls specific to each tenant's backup infrastructure, separating customer subnets and exposing only the required service ports. A customer subnet is an IPv4 network on which customer machines are deployed. Proprietary protocols and internal self-generating authentication certificates are used

throughout the backup infrastructure, adding additional protection to prevent malicious infiltration.

Communication originating from the backup infrastructure toward the Virtustream management infrastructure is restricted to very few ports and must be authenticated to complete transactions. Manual modifications to the backup storage filesystem require multiple user authentication, including validation from a Virtustream security officer.

Dedicated Backup Infrastructure for Each Tenant

Customer-specific backup infrastructure is isolated from the customer environment by a stateful firewall. The backup server OS is hardened and periodically tested for vulnerabilities. Any discovered vulnerabilities are mitigated on a regular basis either by applying released updates or implementing hot fixes.

The backup network is an RFC-6598 communication layer utilizing non-routable IP addressing that prevents outside security issues from impacting the backup assets. Logins and application-specific passwords are unique to every tenant and controlled by each tenant's application management team, therefore limiting exposure if another tenant's credentials are compromised. Periodic updates of tenant-specific application credentials are managed using secure lockbox integration as well as systematic controls to maintain changes.

Access to each customer's backup server from the Virtustream management infrastructure is accomplished with unique sets of rules for each component where communication is limited to a very small number of ports and accessible only by Virtustream-authorized personnel. Virtustream-authorized personnel must be authenticated and authorized using multi-factor authentication to reach a system with the capability to communicate with the backup servers.

Security Controls for Backup Layers

Virtustream backup layers have robust security controls, such as (but not limited to):

- Anti-virus/anti-malware
- Endpoint detection and response
- Host intrusion detection system (IDS) or intrusion protection system (IPS)
- Network IDS/IPS
- Vulnerability scanning
- Whitelist-only egress access through application-level controls

Penetration Testing

Virtustream performs penetration testing against the interfaces between customer systems and backup networks multiple times per year, to ensure they are safe from attacks. These tests occur at least every six months per PCI guidelines on segmentation. In addition, Virtustream uses external penetration testing vendors that specialize in the technology assessed at least annually. We rotate through penetration testing firms to gain new perspectives and apply different approaches when evaluating our interfaces to ensure broad protection from evolving threats.

Vulnerability Management Program

Virtustream maintains an aggressive vulnerability management program. Vulnerability scans against control plane and service management components are performed daily and critical vulnerabilities are communicated quickly for remediation. All vulnerabilities are reviewed and tracked weekly with the Virtustream executive leadership team.

External Audits

Infrastructure for the Virtustream Enterprise Cloud and managed services is audited by external firms and attested against industry-accepted best practices, including:

- SSAE18/SOC2
- PCI
- ISO 9001/27001
- HIPAA/HITECH

Virtustream Managed Security Services

For a truly enterprise-class experience, Virtustream can augment your cloud services with xStreamCare Services for Security and Compliance. These security services are available in two bundles: Essentials and Enhanced.

Essentials	Enhanced
Must have security for every cloud workload	Essentials plus additional security for sensitive and regulated cloud workloads
✓ Anti-virus/Anti-malware	✓ Essentials
✓ Host Intrusion Detection and Firewall	✓ Network Intrusion Detection
✓ Host Integrity Monitoring	✓ Firewall Policy Auditing
✓ Vulnerability Scanning	✓ Log Forwarding
✓ Log Management	✓ OS Hardening Scan
✓ Access to the Trust Platform	✓ Access to the Trust Platform

Table 1: xStreamCare Services™ for Security and Compliance

The table below describes the security bundle services that enable in-depth defense against cyberthreats.

Service	Service Details	Protects	Protects Against
Anti-virus/ Anti-malware	Provides an agent that scans Windows- or Linux-based VMs for viruses and malware	Host	Zero-day attacks, ransomware, malware, malicious URLs, command and control locations, viruses, Trojans
Host Intrusion Detection and Firewall	Endpoint-level intrusion detection services; protects against vulnerabilities as defined in the common vulnerabilities and exposures (CVE®) database, such as detecting propagation of ransomware	Host	Known vulnerabilities in popular applications/OS, insider threats, zero-day attacks, denial of service, SQL injection, cross-site scripting
Host Integrity Monitoring	Monitors and detects changes to files, directories and their attributes that can impact host security on protected systems	Host	Insider threats, zero-day attacks, denial of service, SQL injection, cross-site scripting, changes from desired configurations
Vulnerability Scanning	Scans customer systems for common vulnerabilities via a scanner	Host, OS	Privilege escalation, SQL injection, cross-site scripting, known OS and applications
Log Management	Virtustream security alerts based on aggregation, correlation and monitoring of security and OS logs	OS, Host	Unplanned changes, intrusions, advanced malware attacks as they happen
Data at Rest Encryption	Directory level encryption with privileged user level control	Data	Data breach, data theft
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	Network	Zero-day attacks, brute force attacks, known threats
Firewall Policy Auditor	Provides perimeter firewall reports and perimeter firewall audit results	Network	Finds configuration errors and gaps to avoid brute force and known attacks
Log Forwarding	Provides copy of security logs/ events to the customer-owned log destination/SIEM	OS, Host, Network	Forwards aggregated OS and security logs for integration with analytics systems
OS Hardening Scans	Monitors and reports on customer digital asset compliance with CIS level 1 hardening standards	OS	Configuration drift, privilege escalation, SQL injection, cross-site scripting

Table 2: xStreamCare Services for Security and Compliance Service Details

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 our culture and values differentiate the Dell Technologies family of businesses in the marketplace just as much as our products, services and innovations.

Trust Center

To learn more about how Virtustream keeps your mission-critical applications safe, please visit our Trust Center. For more information about Virtustream cloud solutions and services, go to www.virtustream.com.

About Virtustream

Virtustream LLC, a Dell Technologies business, is the enterprise-class cloud company that is trusted by organizations worldwide to migrate and run their mission-critical applications in the cloud. For enterprises, service providers, healthcare organizations and government agencies Virtustream's xStreamCare Services™ expertise combined with the Virtustream 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.