Pivot3 and HyTrust for Cost-effective, High Performance and Secure VDI

Solution Whitepaper

V 1.1

October 2017

Table of Contents

Introduction

Pivot3 has created this series of Solution Whitepapers with HyTrust to outline the business and technical benefits of solutions that combine the two companies' technologies. In this paper, we examine the challenges that IT organizations face within regulated environments, where encryption and compliance are necessities, and explore how Pivot3 and HyTrust are able to deliver a cost-effective, high performance and highly secure solution.

The Business Challenge

In today's digital world, reports of corporate data breaches consistently make headlines. While many advocate the use of better cyber security measures, human error will always be a vulnerability that can't to be solved by a patch, a quick fix or firewalls. Frustratingly, perhaps, human error cannot be eliminated. What an IT director can do is deliver a granular level of encryption on a secure desktop to mitigate for human fallibility.

There are many solutions for blanket security, but there are also many challenges associated with this 'blanket' process. Probably the most common solution is to provide an "Authentication Token" system such as RSA, and, while this is great for multi-factor access to the data, and offers a large measure of security to the end-point device, it doesn't prevent data breaches occurring should the device be compromised.

Moving back into the datacenter, a system administrator is presented with the usual choices:

Self-Encrypting Drives (SEDs) are the most common hardware solutions in the market, but they are often expensive and take a blanket approach to encryption. There is also the performance penalty associated with the drives performing the encryption, reducing the performance of the overall infrastructure and lowering the density of VDI sessions running on the infrastructure, driving the total cost per desktop into a potentially cost-prohibitive bracket.

Other solutions require the administrator to encrypt the ESXi cluster and ensure that every member of the cluster, and their associated datastores, are also encrypted - the result being several phases of the data path being encrypted and decrypted as data services are applied to the data as it passes through the IO stack. While this is more granular, the risk associated with potential inflight data capture and the encryption/decryption process make it a less secure solution than the SED option.

A more specific challenge in VDI is the rapid creation, deployment and provisioning of desktops, leading to an infrastructure with large amounts of IO, and given the noted performance penalty of encryption, delivering this at scale becomes a performance headache.

It is also the case with VDI that not every desktop requires encryption and protection, so a blanket approach to encryption unnecessarily places additional load on the infrastructure, reducing user density and more importantly, delivering a sub-optimal user experience. User experience has been noted by several analysts as being the primary reason that VDI deployments never scale past the pilot phase.

The Solution

Pivot3 and HyTrust provide a secure, multi-tenant infrastructure solution that delivers the performance, scale, and efficiency required of cloud and virtualized data centers as well as the required levels of data protection and security controls needed to simplify regulatory compliance and safeguard against the risk of breaches and other attacks.

Both products are managed through policies, meaning that system administrators can approach their environments in a workload-centric manner, simplifying and removing the need for complex hardware infrastructure and enabling a modular, fine-tuned approach.

By removing the requirement for blanket hardware encryption, organizations are able to take advantage of a simple, scalable and modular infrastructure. This facilitates a greater level of agility in the IT organization, enabling a more rapid deployment model, without the (often) long lead times associated with purchasing hardware based encryption products. Costs are also removed as multiple hardware infrastructures for “Sensitive” and ‘Non-Sensitive” workloads no longer need to be designed and maintained; encryption is simply applied to the VMs as they are deployed, and Pivot3’s simple, policy-based quality of service (QoS) means that they are immediately given the appropriate level of performance and priority.

HyTrust Workload Security

Scalable & Flexible Data Protection

HyTrust DataControl supports up to 5,000 encrypted workloads per HyTrust KeyControl cluster, enabling a single large pool of VDI users in Enterprise environments. There are no limits to the amount of encrypted data other than those imposed by the underlying workload operating system. Customers can choose to protect entire workloads leveraging disk encryption, folder/directory encryption or individual file encryption. Using disk encryption provides the highest level of workload protection. Working at the block level, the entire disk is encrypted and any disk can be protected, including boot (C: on Windows or root on Linux). Policies may be set up in HyTrust KeyControl to prevent a workload from booting up, or an encrypted data volume from being accessed, when specific conditions apply, such as changes in hardware signature, or even contingent upon hardware attestation leveraging HyTrust CloudControl and HyTrust BoundaryControl. HyTrust BoundaryControl allows for geo-sensitive data protection, for users that may travel globally, yet have access to shared drives or global file systems in territories that require sovereign data controls.

Regardless of disk size, disk encryption does not require downtime. “Dynamic Rekeying” allows for encryption to be applied with zero operational downtime, regardless of whether it is during initial encryption or when key rotation is required, a fundamental data security best practice. Notice that when performing a rekeying operation with DCPA, data is never decrypted to disk. From a performance perspective, when an encryption operation is kicked off, DCPA encrypts data only when disk I/O is idle, preventing the encryption operation to affect the applications running on the workload. This avoids an additional performance penalty during VDI boot storms and the typically IO intensive process during a VDI session deployment.

In addition to disk encryption, HyTrust DataControl provides folder level encryption for Linux, enabling the encryption of all files within a specific folder/directory while retaining the high level of key management security provided by HyTrust KeyControl. Encryption keys are generated and stored within HyTrust KeyControl, delivered securely to only workloads that have been registered with the HyTrust KeyControl cluster while multi-tenancy policies still apply. The encrypted filesystems may also reside on a remote server (e.g. via NFS). Lastly, file-level encryption can be used to share files securely without the need to directly share encryption keys. A file encrypted from a workload (e.g. server, workstation) that is part of the HyTrust DataControl environment can be accessed from any other workload if it is allowed per policy.

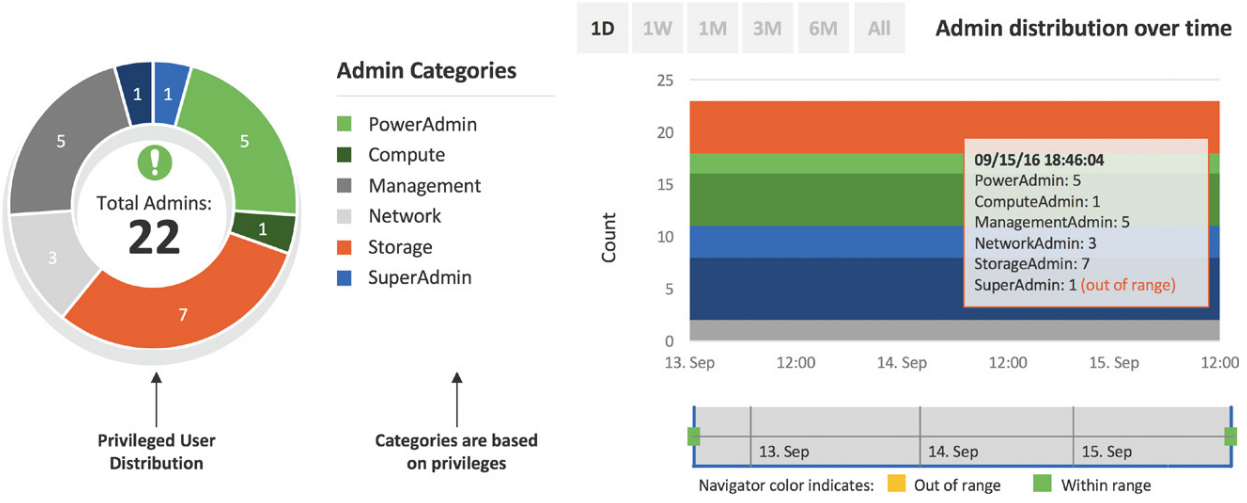
Role-Based Access Controls/Role-Based Monitoring (RBAC/RBM)

One of the most common breaches of secure desktops occurs when Administrators have access to content that they shouldn't, by granting privileges designed to allow Administrators to resolve issues and fix problems. This can be a problem where data is sensitive and when the VDI solution or support is outsourced.

By enabling RBAC, an organization can restrict the administrative privileges of a support engineer to only be able to access, fix and view the necessary parts of the infrastructure to do their job. When combined with Role-Based Monitoring (RBM) an organization can watch for "unexpected behaviors" and take appropriate actions. For example, an administrator for the EMEA team copying data from VMs in the USA to a datastore located in APAC, or migrating production VMs to an unexpected cluster, possibly used for test and development, would be flagged.

Tying this into data fencing, particularly in VDI, and especially in healthcare, financial services and other industries handling sensitive client data, leads to a more robust and enforceable set of policies and reduces the potential for data breaches

Beyond RBAC, most organizations also require an efficient and flexible way to:



1. Grant privileged users temporary permissions needed to perform infrequent duties.

2. Have greater control over the use of powerful privileges by users who need those privileges to do their daily jobs.

For example, a virtualization operations group needs ongoing authorization to create and delete VMs used for non-production applications, but management also wants the ability to approve or deny any attempt by this group to delete a production virtual machine.

Because the VMware platform does not provide a viable way to enable one-time approval of a specific operation attempted by a specific privileged user, organizations have turned to HyTrust CloudControl's Secondary Approval capability for both vSphere and NSX operations. From a workflow perspective, this feature allows authorized users to configure HyTrust CloudControl to require additional approval before privileged users can perform sensitive or disruptive operations on specific virtual objects (e.g. delete or power off a virtual machine, edit a firewall or create an edge services gateway). The process requires that a designated group of approvers authorize an operation attempted by a privileged user before that operation can proceed.

Dynamic & Rapid Rekeying

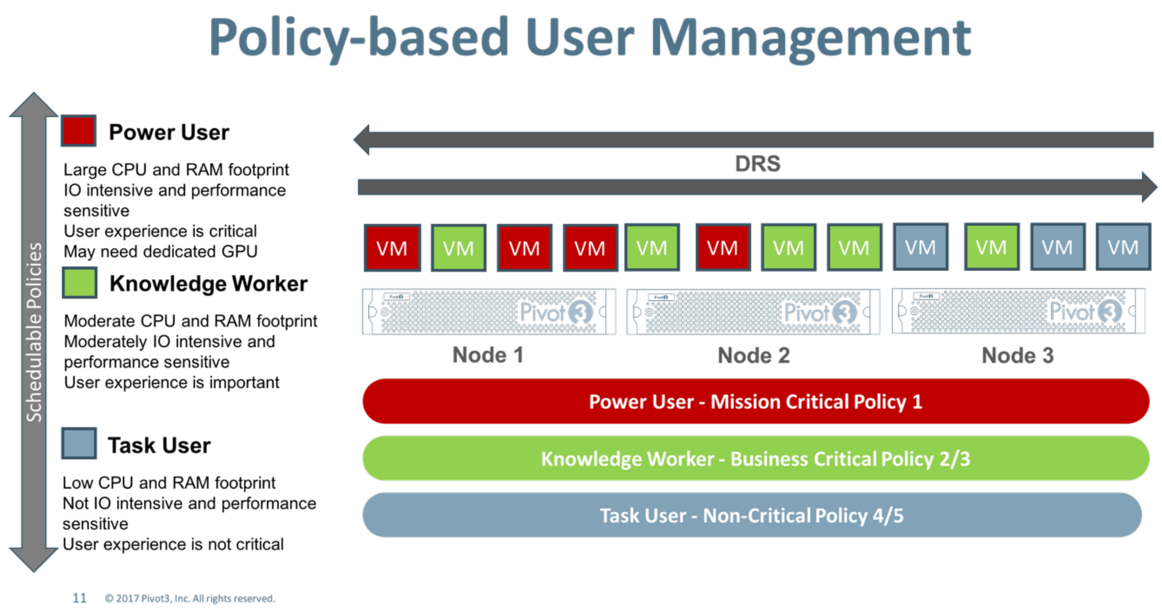
User acceptance in VDI is vital, and is predicated on desktop performance in 99% of cases. Most organizations schedule changes of encryption keys on a regular basis as a best practice and to meet specific compliance requirements. HyTrust DataControl is the only product on the market that can allow for rekeying of encryption keys without any downtime. In addition, with scheduled based re-keying, administrators can literally "set and forget" – making the process very easy with no burden on operations.

In a VDI environment, this non-disruption of a user's desktop experience allows for compliance and user experience to be maintained simultaneously, leading to happier users and auditors.

Pivot3 for VDI

Smarter Infrastructure for Better VDI

Hyperconverged infrastructure (HCI) can directly address the issues of scalability, cost and performance by collapsing the traditionally silo'd tiers of infrastructure into modular building blocks based on industry-standard hardware. By combining compute, storage, networking and virtualization, HCI eliminates infrastructure complexities and simplifies infrastructure management.



Policy-based User Management

🟥 **Power User**
Large CPU and RAM footprint
IO intensive and performance sensitive
User experience is critical
May need dedicated GPU

🟩 **Knowledge Worker**
Moderate CPU and RAM footprint
Moderately IO intensive and performance sensitive
User experience is important

🟦 **Task User**
Low CPU and RAM footprint
Not IO intensive and performance sensitive
User experience is not critical

Power User - Mission Critical Policy 1
Knowledge Worker - Business Critical Policy 2/3
Task User - Non-Critical Policy 4/5

11 © 2017 Pivot3, Inc. All rights reserved.

Pivot3's HCI solutions optimize virtual desktop deployments by providing a modular, policy-based platform that minimizes infrastructure footprint and TCO, delivers seamless user experience, and simplifies the transition from pilot to full-scale deployment.

Breakthrough End-User Experience

A superior end-user VDI experience is closely tied to the storage IO performance of the underlying infrastructure. Many VDI implementations slow down or even come to a screeching halt during periods of high IO activities, such as boot or login events. Pivot3's unique distributed scale-out architecture delivers outstanding IO performance at lower latencies by ensuring all drives in a cluster participate in all IO activities simultaneously. Additionally, Pivot3 Acuity HCI platform provides advanced policy-based QoS coupled with NVMe PCIe flash IO acceleration, ensuring consistently high IO performance. Lastly, performance-enhancing features like global read/write cache and hypervisor pass-through also help deliver superior response times. These capabilities combined, enable blazing fast response times for end-users.

Cost-Effective VDI with Lower Footprint and Higher Density

Cost is often one of the reasons VDI deployments fail to achieve positive ROI. Pivot3 delivers cost-effective VDI by delivering up to 3X the desktop density per node. Pivot3's HCI operating environment is much more efficient than alternative HCI solutions, enabling higher VM density. Policy-based QoS coupled with an NVMe flash storage tier further improves density by eliminating IO bottleneck for the most important VDI workloads. Additionally, Pivot3's patented erasure coding enables up to 94% usable capacity while ensuring market leading resiliency and availability. These capabilities, combined with many other performance enhancing features, enable up to 3X VM density while delivering up to 6X storage performance.

Simple, Predictable Scale from 100s to 1000s of Desktops

Pivot3's distributed scale-out architecture ensures linear predictable scalability, not only for capacity, but also for storage IO and available bandwidth. As you add more nodes to an existing Pivot3 cluster, the data is automatically and non-disruptively re-balanced on the expanded storage pool. By adding more nodes, effective IO capacity is automatically added because all volumes and data sets are distributed across all available drives and nodes. Each node brings 2 X 10Gbps storage network connections, so the effective throughput scales as you scale the cluster. Linear scalability is critical in VDI environments. As the number of desktops grows, IT organizations can predictably scale their infrastructure to meet their needs.

Summary

The ability to combine Pivot3 Acuity HCI and HyTrust Workload Security solutions allows IT organizations to leverage best-in-class solutions to create a cost-effective, high performance and secure virtual desktop infrastructure that advances their end user computing strategy.

HyTrust's granular approach to encryption means that only those users that need to work with sensitive data use encryption, keeping deployment costs lower. Pivot3's modular approach allows VDI to be deployed in simple, manageable phases, and the unrivalled VDI density Pivot3 brings ensures that datacenter footprint is minimal and cost per desktop is kept affordable.

Validated Solutions Reduce Risk and Speed Deployment

Pivot3 and HyTrust are Technology Alliance Partners and work together to modernize customers' IT infrastructure by leveraging Pivot3 smarter hyperconverged infrastructure and HyTrust Workload Security solutions. Pivot3 and HyTrust invest in validating, documenting, deploying and supporting joint solutions and services required for businesses to operate 24x7x365.