TECHNOLOGY BRIEF

archTIS

MEETING THE US PRESIDENTIAL EXECUTIVE ORDER FOR ZERO TRUST

> *"To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks.and invest in both technology and personnel to match these modernization goals."*
>
> Executive Order on Improving the Nation's Cybersecurity

PRESIDENT BIDEN'S EXECUTIVE ORDER ON IMPROVING
THE NATION'S CYBERSECURITY

Executive Summary

With the new presidential cybersecurity Executive Order for Zero Trust issued for U.S. federal agencies to universally move to a zero trust architecture, agencies are scrambling to identify technologies to help them meet the new requirements. There's one caveat, traditional zero trust architecture addresses network and applications security, not the data that sits behind them. Without applying the same principles of zero trust to the data behind the network it protects, we're still in for the host of data breaches caused by what the security world calls 'insider threats'. The term covers everything from insider spies and moles deliberately leaking information or selling it to the highest bidder, through to negligent office workers leaving a laptop on a bus or sharing a file with the wrong email address.

Addressing The Zero Trust Blindspot

One way to address this zero trust blind spot to stop data loss from negligent and malicious insiders altogether is by using Attribute-Based Access Control (ABAC). ABAC extends the zero trust security model to the object level. Instead of being able to access a document on a server automatically because you are already authenticated into the system, it will instead determine whether you can access the file by evaluating attributes (or characteristics of data and/or users) to determine a given file's access, usage and sharing rights.

The advantage of a data-centric ABAC-based security approach is that an individual file's access rights can be dynamically adjusted based on the sensitivity of the file and the user's context in real-time to evaluate and validate each file's attributes. This includes security classification and permissions and attributes such as security clearance, time of day, location, and device type to determine who can access, edit, download, or share a particular file. Like Zero Trust network architecture, ABAC sets the default to deny access unless these attributes can be validated against business policies governing access and sharing conditions.

This level of granular, dynamic access control also provides additional benefits to the Defense and Intelligence community. A data-centric ABAC Security approach offers Defense and Intelligence agencies the ability to quickly and easily compartmentalized sensitive information, balancing the need-to-know principle with the need to share, whilst simply administrating the policies that control those communities of interest. It can also be applied to enterprise search tools and work flows to allow approved parties to identify information that may be of interest without revealing that information.

Finally, it enables information at different classifications to be hosted and accessed in a single data repository forming the foundation of Multi-Level Security (MLS) and Multi-Classified Networks. This provides the ability to integrate or reduce the number of air-gapped networks operating at different or varying levels of trust or classification. This is critical when speed, integrity and provenance of information is critical in its dissemination.

What is Multi-level security (MLS) and why is it important?

A security classification is the hierarchical category assigned to information and material that identifies the degree of damage that unauthorized disclosure or compromise would cause to a nation, generally regarding military or other government business. The classification denotes the degree of protection and control required for the storage, transmission, and utilization of the information.

Alongside security classification is a compartmentalization layer of separation and associated control requirements. Sometimes referred to as codeword, sensitive, compartmentalized, and can include releasability, caveats or rules around the sharing or dissemination of that information artefact.

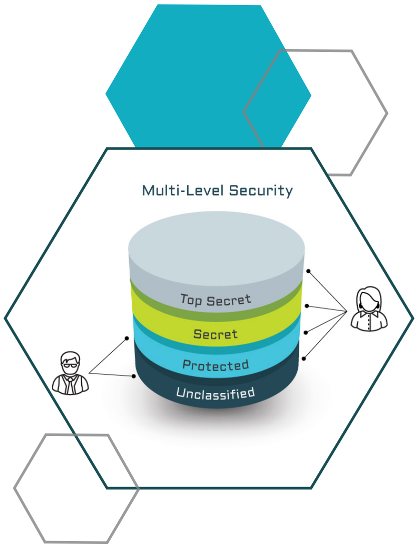
All systems have security boundaries, whether logical and enforced, or ephemeral and inadvertent. A security boundary naturally exists wherever two different "security domains" (which could be a set of security requirements, control objectives, or even handling characteristics) come together for some reason. It can be between classifications, between compartments, between organizations, between networks, between systems, or even between nations.

This sort of complexity means that we need the ability to measure and enforce contextual security, with rules or policies that are defined, required, and applied – also referred to as "dynamic policy enforcement" that can provide assurance which can be independently verified by a security assessor.

An MLS capability (system, platform, or environment) allows information at different classifications to be stored and accessed within a single security domain, while enforcing different access policies and compartments dynamically depending on context, with the assurance that the separation is effective.

MLS provides your organization with the ability to:

- Enable custodians to label and tag their content creations in the system.
- Controls and releases information to individuals/devices/locations that meet the contextual rules.
- Enables dynamic policy enforcement and access controls to information.



By adding controls like Attribute-based Access Control (ABAC), MLS becomes even more effective. When utilizing ABAC as the dynamic policy enforcement method you can provide granular access control at the most appropriate context and enforce the principles of zero trust at the data layer.

- Enforce contextual controls based on labels, tags, and other attributes.
- Enable granular controls to apply either between or inside security domains.

What are the benefits of combining MLS and ABAC for Zero Trust?

By adding controls like Attribute-based Access Control (ABAC), MLS becomes even more effective. When utilizing ABAC as the dynamic policy enforcement method you can control provide granular access control at the most appropriate context and enforce the principles of zero trust at the data layer.

These attribute controls can be expressed as a key=value pair (for example [Nationality=Australian], [Location=Canberra, Australia], or [Organization=archTIS]). By dynamically measuring the attributes of the user or device and aligning it to the rules of access for the information, ABAC can be an effective way to ensure only the right people, in the right context can get access to the information.

MLS combined with the dynamic capabilities of ABAC can enable and support complex information sharing challenges and offers several benefits to:

- Increase the accuracy, provenance and speed of getting the right information to the user, within multiple operational and security contexts.
- Improve access management of compartmentalized information, within contextual constraints.
- Assist to collapse networks and reduce the number of systems that users have to interact with, including potentially within deployed scenarios.
- Enable multi-national information sharing within mission related network environments, potentially improving interoperability and effectiveness.
- Enable files and documents to be rapidly created and shared respecting the security rules and set by the owner.

Fast Tracking Zero Trust Data Security to Comply with Mandates

archTIS develops and markets two products to ensure that classified and sensitive information are shared securely using ABAC and MLS to extend the zero trust security model to the data level.

NC Protect

archTIS also delivers dynamic data-centric security for Microsoft 365 applications (SharePoint, Teams, Office, OneDrive and Exchange). NC Protect automatically finds, classifies, and secures unstructured data on-premises/cloud/hybrid environments for all Microsoft environments and dynamically adjusts data access and protection based on real-time comparison of data and user attributes. To ensure that users view/use, and share files according to DOD/mission requirements, it uses a data-centric security approach that evaluates each file's attributes (security classification/permissions), user attributes (security clearance, time of day/location, device, etc.), to determine who is able access, edit, distribute, and download files for collaboration. NC Protect enables secure, distributed decision-making by applying zero-trust (ABAC) to any Microsoft collaboration/coalition environment.

Kojensi

Kojensi is a multi-level, information-sharing, and security platform, allowing joint/coalition partners to share/collaborate using classified information. This patented security platform uses ABAC to define the rules of who accesses information, under what conditions. Information is secured at the perimeter, and within the system. Kojensi keeps documents secure, from NIPR/TS/SCI, increases productivity across the workforce, allows users to collaborate securely, while being easy to use. Kojensi deploys on location/enterprise, cloud, or a field deployable appliance. Documents/file access is controlled by security classification/organization releasability, provides a suite of collaboration tools that dramatically improves productivity, real-time, and with partners from any service/country (i.e. JADC2/ABMS) based on mission/mission requirements.

Summary

The U.S. Executive Order on Zero Trust sets the path forward for government, defense and enterprises alike to protect against evolving cybersecurity threats. But, just as with any other methodology you need to address any gaps – in this case making sure you extend the same 'trust no one' ethos that is critical to its success down to the data itself and selecting the right technologies to implement it.

Contact archTIS to learn more about implementing ABAC and MLS based information protection.