STEELDOME
Data Protection in the Cloud Era

WHITEPAPER SERIES

ADDRESSING THE NEW THREAT IN MODERN IT INFRASTRUCTURES

INFINIVAULT™: A NEW APPROACH IN THE WAR AGAINST RANSOMWARE

STEELDOME
Data Protection in the Cloud Era

CONTENTS

STEELDOME
Data Protection in the Cloud Era

EXECUTIVE SUMMARY

Data has become a new global currency. As with other currencies, it has also become a target for threats from those who wish to exploit its value. Ransomware is the new threat to data and it's wreaking havoc on businesses of all sizes around the world.

Until recently, if you ask an IT organization to describe typical causes for service outages they would most likely mention network failures, power failures, hardware failures, user error, etc. In today's world, we can add ransomware to that list.

Ransomware attackers (aka. threat actors) work to infiltrate an organization's network. Once the network has been penetrated, one of the first orders of business is to access and destroy the backup data and any ability to recover. The next step is to encrypt the victim's live production data. Once the encryption is enabled, the data is literally cut off from the IT systems and applications which access the data. The result is a devastating IT systems crash resulting in an outage for your business.

Typically what follows is some form of communication from the attacker indicating they have seized your data and if payment is not received within a certain period of time, the data will be permanently deleted. Unfortunately, statistics show that even once the ransom is paid, organizations have a 50/50 chance of actually receiving the keys to unlock the data.

Even in the best case scenario where the attacker provides the keys to decrypt the data, the time it will take to decrypt is usually significant. Then once the data is finally decrypted, the organization can begin the recovery process. This entire experience won't be just painful, it will be your organization's worst nightmare.

STEELDOME
Data Protection in the Cloud Era

EXECUTIVE SUMMARY

Traditional methods of combating ransomware have generally involved various forms of firewalling, monitoring and detection. While certainly necessary, these only provide partial protection against what some experts in the industry view as an inevitability given enough time. To make matters worse, the security framework must also be built to protect the organization from its own employees (aka. insider threat). Considering all of these elements, coupled with the ever increasing complexity of today's modern IT infrastructures, it's no wonder why we read about security breaches on a daily basis.

The industry needs a definitive approach to safeguarding the most important asset in the data center, which is the data itself. This is precisely what will be covered in this whitepaper.

STEELDOME
Data Protection in the Cloud Era

THE BAD NEWS: LATEST STATISTICS

- The number of ransomware attacks performed against organizations doubled in the first half of 2021 alone. 2021 is expected to close out the year with 714 million ransomware attack attempts.

- Across all known attacks, businesses in the United States were the target over 54% of the time.

- The top industries attacked in 2021 (in order from the highest occurrence to lowest): Manufacturing and Supply Chain, Financial Services, Transportation, Technology, Human Resources, Healthcare, Retail, Government, Energy and Education.

- Ransomware-as-a-service is now available to malicious hackers around the world to provide subscription services to those who want to launch coordinated attacks against organizations.

STEELDOME
Data Protection in the Cloud Era

THE GOOD NEWS: THERE IS A SOLUTION

Defensive strategies within the network are critical in preventing an attack from happening. This strategy must also include a defense for the very thing the attackers are after: *your data*. InfiniVault™ provides for this defense through the following design philosophies:

PHILOSOPHY	PURPOSE	BENEFIT
Security First	Provide access and operational security integrated end-to-end	Maximum protection for data in-flight and at rest
Cloud Backed	Leverage global cloud based storage resources	Access to virtually unlimited cloud storage resources
Software-based	Provides zero hardware dependency	Significant cost savings with maximum deployment flexibility
Zero-trust Framework	Establish strong authorization and access controls	Maximum protection against unauthorized access
Zero-day Defense	Eliminate threat from new and unknown vulnerabilities	Reduces complexity of tooling required to account for all possible vulnerabilities within the network
Proactive Monitoring	Real-time monitoring for virus and malware signatures as data is written to the vault	Allows for proactive detection and response to threats potentially before they are able to activate on the network
Data Fidelity	Ensure data integrity and availability even under unfavorable operating conditions	Data is safeguarded against cloud site failures and silent bit error corruption
Minimal Attack Surface	Restrict access to only necessary protocols for vault operation	Reduces attack surface exposure
Common Protocols	Provide vault access via common universally accepted communication protocols	No agents, proprietary components or other intrusive software required
Ease of Operation	Remove provisioning and operational burden from customer	Simplifies mission. Customer only needs to focus on what data needs to be protected by the vault

STEELDOME
Data Protection in the Cloud Era

WHAT IS INFINIVAULT™?

InfiniVault™ is a highly-secure, zero-day (no warning), software-based data protection appliance. It leverages simultaneously any public cloud provider storage resource to distribute and store data under its protection. As data is written to the vault, it goes through a series of processes which ensure data survivability, integrity, security and immutability. All of these processes are crucial, but immutability is the most significant in preventing the impact of ransomware.

The vault security is of utmost importance which is why only well established data transfer protocols are made accessible to the customer network. Additionally, if the customer has to recover from a data loss event (regardless of reason), the customer is only granted access to the recovered data once multiple levels of authentication are performed by SteelDome security engineers.

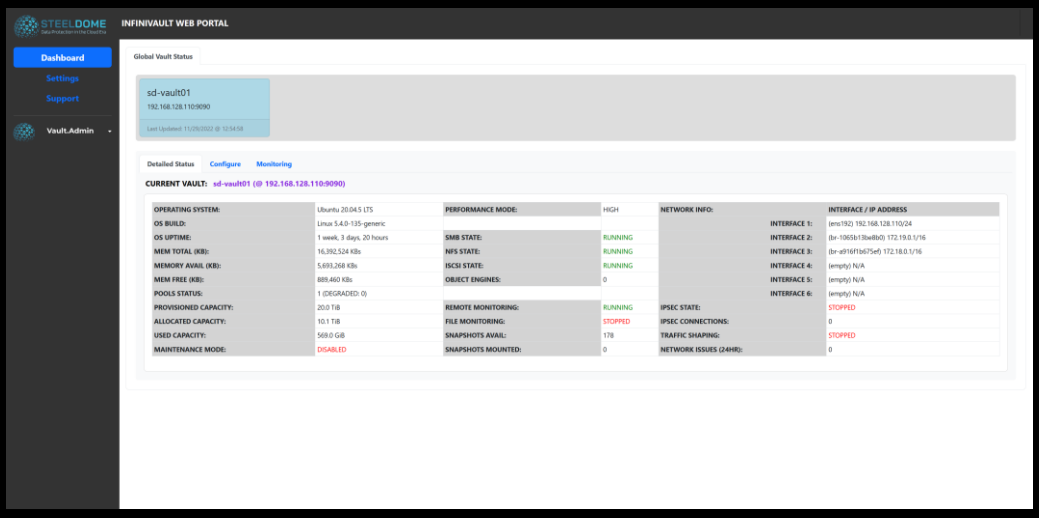
The vault requires no configuration or management from the customer and is delivered fully operational and secure immediately ready for use within their infrastructure. It has been designed from the ground up to be as simple as possible to use while highly effective at securing data and defeating the severe impacts of ransomware.

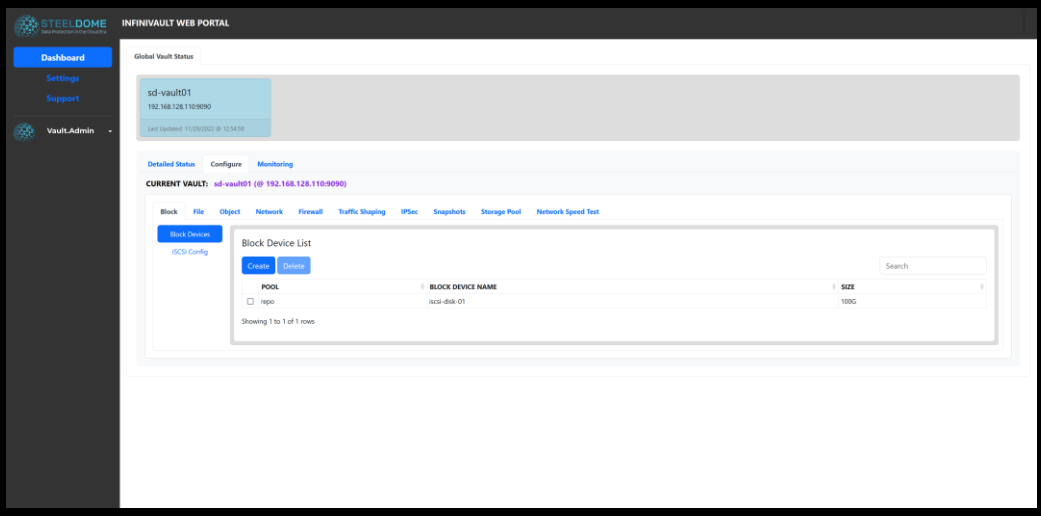
STEELDOME
Data Protection in the Cloud Era

WHAT IS INFINIVAULT™?

A sophisticated monitoring, reporting and alerting interface is also provided to indicate and track overall system health. Additionally, this interface is configured to monitor for specific events and trends which could indicate suspicious activity such as ransomware.

SteelDome InfiniVault™ Global Fleet Management Interface





STEELDOME
Data Protection in the Cloud Era

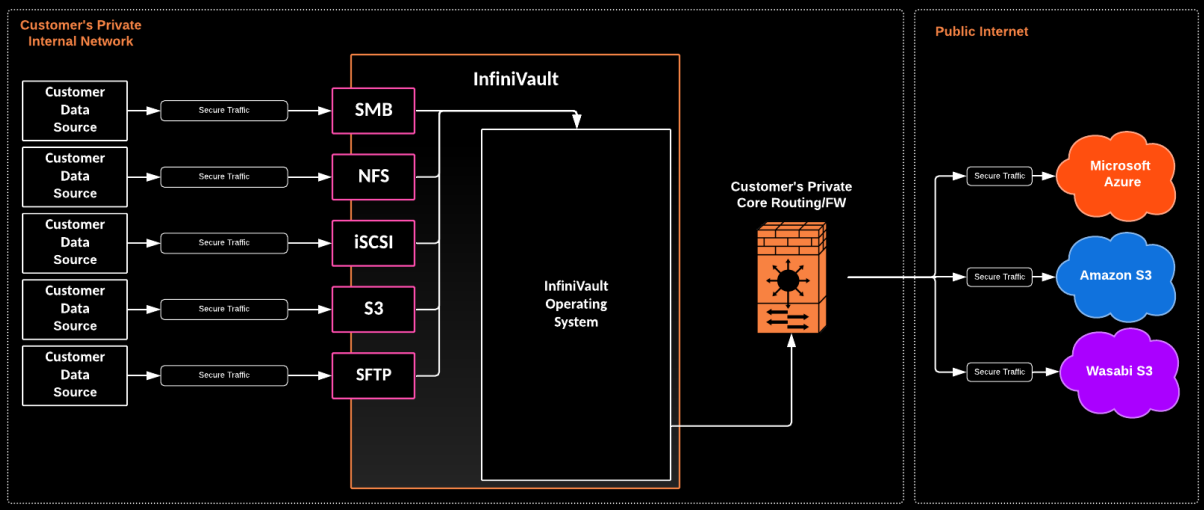
INFINIVAULT™ DEPLOYMENT SCENARIOS

InfiniVault™ is software based which delivers maximum flexibility within various deployment scenarios. While there are many variations for deployment, this document will cover three of the most common types: *On-Prem Private Infrastructure Deployment*, *Public Cloud Infrastructure Deployment* and *SMB Deployment* (where no infrastructure exists at all).

Private Infrastructure Deployment

In this deployment scenario, the InfiniVault™ software is deployed as a virtual machine. The virtual machine is compatible with all major hypervisors such as VMware ESX and Microsoft Hyper-V.

The virtual machine is delivered fully operational to the customer. Once deployed through the virtual machine import process, the vault is accessible on the private network through one of five universal data transmission protocols (SMB, NFS, S3, iSCSI and SFTP). The vault is configured to only communicate with trusted endpoints to limit the attack surface.



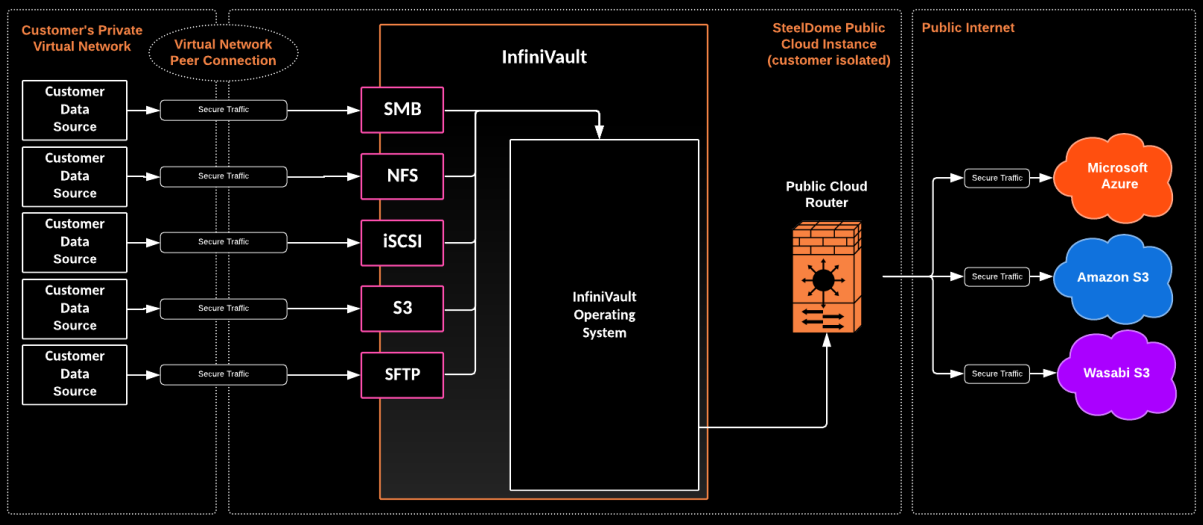
STEELDOME
Data Protection in the Cloud Era

INFINIVAULT™ DEPLOYMENT SCENARIOS

Public Cloud Infrastructure Deployment

In this deployment scenario, the InfiniVault™ software is deployed as a virtual machine on any of the global public cloud provider platforms such as Amazon Web Services and Microsoft Azure.

The virtual machine is delivered fully operational to the customer. Once deployed, the vault is accessible to the customer's private cloud network through one of five universal data transmission protocols (SMB, NFS, S3, iSCSI and SFTP). The connectivity between the vault and the customer's network is made possible via a private peering session between the two networks. The vault is configured to only communicate with trusted endpoints within the customer's private network segment to limit the attack surface.



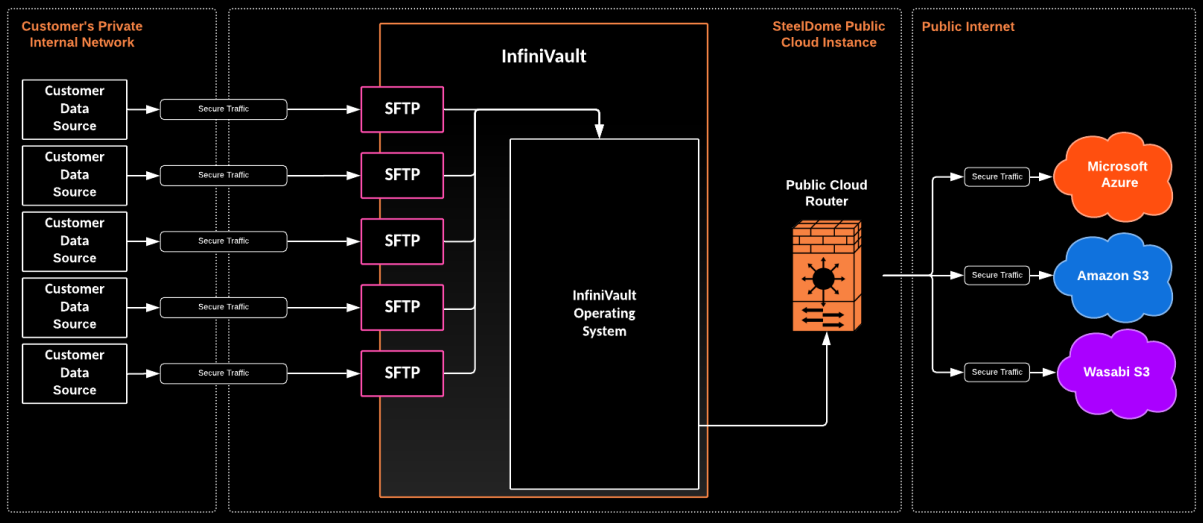
STEELDOME
Data Protection in the Cloud Era

INFINIVAULT™ DEPLOYMENT SCENARIOS

SMB Deployment

In this deployment scenario, the InfiniVault™ software is deployed as a virtual machine on a global public cloud provider platform such as Amazon Web Services and Microsoft Azure.

The virtual machine is delivered fully operational for use by the customer. Once deployed, the vault is accessible to the customer's private office network through Secure FTP (SFTP). The SFTP client is used for scheduled transmission of the customer data. The vault is configured to only communicate with the trusted customer endpoint (usually the external IP address of the customer's firewall) to limit the attack surface.



STEELDOME
Data Protection in the Cloud Era

CONCLUSION

Ransomware is a pervasive and serious threat to organizations everywhere. Many organizations reading this right now have already been compromised and don't even know it... yet. InfiniVault™ provides the ultimate defense against this threat. While the vault will not stop the attack, the vault will provide a means of rapid and reliable recovery beyond anything available in the marketplace today.

The longer an organization operates without a data protection mechanism such as the InfiniVault™, the greater the likelihood they will suffer a devastating data loss event due to ransomware.

Contact SteelDome Cyber today for more information and to request a live demo of the InfiniVault™.

SteelDome Cyber, LLC
www.steeldomecyber.com
(888) 362-1337