

Xi Beam: Security and Cost Governance for Nutanix

KEY FEATURES

- Automated security audits and compliance remediation
- Network, VM, data and access related security audits
- Cluster and VM Costing utilizing a TCO model for accurate cost analysis
- Automated Showback and Chargeback reports

BEAM CAPABILITIES FOR NUTANIX ON-PREM ENVIRONMENTS

Beam is a multi-cloud governance platform that provides security compliance and cost governance capabilities for Nutanix, AWS and Azure clouds. Beam helps with real-time detection of security vulnerabilities and compliance validation with regulatory policies using 300+ automated audits. Beam also provides cost governance capabilities including Nutanix private cloud metering, automated chargeback reports and workload cost analysis across Nutanix and public clouds.

In this datasheet we go into detail about Beam's security and cost governance features for Nutanix on-premises environments.

NUTANIX COST GOVERNANCE IN BEAM

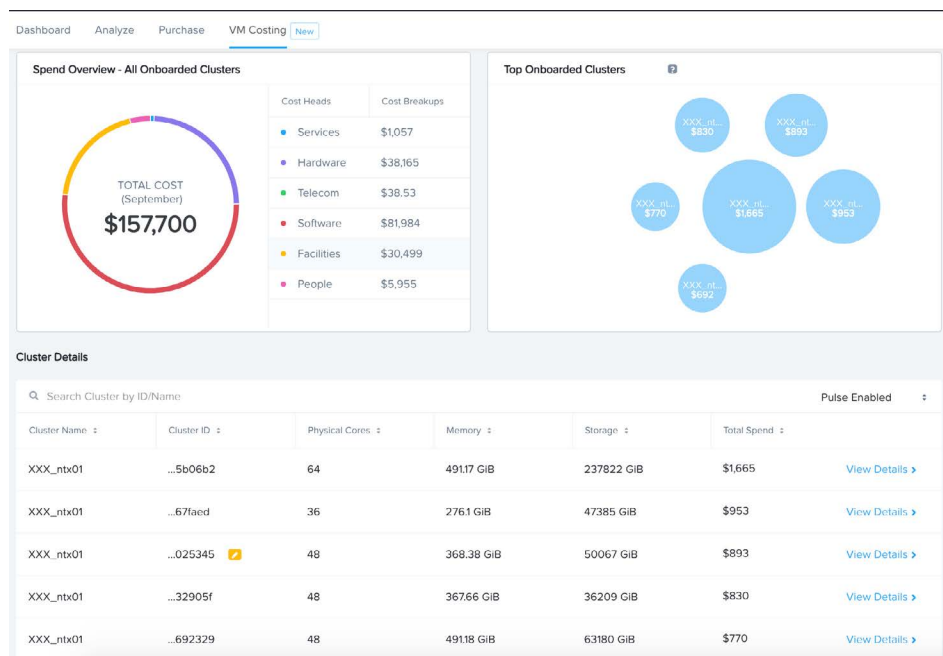
Private Cloud Metering and Chargeback

Beam's key cost governance capabilities include metering and chargeback for Nutanix. This utilizes a built-in Total Cost of Ownership (TCO) model that calculates all direct and indirect costs of owning and maintaining your Nutanix infrastructure. The TCO model uses an assumed market price for the Nutanix products and also allows you to easily configure the Nutanix product costs. There are 6 different cost heads in the TCO model:

- **Hardware:** Nutanix or third-party hardware license costs
- **Software:** Nutanix or third-party software license costs
- **Facilities:** Power, cooling and datacenter infrastructure costs
- **Telecom:** Ethernet / top-of-rack switch costs
- **Services:** One-time or recurring third-party services costs
- **People:** Salaries for IT administrative staff

“Beam moves us out of the realm of uncertainty, giving us a clear view of the security of our Nutanix infrastructure”

-Dominic Maidment Technology Architect
Total Gas & Power



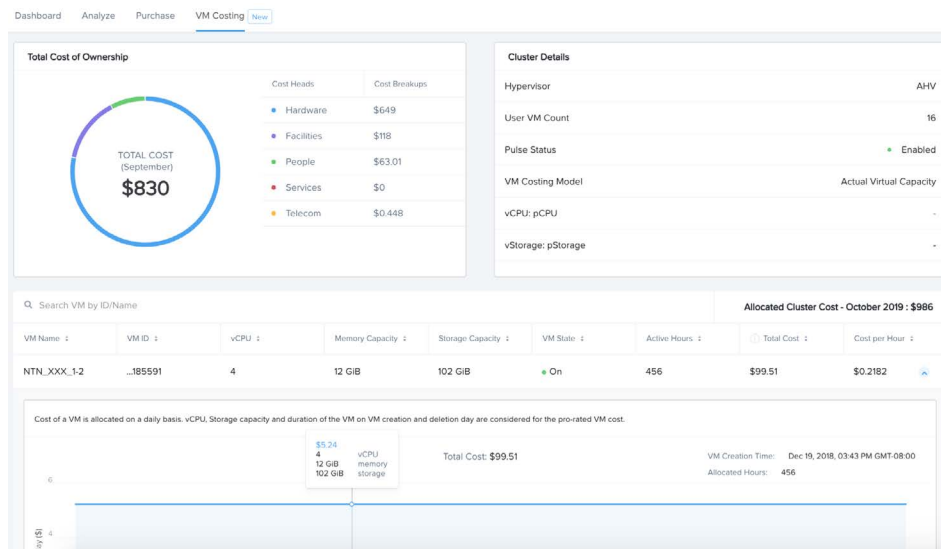
The TCO model is customizable for each cost head giving you the flexibility to configure the costs to match your specific needs. The key input parameter that the TCO model depend on is the number of Nutanix nodes. With the TCO model configured accurately, you will be able to analyze the true cost of the VMs and workloads running on your Nutanix infrastructure.

Beam detects the number of nodes and product license details associated with your Nutanix clusters through your purchase history and calculates the cost per cluster using the TCO model. If you have enabled Pulse Insights in Prism Central, Beam will be able to detect the VMs running in each cluster.

Beam will then allocate the cluster level costs to the VMs within that cluster based on the virtual CPU and virtual storage configuration, and the VM state. Users can either get dynamic VM costs based on the existing virtual capacity consumed by the VMs or set a target virtual capacity by configuring the compute and storage overcommit ratios.

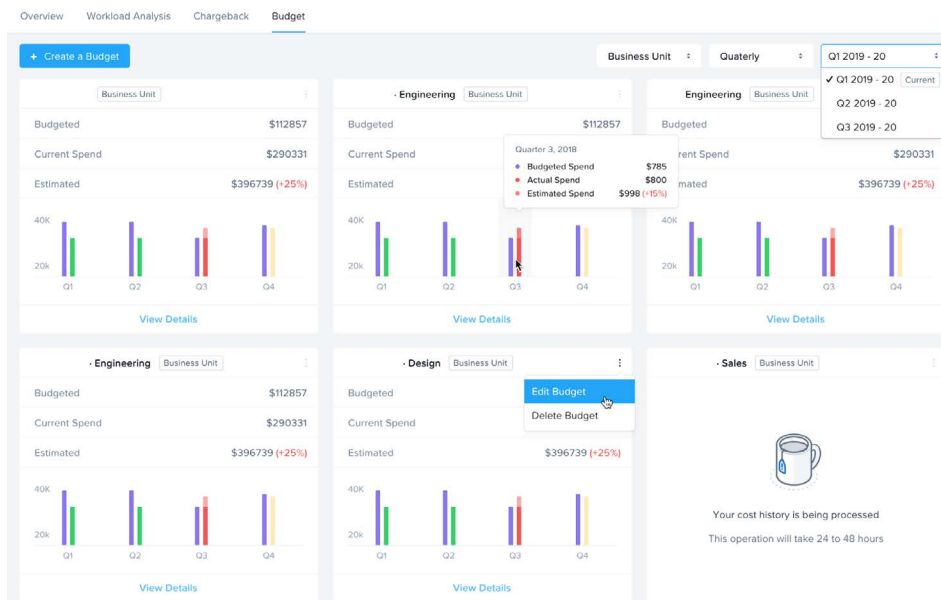
PREREQUISITES

- Most of the security audits depend on AHV
- Cost governance features are hypervisor agnostic
- Only Nutanix HCI is currently supported.

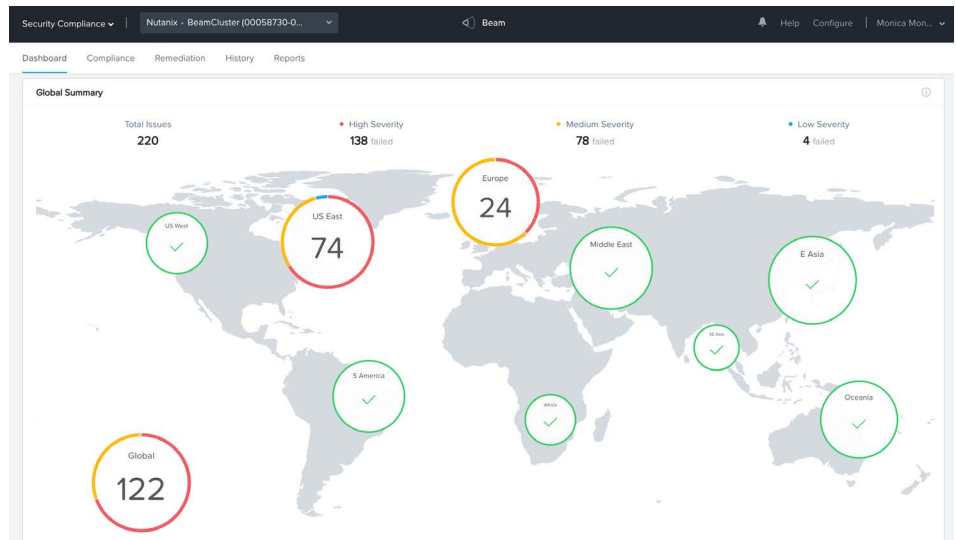


With the cluster and VM level costs accurately configured, users can create spending reports by grouping together various VMs and clusters using tags and categories (same as defined in Prism). This allows users to create segmented spending views for their teams, projects, regions, etc. These detailed reports can be used to chargeback the Nutanix investments appropriately to the relevant business units or cost centers.

Beam's chargeback capabilities are completely multi-cloud including Nutanix and public clouds like AWS and Azure. Beam also allows you to create budget views to track spending against allocated budgets and receive alerts before spending exceeds the budget.



NUTANIX SECURITY COMPLIANCE IN BEAM

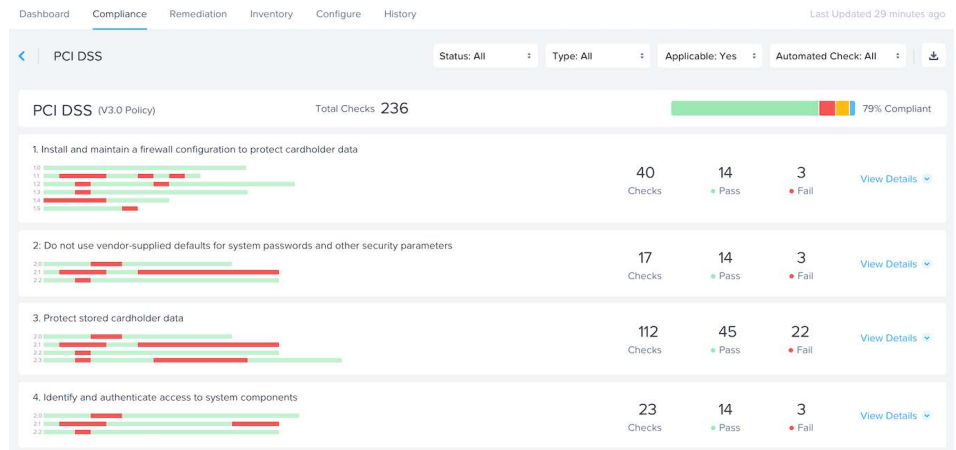


Detection and Remediation of Security Vulnerabilities

Beam's security compliance capabilities come with 300+ out-of-the-box security audits for Nutanix AHV environments. These security audits provide details of any resource misconfigurations in near real-time. The security audits can be classified into the following broad categories:

- Network audits
- VM audits
- Data audits
- Access audits

Some examples of Beam's security audits include publicly accessible TCP/UDP ports, unencrypted data, VMs without backup protection, and much more. In addition to detecting the resources that fail these security audits, Beam also provides remediation actions that you need to perform to improve the security baseline of your infrastructure. With Beam you can easily detect and remediate security vulnerabilities for your Nutanix on-prem infrastructure and improve your cloud and data security.



Regulatory Policy Compliance

Beam also provides out-of-the-box policies that can help validate your level of compliance with regulatory policies such as PCI-DSS (available now), HIPAA, NIST (coming soon), etc. Beam's Compliance features can be used as a system of records that maps all the necessary process, documentation and configuration steps you need to take to ensure that your infrastructure is in compliance with these regulatory policies.

For example, in order to comply with PCI-DSS policy, one of the key steps is installing and maintaining a firewall configuration to protect cardholder data and also ensuring that data-at-rest (DAR) encryption is enabled. Beam can be used to create a record of the formal process steps and documentation that you have put in place to approve and test all network connections and changes. Beam also runs automated audits to validate that DAR encryption is enabled on all your Nutanix clusters and provides a report detailing the clusters that fail that audit so that you can take remediation actions.

Learn more and start your free trial at
www.nutanix.com/beam



T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | [@nutanix](https://twitter.com/nutanix)

©2019 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all product and service names mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. All other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s).