Book of Network Services - Security Central

[PDF generated August 17 2023. For all recent updates please see the Nutanix Bible releases notes located at https://nutanixbible.com/release_notes.html. Disclaimer: Downloaded PDFs may not always contain the latest information.]

Nutanix Security Central is a Software as a Service (SaaS) based offering that provides microsegmentation security planning, threat detection alerts, and continuous compliance monitoring. Using multiple Machine Learning (ML) models and algorithms such as Louvain, Arima, tree based, and clustering, Security Central gives insight into the security of your on-premises deployments based on over 500 audit checks and security best practices.

The Security Central portal at https://flow.nutanix.com/securitycentral provides an inventory and configuration assessment of your cloud and on-premises infrastructure to scan for common and high-risk configuration errors. Security Central users can also get instant insights on security status by using custom or system-defined SQL like queries. Powered by this inventory and coupled with compliance tracking tools, security posture monitoring is also provided. Finally, network flow data ingested from on-premises AHV clusters provides near real-time threat detection based on machine learning analysis of traffic patterns.

Supported Environments

- Nutanix on-premises
  - Private cloud using AHV with Flow Network Security enabled

- Public clouds: AWS and Microsoft Azure
  - Monitor resources and services within your Public Cloud infrastructure

Management Interface(s)

- Nutanix Security Central SaaS UI
- Flow Security Central VM (FSC VM)
  - Initial configuration and upgrades when necessary

Implementation Constructs

Security Central introduces a few new constructs to provide a security monitoring and management framework. Here are the two elements introduced:

- Flow Security Central VM (FSC VM) [Required only for Nutanix on-prem]
  - Used during initial configuration
  - IPFix log collection
  - Inventory collection
  - Push security policy configurations

- Security Central SaaS
  - Security posture monitoring
  - User & network anomaly detection
  - Compliance reporting
  - Microsegmentation security planning
  - Multi-cloud inventory and query

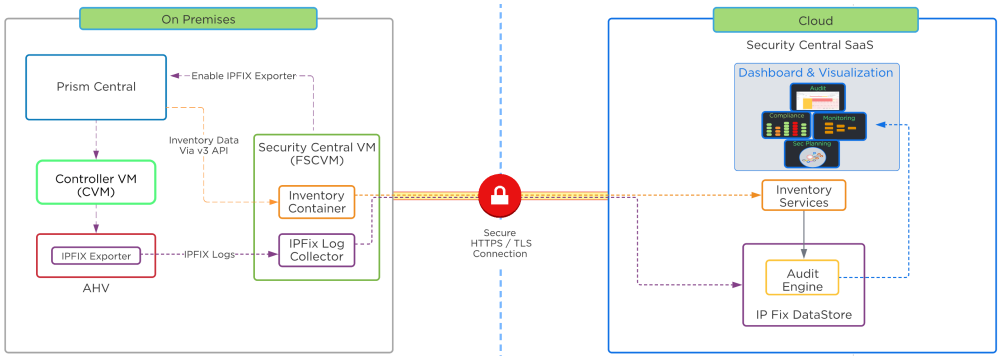
Upgrades

- Automatic as Security Central is a SaaS platform
  - As new features are released, they are available at the next login.

- On occasion, an upgrade to the on-prem FSC VM may be required to enhance functionality
  - Upgrades can be performed on the Flow Security Central VM Settings page

- The latest FSC VM images (both GUI and server-only) are located on the Nutanix Portal

Security Central Architecture Overview



Security Central Architecture Overview

Security Central High Level Architecture Detail

Security Central introduces a new service VM known as the FSC VM, which is required to enable security monitoring for Nutanix clusters. The FSC VM acts as a proxy and aggregates information from the Nutanix clusters. It then sends this information to Security Central through a secure network connection. The FSC VM collects inventory information about the environments and VMs, referred to as metadata. Security Central does not collect any data owned by the VM, such as installed software packages and versions, but integration with partner agents such as Qualys is available to enrich the metadata.

Once installed, the administrator connects to the FSC VM UI to enable network log collection. The FSC VM then instructs Prism Central to enable the IPFIX exporter on all AHV clusters managed by this Prism Central instance. The FSC VM also collects cluster inventory information from Prism Central for all registered clusters and VMs. The inventory information collected includes items such as VM names, connected network information, configuration information and any categories which may be assigned to the VMs. Inventory polling recurs every 3 hours and the SaaS portal can log changes and perform analysis.

Inventory and IPFix logs are securely transmitted to the Security Central SaaS environment using HTTPS/TLS connections. IPFix logs are transmitted in 15 minute intervals allowing the FSC VM to transmit data in batched increments, decreasing storage capacity required for the FSC VM and reducing network constraints to the cloud. Administrators can push required inventory updates to the cloud manually using the FSC VM user interface if needed.

An FSC VM is needed for each Prism Central (PC) deployment regardless of the number of clusters managed by that PC. The FSC VM will facilitate internal communications to Prism Central, and outbound communication to the SaaS portal. Security Central uses the TCP ports listed below for communication between components. Please ensure that your firewall has the following ports open:

- TCP Port 9440 for the FSC VM to connect to the Prism Central VM
- TCP Port 443 from the FSC VM to connect to *.nutanix.com and *.amazonaws.com

Refer to the Security Central Ports and Protocols page for the complete list of ports.

The FSC platform undergoes strict security controls. Visit Nutanix Trust to view FSC compliance certifications and learn more.

To ensure you meet the configuration requirements for the Flow Security Central VM, please consult the Security Central Guide.

Core Use Cases

- Monitoring and Visibility
  - Multi-cloud dashboards, asset inventory, reporting, and alerts

- Audit and Remediation
  - Insights on Nutanix environments and public clouds using real-time, automated security audits

- Compliance
  - Continuous environment monitoring, automated compliance checks, and assessment for STIG, PCI, and HIPAA

- Security Planning
  - VM to VM network traffic visualization, workload categorization, automated security policy recommendation

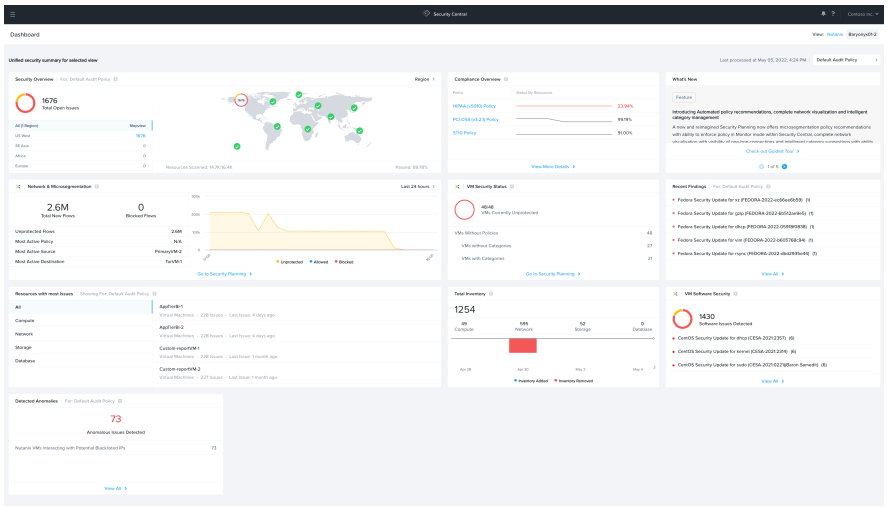
- Investigating Violations
  - Perform detailed investigation with an SQL like query language

- Threat Detection Alerting
  - Network- and user-based anomaly detection. End user behavior analysis (EUBA) helps to detect internal and external security threats

Security Central Key Features

Main Dashboard

The first screen presented after successful login to Security Central is the main dashboard. The dashboard provides an at-a-glance view of the many areas monitored and alerted on by Security Central. More detailed displays can be launched from the context of each individual widget.



Security Central Main Dashboard

Audit and Remediation

Utilizing security audits provides deep insights into the security of your on-premises deployments. Security Central runs more than 500 out-of-the-box automated security audits of your environment and reports any audit failures along with steps to remediation. Security Central audit checks align to the following categories and Nutanix security best practices:

- Access Security
  - Configuration and alerts for items that could allow unprivileged access or lack of access auditing

- Data Security
  - Nutanix clusters without Data-at-Rest Encryption (DARE) enabled. DARE is an essential component to securing your infrastructure that prevents unauthorized access to data by systems and users that do not possess the encryption keys.

- Host Security
  - Nutanix VMs without backup protection enabled, making it difficult to recover should a VM be infected by ransomware

- Logging & Monitoring
  - Prism Central critical alerts unacknowledged could indicate that alerts are being ignored or missed. These alerts can indicate a potential exposure risk that could put your infrastructure in jeopardy

- Network Security
  - VMs allow all traffic from all sources can create an exceptionally large attack surface for malicious actors to compromise the VM and infiltrate your environment.

In addition to the constantly updated built-in audits, Security Central provides the capability to customize audits and reports using Common Query Language (CQL). This allows you to run CQL queries on your cloud inventory for various attributes, and create audit checks for your specific use-cases.

Compliance

Compliance is critical for many Nutanix customers. Maintaining compliance allows you to validate that your company's operating environments meet the governing standards they must follow. Monitoring environments for compliance can be challenging and time consuming. Continuous compliance monitoring capabilities are needed to stay on top of ever changing requirements, regulations and environments. Customers benefit from automating these checks, allowing for a concise view and faster time to resolution when addressing compliance violations.

Security Central provides audit checks for common regulatory frameworks such as PCI-DSS, HIPAA, NIST and Nutanix security best practices using the Nutanix STIG policy. The Compliance dashboard provides a compliance score for each of the frameworks being monitored. The score elements can be further examined to view elements of the given framework that are monitored and audited, the number of passed checks and the number of failed checks. The compliance view provides detail on these checks such as which check failed, which section of the framework the check is associated with, and what issues were discovered. The compliance reports and their details can also be exported for offline use and sharing. Security Central also provides extensible capabilities that allow you to create custom audits and custom compliance policies that are based on your business requirements.

Findings and Alerts

> "A problem well-stated is a problem half-solved." - Charles Kettering

With the ever changing threat landscape, security monitoring and alerting is critical in today's environments. Continuously monitoring for and alerting on threats and vulnerabilities found in your network, security controls, servers, endpoints and user applications allowing a proactive approach to alerting in order to strengthen your overall security posture and providing a quicker time to resolution when an issue is detected.

The Findings and Alerts view within Security Central provides a view into your current security posture. This view displays detected configuration issues and anomalous behaviors observed in your Nutanix clusters that are being monitored by Security Central. These findings are based on the selected audit policy. Users have customizable options on how these issues are displayed, providing great flexibility to tailor the findings by audit categories, resources, roles, and business requirements.

Threat Detection Alerts are included within the Findings and Alerts view. Security Central analyzes the Nutanix IPFix network logs to detect and report observed potential threats and anomalous behavior occurring within the monitored Nutanix clusters. These alerts are modeled using machine learning and observed data points. The following are some of the potential threats and behaviors being detected along with the minimum number of days or data-points that must be observed in order for the anomaly to trigger an entry or alert :

- VMs communicating with Blacklisted IPs (known suspect IPs)
  - 1 data-point
- VMs with potential Dictionary Attack
  - 1 data-point
- VMs with potential Denial of Service (DDOS)
  - 21 days
- VLANs with unusual network behavior
  - 21 days
- VMs with unusual network behavior
  - 21 days
- VMs with potential Port Scan Attack
  - 21 days
- VMs with potential Data Leak Attacks
  - 21 days

Security Planning

When planning to secure an application, there are many components to discovery and information collection required to create an effective security policy. Gathering this information can be quite the challenge. You are often tasked with collecting logs from firewalls, networking gear, applications and operating systems to gain an understanding of your application's communication profile. Once that data has been gathered and analyzed, you will consult with the application owners to compare the observed findings to the expected behavior.

Security Central's ML-based Security Planning provides a detailed visualization to aid you in discovery and planning of your application security policies. You can visualize your network traffic flows within your Nutanix on-prem clusters and Security Central makes recommendations on how to categorize and secure your applications.

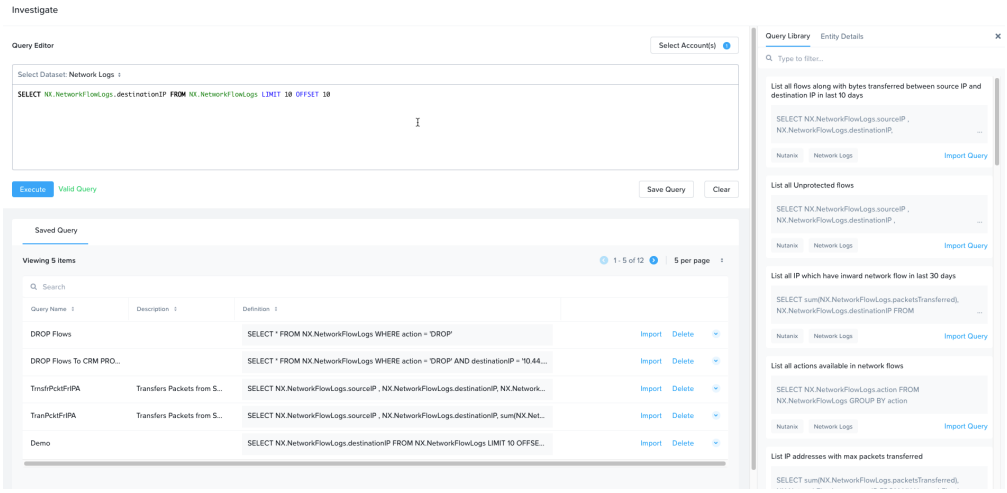
Within the Security Planning section, you have the flexibility to utilize up to 2 levels of groupings for your applications and environments. This capability allows you to drill down your analysis to specific clusters, VLANs, VMs, and categories, making it extremely helpful to focus on securing your applications. With this grouping, you also have the capability to download all observed or filtered network traffic for further offline sharing, discovery, and planning.

Using the inherent machine learning capabilities, Security Central also has the ability to make category recommendations and assignments to VMs based on observed network flows. This can be especially useful in new microsegmentation or application deployments. Categorizing your application VMs is an important step to securing your application. To take it a step further, Security Central can also generate inbound and outbound rule recommendations and create application security policies in monitor mode on your Nutanix AHV clusters.

With the security policy in monitor mode, you can observe the behavior of the application being secured, without applying the policy actions. You can use Prism Central to make edits of the policy if needed prior to enforcing the policy.

Investigate

Investigate helps you analyze security and operational insights for your hybrid cloud infrastructure. It allows you to analyze network logs and security configurations using CQL (Common Query Language). CQL queries offer a user-friendly experience, similar to SQL. To get desired almost real-time results, you can effortlessly run CQL queries on both on-premises and public cloud infrastructure.



Investigate supports following types of queries:

- Inventory and Config: Search for the resource inventory and configuration in your on-premises and public cloud environments
- Network: Search network events in your on-premises environment

Providing cross stack visibility is one of the prime use case for investigate in hybrid cloud environments. For example, in most cases we have multiple stacks of security rules. For the on-premises side we may have Flow Network Security policies and in cloud we may have security groups on EC2 instances. In this case investigate queries can provide a list of all the microsegmentation policies and AWS security policies applied to particular VMs.

The investigate feature also provides a library of most used queries to start with and sets the baseline to create more complex queries based on your needs

Example queries:

- List VM with status (protected or unprotected) and the policy name if the VM is protected

```
SELECT NX.VM.name, NX.VM.NetworkPolicy.*, NX.VM.Category.* FROM NX.VM
```

- List all tags of EC2 instances in AWS

```
SELECT AWS.EC2Instance.Tag.tagKey, AWS.EC2Instance.Tag.tagValue, AWS.EC2Instance.instanceId, AWS.EC2Instance.name FROM AWS.EC2Instance
```

Integrations

Security architectures often consist of solutions from multiple vendors to build a defense-in-depth posture. Solutions that monitor endpoints for threats and vulnerabilities, ticketing systems, log management, and threat and event analytics can all be critical components in a security architecture. While these products are essential, they are often standalone with limited integration with other components of the security infrastructure. Integration is key to bringing security solutions together within the construct of a security architecture. This drives efficiency and faster time to threat awareness, analysis, and threat remediation.

Security Central provides the capability to integrate non-Nutanix applications directly with Security Central. These integrations cover multiple solutions from OS level monitoring and protection to enterprise ticketing systems and analysis engines. Some of the supported integrations are listed below:

- Splunk
- Webhook
- ServiceNow
- Qualys

More detailed information on the specifics of each integration can be found in the Security Central guide.