TECH BRIEF

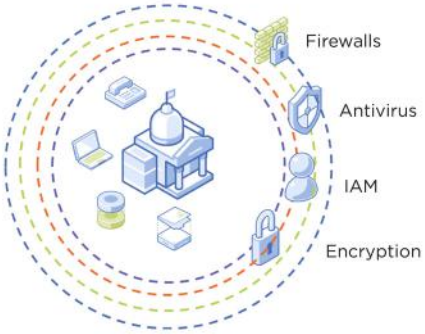
Nutanix and Zero Trust Architecture

Accelerate your alignment to NIST SP 800-207 Zero Trust Architecture

NIST SP 800-207
Zero Trust Architecture

The concept of trusted and untrusted networks was for years the basis of how we protected datacenter infrastructure. Like the analogy of a castle protected by a wide and deep moat, issues arise when the enemy can bypass perimeter protections since no other roadblocks exist to prevent their advance. Zero Trust Architecture (ZTA) was the solution developed to give greater protection to data given the disparate nature of IT infrastructure as it exists today. ZTA was ratified by the publication of NIST SP800-207, and further referenced in this NSA Cybersecurity Information sheet, plus the Presidential Executive Order released in May of 2021. The questions you may have on what does this all mean? And how will it affect your datacenter and application architecture going forward?

The NIST Special Publication for Zero Trust provides a high-level strategy for Government to Government (G2G) and Government to Business (G2B) enterprises to follow that have a mandate to ensure data protection and work on the premise that access to digital objects, like resources, data, and metadata, should never be implicitly granted but instead should be constantly and continuously evaluated to be appropriate.



This strategy moves the boundary of challenge response from a perimeter-based approach to an approach that is closer to the resource being accessed. But don't be fooled into thinking this simply addresses Identity and Access Management (IdAM) principals or network security best practices. It's a strategic document with considerations for how modern enterprises architect their IT, with public cloud utilization, app development, monitoring, and more. It also covers enterprise best practices regarding all data access methods from all source locations, users and even access by services.

Hybrid adoption of ZTA is likely to be common early on, where elements of ZTA are deployed piecemeal with a goal to transition the traditional approaches to security from perimeter-based protections to a more pervasive model that is resource or application centric.

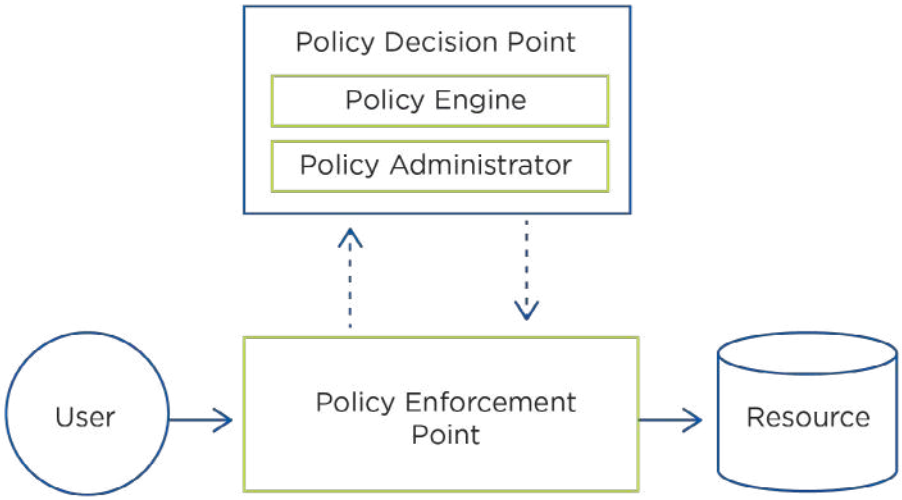
PE'S, PA'S PDP'S AND PEP'S

Policy Engine (PE), Policy Administrator (PA), Policy Decision Point (PDP), and Policy Enforcement Point (PEP). All sounds a bit complicated right? These four abbreviations are the cornerstone architectural aspects for ZTA enforcement.

Each of these logical components (PE, PA, PDP & PEP) can be satisfied by a singular process or technology for each function, different solutions working together for each function, or a single technology component that satisfies all functions of the security policy.

The parts combine to provide access based on business, process, and user need-to-know concepts. A Security **Policy Engine** works with a **Policy Administrator** to determine Authentication (AuthN) and Authorization (AuthZ) of an access request to a resource. These components live inside of a **Policy Decision Point** in the control plane. The **Policy Enforcement Point** is where the policy decision point action is applied in the data plane. The enforcement point can be in front of or at that resource being accessed.

Sometimes this process can be brokered by an "Agent" and a "Gateway," but ostensibly the goal is to prevent implicit trust to all resources simply because they reside within the same network. The notion that "just because you've connected to the VPN", should not mean you are able to access every resource. Trust should be established as close to the resource being accessed as possible, in every instance.



If you now expand this concept out to more than just network enforcement, and include service-to-service access requests you can see ZTA is more than just a simple guideline for enhanced network security.

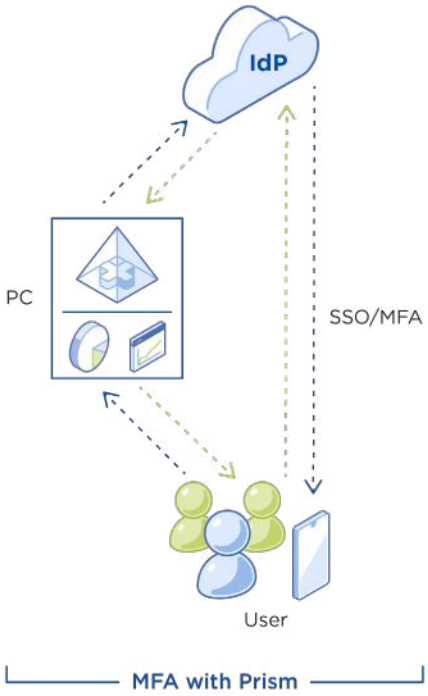
NIST SP800-53 Rev 4 Security & Privacy Controls for Federal Information Systems and Organizations

GET A HEAD START!

Nutanix can facilitate an easier transition to a ZTA future by providing the necessary foundation on which G2G and G2B enterprises can build their Hybrid Multicloud Infrastructure.

Beginning with a true cloud OS in Nutanix AOS, and the security enforcement, which was architected with ZTA concepts baked into its fabric. AOS is hardened out of the box with machine readable Security Technical Implementation Guides (STIGs), and maintains this security baseline by self-healing deviations or "drift" with a system wide Security Configuration Management Automation (SCMA) daemon.

With support for UEFI Secure boot for User Virtual Machines (UVM) and the Nutanix native hypervisor AHV, a circle of trust in the boot process can be established, preventing unverified implicit trust. AHV also receives the benefit of hardening out the box with STIGs aligned to NIST SP 800-53 Framework for Federal Information Systems, and maintains this secure state, again, with SCMA. Both AOS & AHV combine to provide an intrinsically (built-in) hardened, scalable, cloud OS solution for the modern hybrid datacenter.



MANAGING A ZTA SOLUTION:

The Nutanix cluster management interface, Prism, is where Zero Trust Architected applications can be built and monitored. From provisioning access control and advanced authentication such as MFA, to establishing software defined networking environments with lateral (East - West) stateful firewall protections, to managing PKI certificates, enabling cluster wide Data-at-Rest (DAR) encryption, as well as encryption for data-in-transit. All of this can be easily established, within minutes of standing up your cluster, in Prism.

Using third party Identity Providers (IdP) supporting Secure Authentication Markup Language (SAML) protocols can enable capabilities like Single Sign-On (SSO) and Multi-Factor Authentication (MFA) for Prism access, further enhancing IdAM controls.

MICROSEGMENTATION IS ZERO TRUST

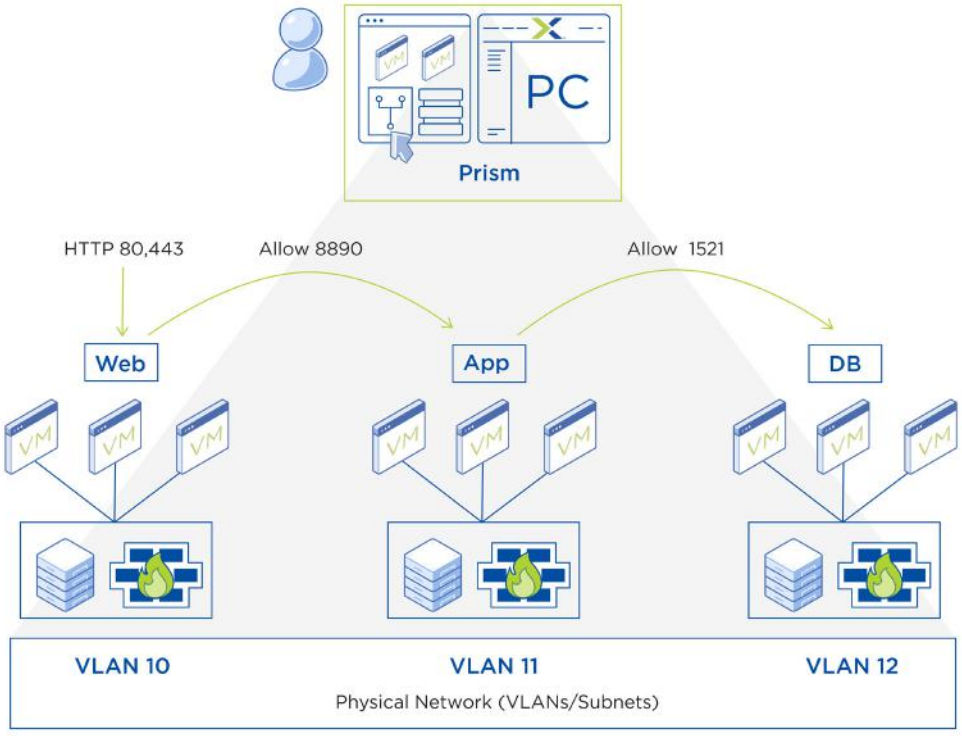
An obvious consideration for ZTA is in network isolation. Section 3.1.2 of the NIST SP800-207 discusses the process of enterprises using Microsegmentation as a design objective. The goal of ZTA is to move the challenge response activity from the perimeter to a more ubiquitous, enforcement process.

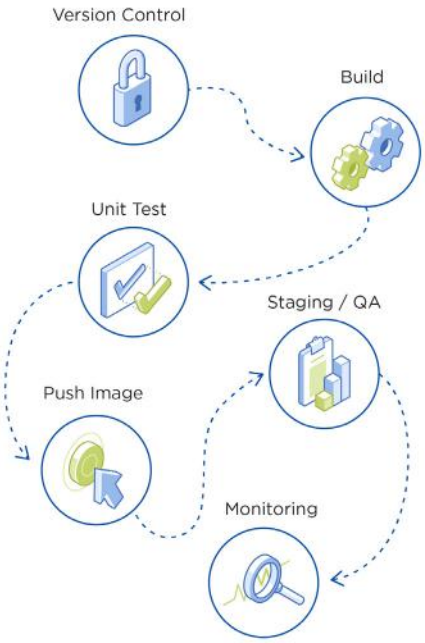
Nutanix Flow is a microsegmentation capability built right into AHV with no additional software to install on the endpoint. It can be activated and configured in minutes to act as a VM level firewall that can send event data about connections, act as a firewall that can enforce static trust boundaries where still required (such as only opening well known ports, or isolating completely, high security zones).

Next Generation Firewalls (NGFW) can further enhance the experience by providing those next gen networking capabilities but without the hindrance of hardware installations, delivered via Virtual Appliances (VAs); i.e. L7 deep packet inspection, IDS/ IPS, URL filtering, VDI protections, and more.

All of these advanced capabilities are monitored, with event logs able to be shipped to a syslog server integrating seamlessly with your existing Security Incident Event Management (SIEM) process.

All these activities don't further burden an already stretched Security team: security policies are set in Prism Central (a familiar interface), and they are applied to VMs using easy to understand metadata tags as "Categories" which lend themselves to the dynamic nature of cloud computing; new VMs are protected according to the category they have been allocated; and VMs are scaled or self-provisioned without infringement to the Operational Security (OpSec) of the enterprise.





DEVOPS & APPLICATION LIFECYCLE MANAGEMENT

Today, with the increased adoption of containerized applications, using technologies like Docker, Kubernetes (K8), alignment to frameworks like ZTA might seem antithetical to the goal of security due to a focus on availability and speed over constriction and confinement of sensitive resources. Also, with the ephemeral nature of containerized apps managing IAM and FW rules for these expansive, dynamic applications can seem daunting.

Adding to all this ambiguity is the lack of clear authority or guidance on how assessors are meant to measure this process in a security context.

To bake compliance directly into the development pipeline takes three elements:

1) A clear process for following a Security Development Lifecycle (SDLC) process, for developers, testers, QA etc.

2) Detailed auditing and reporting of all actions taken, both manual and automated.

3) A simple to use platform to allow for automation in application provisioning and scaling.

Setting this type of framework within the process is easy with Nutanix Calm, which is a multicloud application management framework that uses blueprints to automate lifecycle management. It is easier and gives a consistent repeatable approach to SDLC within a CI/CD pipeline. This also removes the potential for human error, which, if unchecked, could be multiplied across the environment when scaled.

For large environments, the ability for end users to self-provision resources, while maintaining the ZTA principles of “need-to-know” and ubiquitous security enforcement is also of concern. However, with Nutanix Calm, integration to tools such as Service Now as well as being able to tie into Prism security policies with Flow, dynamic application FW rules can be applied to these self provisioned environments, automating the security workflow.

Microservices and containers offer some unique characteristics that support security best practices,such as microservices emphasize an architecture with one function per service/ container; moreover, they also support a ZTA ethos by impermanence. Services can be spun up and wiped away relatively easily and at the requirements of the application, thus reducing the exploitable footprint of a threat vector.

STORAGE SOLUTIONS

The ability to control and monitor file-level access is very much in line with the principals of ZTA. As is the importance placed on data resiliency for hot and cold data. In the data-tiering process, with Nutanix Objects and its compatibility with S3 Object Lock specification, allowing for Write Once Read Many (WORM) effective ransomware storage protections are easily established.

Nutanix Files, for file-level storage, offers a rich auditing API, where applications can subscribe and receive real time notifications of file related events, such as creation, deletion, reading, permission changes etc.

Files Analytics (FA) is the Nutanix analytics dashboard used to consume these insights and further provide rich insights to the underlying data and user activity. FA receives all file activity for registered file server instances, this logging helps to form an audit trail so admins can review events on specific data and actions by specific users.

This dashboard of information shows capacity trending, data age, anomaly alerts, and permission denials (the last two specifically geared towards security vulnerabilities and powerful against the real time identification of malware or other spurious activity). Many more capabilities can deepen your understanding of user activity, identify "normal" behavior, and implement a Zero Trust policy with regard to file level access.

A HOLISTIC ZTA VISION

We've explored quite a few technologies and identified where Nutanix Hybrid Cloud can help facilitate a transition to establishing NIST SP 800-207 Zero Trust aligned architecture for the modern Hybrid Multicloud datacenter.

When being driven by mandates to adopt resources in the public cloud space, but logic dictates that many applications should remain protected in the private datacenter, it would be critical to maintain a uniform structure of Zero Trust to bridge those two environments with a single Cloud OS.

ABOUT NUTANIX

Our industry-leading Hybrid Multicloud platform enables military and government organizations to run their apps and workloads with unparalleled simplicity and performance in whichever cloud makes sense—private, public, or edge—that best supports operations, compliance requirements and their mission.

Nutanix products were tested and selected for inclusion on the Department of Defense Information Network (DoDIN) Approved products List (APL). https://aplits.disa.mil/processAPList.action.

The DoDIN APL certification along with four FIPS 140-2 certifications for cryptographic modules and the Common Criteria certification for AOS and AHV, demonstrates Nutanix's commitment to building in the necessary security functionality to our products.

NUTANIX™
YOUR ENTERPRISE CLOUD

T. 855.NUTANIX (855.688.2649) | F. 408.916.4039
info@nutanix.com | www.nutanix.com | @nutanix