

YOU[✓]ATTEST[®]

Identity Attestation
Automated and Simplified

<https://YouAttest.com>

YouAttest – Identity Attestation

- Formed Q4, 2019, First Customer, Q4, 2020
- 3.8 million attestations performed
- Focus: Simplifying identity recertification
- Markets: Healthcare, Financial, Insurance, Retail, Education
- Key customers: Guardant Health, Convex Insurance, Medline
Vituity, Mattel
- Cloud based: AWS Platform, SOC 2 Type II Certified
- Patented AI Zero Trust Score, 2024 (U.S. 12184,676 B2)

FACT:

**All organizations must know who has access to what
around sensitive information.**

REALITY:

**Outside of a few entities with teams of auditors,
very few know who has access.**

This is a problem.

YouAttest – Identity Attestation

- The fastest “Time to Value” Identity Governance product
 - Certifying **“Who has Access to What”**
- A **Zero-Code**, Ready-to-Attest cloud solution to:
 - Attest all identity resources in the enterprise
- **Governing:**
 - Who has access to sensitive data (PHI, PII, CUI)
 - Executing on the “Principle of Least Privilege”

Situation:

- DISA Next Strategy (FY 2025–2029) outlines Strategic Imperatives:
 - #1: Operate & Secure the DISA portion of the DoD Information Network
 - OP 1.1: Provide relevant, modern enterprise/business tools
 - OP 1.3: Manage the agency
 - #3: Optimize the network
 - OP 3.2: Divest technical debt
- DoD ICAM Reference Design & **DoDI 8520.04** mandates **access accountability (2.2.2), access review (2.2.2.2), privileged access (4.2.3)**, and closing capability gaps (C.2.2)
- DoDI 8520.04 §4.2.A(5) & DoDI 8530.01 §14.b require DISA to **operate, test, secure enterprise ICAM services**

Complication:

- Legacy tools **lack automation**; manual access reviews delay remediation and **increase risk**.
- The warfighter and DISA must **modernize Enterprise & Business Tools (OP 1.1)** while **reducing technical debt (OP 3.2)**, yet **ICAM compliance demands frequent attestation**.
- Without scalable solutions, DISA's agency-wide access governance and network hardening efforts are **at risk of stagnation**.

Questions:

How can YouAttest enable DISA and the warfighter to:

1. **Automate User Access Reviews (UARs)** to support ICAM accountability and privileged user logging (aligning with DoDI 8520.04 & ref-design 2.2.2)?
1. Modernize enterprise tools, **reduce audit friction**, and align with OP 1.1 + OP 3.2 (technical-debt divestment)?
1. Support agency management (OP 1.3) by **providing streamlined compliance reporting** and governance dashboards?

Solution:

- **Implement YouAttest's cloud-native UAR System for DISA**
- **Automated & policy-driven access reviews** (access accountability 2.2.2.2; privileged flow 4.2.3)
- **50-85 % faster review cycles**, reducing zombie accounts, license waste and over-privileged accounts
- **Zero-code, cloud-based deployment** – rapid modernization of enterprise tools supporting OP 1.1
- **Audit-ready reporting dashboard** for agency governance (OP 1.3)
 - Supports DoDI 8520.04/8530.01 requirements on secure ICAM service operation
- **Reduces legacy tool burdens** and accelerates technical debt divestment under OP 3.2



YouAttest Overview

CSF 2.0 PR.AA-05

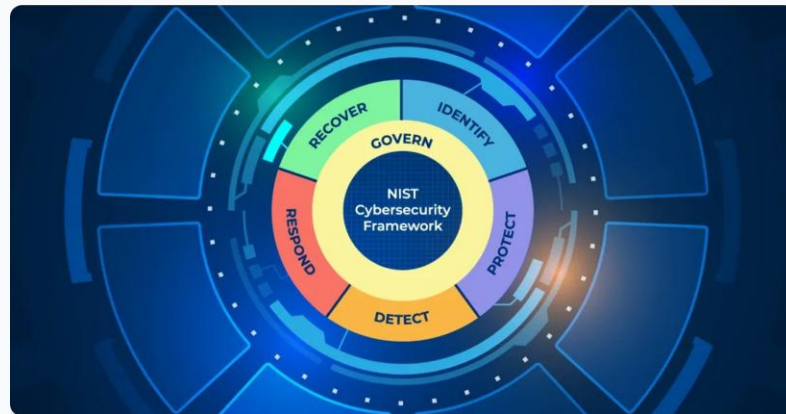
Identities and access must be reviewed

NIST 800-171: req 3.15; NIST 800-53: PR-AC-6

- ✓ **Example 1:** Review logical and physical access privileges periodically
- ✓ **Example 4:** Periodically review the privileges associated with critical business functions to confirm proper separation of duties

The **Principle of Least Privilege (PoLP)** is a fundamental concept in identity and cybersecurity.

It is outlined in NIST CSF 1.1 and 2.0, NIST SP 800-53 , NIST SP 800-171 and other NIST guidelines to ensure access to sensitive data, such as PHI, PII, **and CUI**, is restricted to the minimum necessary for authorized tasks.



Key Benefits of Access Reviews

- ✓ Reduced security risk
- ✓ Regulatory compliance
- ✓ Proper access control
- ✓ Audit evidence

User Access Reviews Required

Cyber Regulations by Industry



YouAttest allows enterprises to meet compliance for the following vertical markets:

| | | |
|-----------------|---|---------------------|
| Healthcare | ➔ | HIPAA/HITRUST |
| Finance | ➔ | FFIEC, GLBA |
| Insurance | ➔ | NAIC |
| Publicly Traded | ➔ | SOX 404B |
| IT Services | ➔ | SOC 2 Type 2 |
| Retail | ➔ | PCI-DSS |
| Defense | ➔ | CMMC, NIST 800-171 |
| International | ➔ | ISO/IEC 27001, GDPR |

Addressing the Identity Rights Gap Issue

YouAttest Automates:

Security

- **User Access Reviews**

- Applications, Groups, Users

- Discovers and Eliminates:

- **Ghost, Orphaned Accounts, Excess Privileges**

Governance

- Creates Identity Access review “evidence” (reports) for:

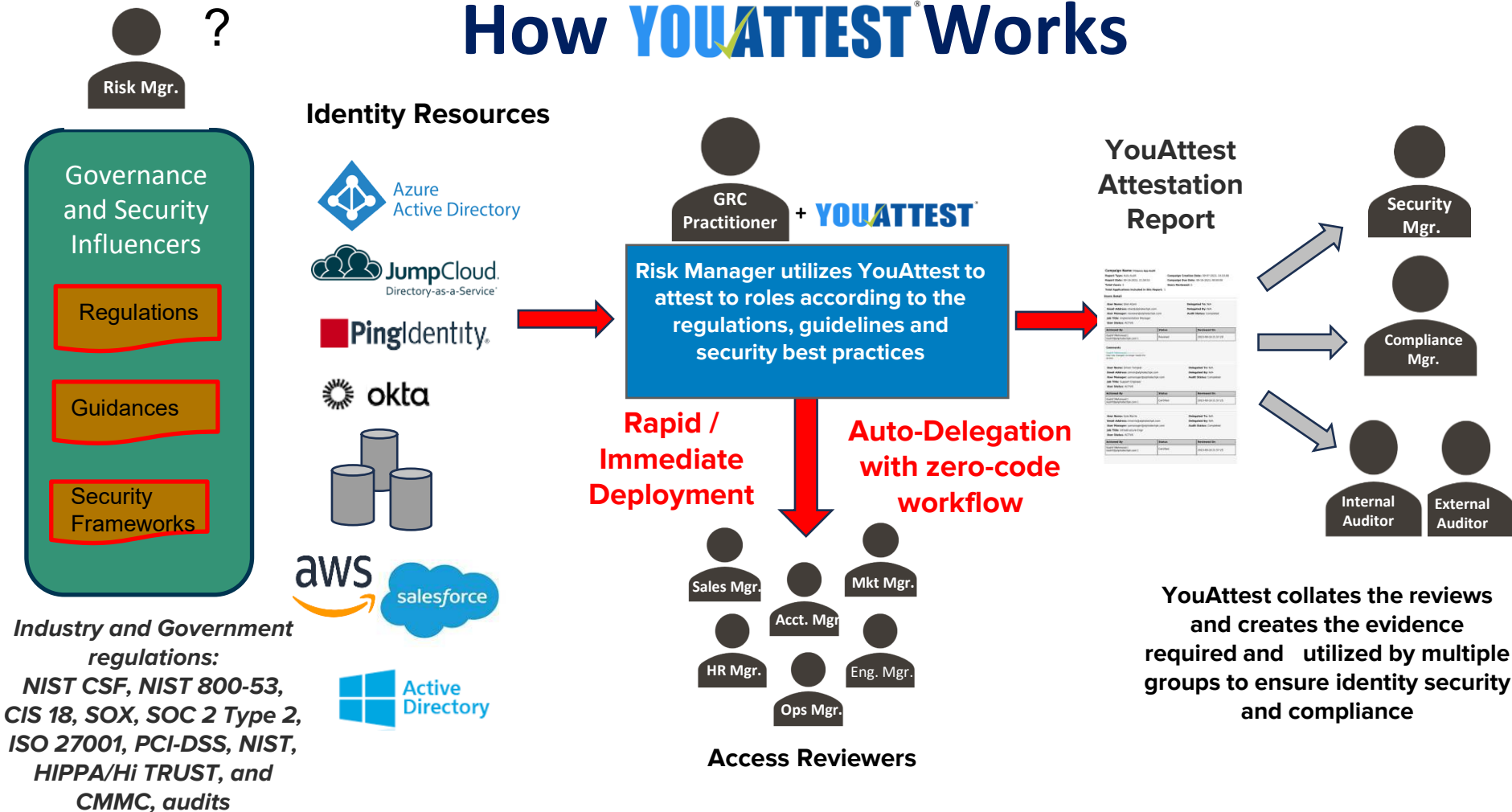
- **SOX, SOC 2 Type 2, ISO 27001, PCI-DSS, NIST, HIPAA/HITRUST, CMMC**

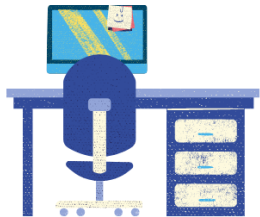
Big Differentiator:

Integration & AI

- **Rapid Integration** to all resources: AD, Entra ID, Okta, Salesforce, AWS, JumpCloud, & API and generic uploads
- Built-in SSO for complete and accurate identity reviews
- **AI Based “Identity Trust” Risk Score**

How YOUATTEST® Works





YOUATTEST® vs Manual



Access Review Action:

- Export to CSV or import from SSO tool
- Identity Managers
- Create separate attestations per manager
- Send attestations to managers
- 1st line Managers delegate to 2nd line
- Enable YouAttest multiple reviewers
- Mgr. conducts review verifying role info (per review)
- Nag emails/reminders
- Collate/Format reports to single view
- Reports in centralized, cloud repository
- **Repeatable**

YouAttest:

0.5 -1 hr.
Auto
Auto
Auto
30 mins
Auto
0.5 – 2 hrs.
Auto
Auto
Auto
Yes

Manual:

1 hr.
2-4 hrs.
4-12 hrs.
2-4 hrs.
12 hrs.
4-12 hrs.
4-12 hrs.
2-10 days
4-12 hrs.
4-12 hrs.
No

4-12 hrs.

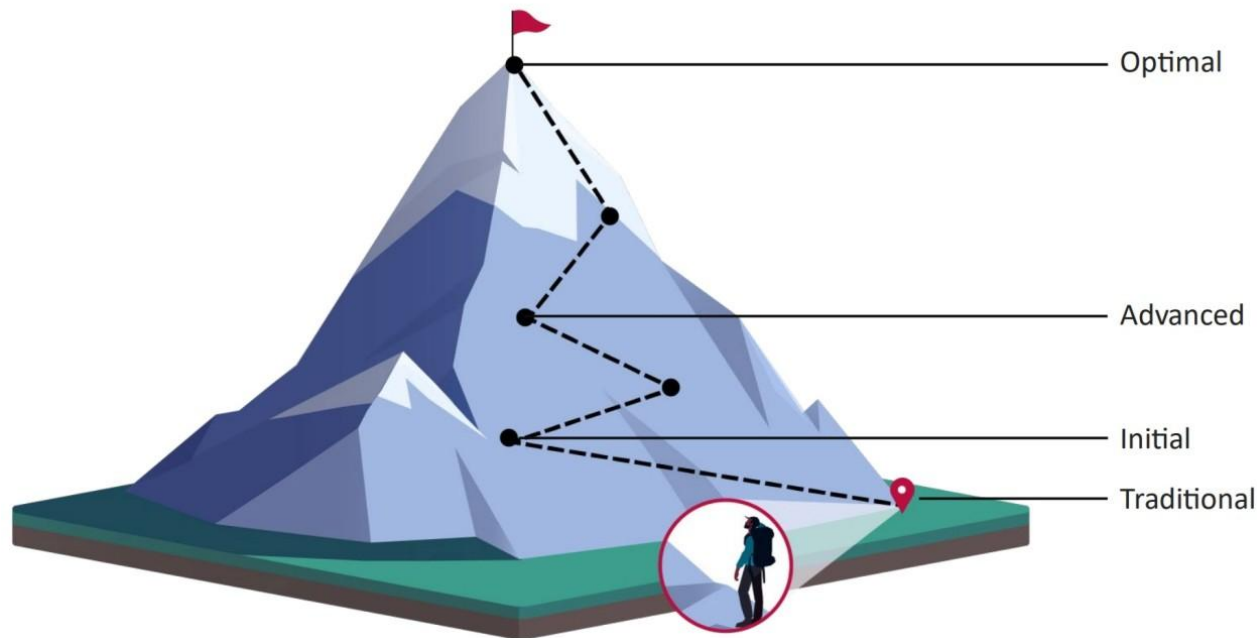
5-14 days

The CISA Zero Trust Maturity Model

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

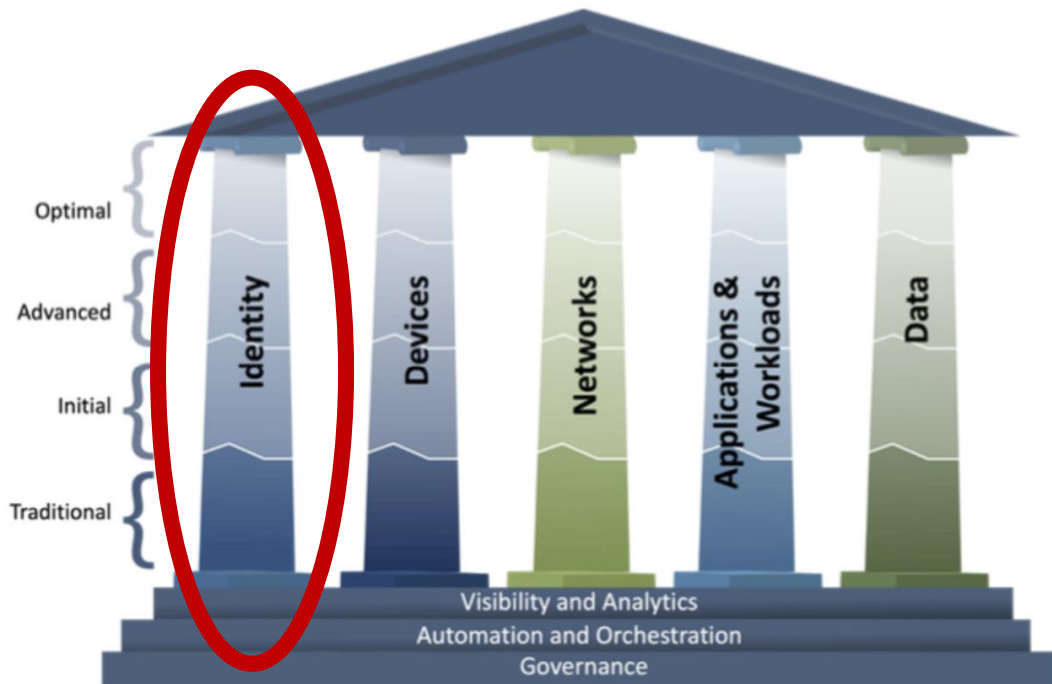


Zero Trust Maturity Journey



The CISA Zero Trust Maturity Model

https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf



Source: CISA Zero Trust Maturity Model, Figure 3

The ZTMM Explained for IGA / YouAttest

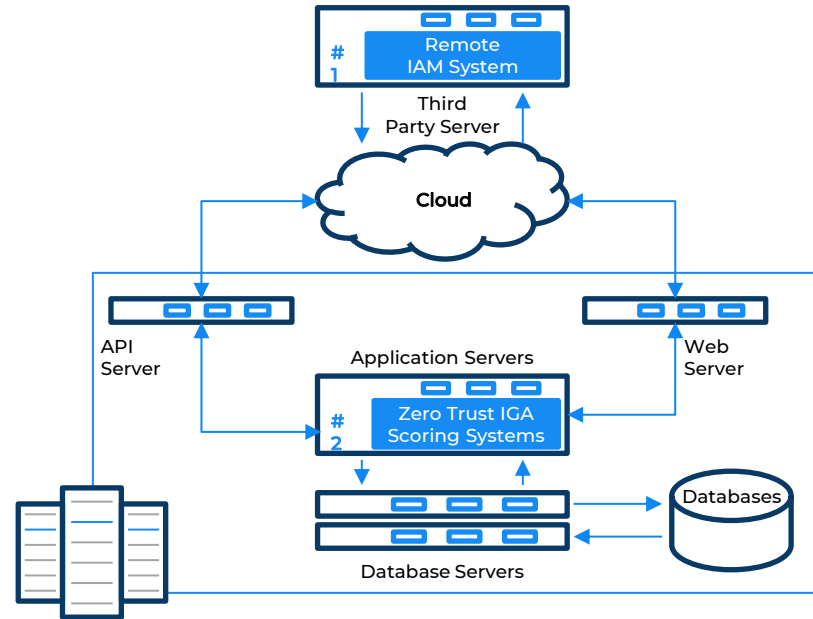


| State | Traditional | Initial | Advanced | Optimal |
|--|-----------------------------------|--|---|--|
| The ZTMM Theory: | How enterprises are working today | First Step to Zero Trust – Automation is key | Intelligence Becomes part of tools | Intelligence is fed back into all secured transactions |
| What it means for IGA – Identity re-certification | E-mails, Spreadsheets, manual | Automate the access review process through tools | Immediate review of key changes in “material” components. Begin intro of scores | Full use of Realtime IGA score fed back into transaction authorizations |
| YouAttest | N/A | Automated User Access Reviews | Triggers, YouAttest ITS (Identity Trust Score) information | YouAttest ITS score fed back into transaction authorization in real time |

YouAttest “Zero Trust” Identity Confidence Score

- Solution Utilizes existing IAM technology
 - Azure AD, Okta,
 - Utilizes existing YouAttest SSO and Data collectors
- **Identity Threat Detection & Response**
 - YouAttest is able to create a identity confidence score that helps enterprises identify over-privileged and low confidence identities.
- **KRI – Key Risk Indicator**
 - YouAttest displays the score to help enterers determine which identities are at risk.

#1 IAM solution (Azure AD, Okta, etc.)
#2 YouAttest Identity Confidence Score



4346.008US1 - IAM Endpoint API Collection for Zero Trust Score System

The Model:



An unsupervised learning to understand user group inside and environment, find natural underlying structure of user using clusters.

In Detail:

1. Identify over-privileged users
(via group anomalies)
2. S.o.D. score (Segregations of Duties)
3. Last time user has been reviewed

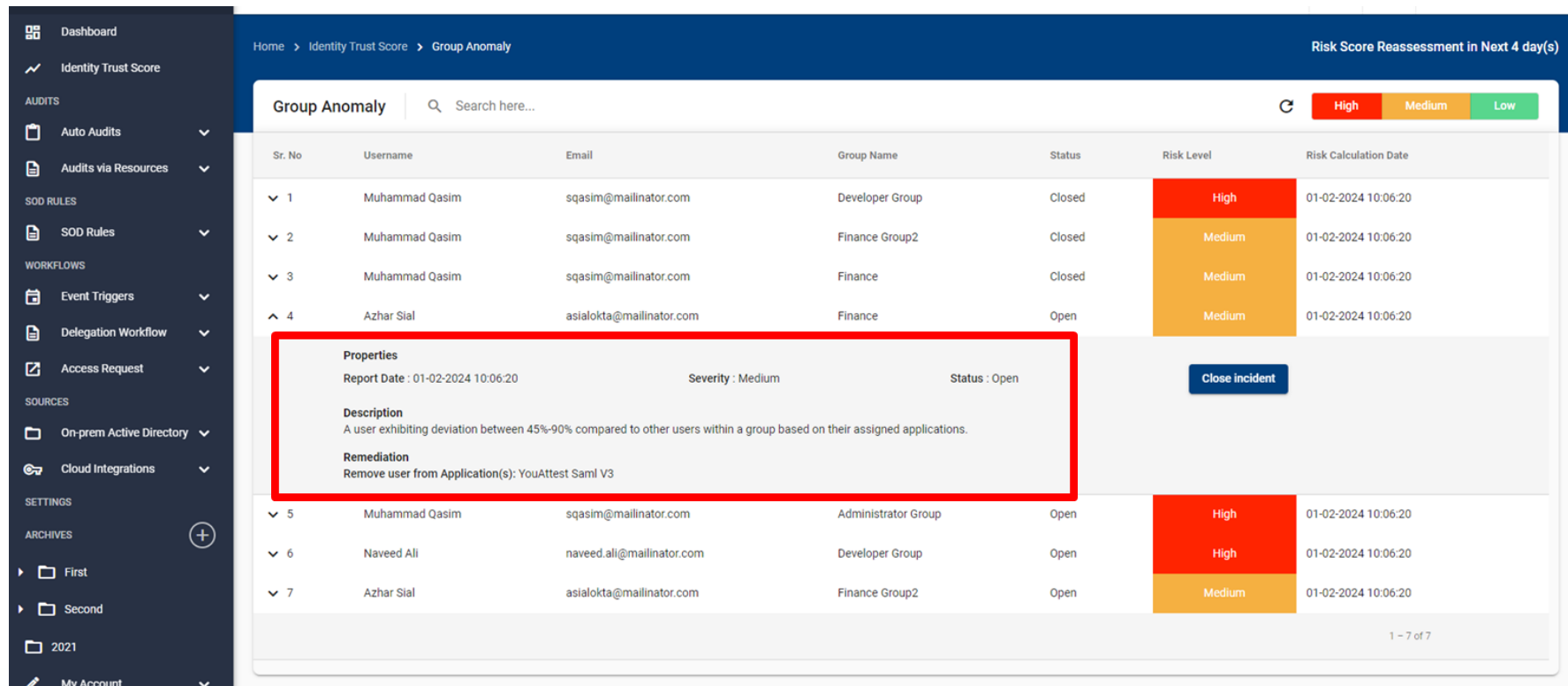
The Result:

A real time identity trust score for use in data, application and network access.

Key Differentiator

YouAttest factors the last time this account has been reviewed for access rights

YouAttest “Zero Trust” Identity Confidence Score



Dashboard

Identity Trust Score

AUDITS

- Auto Audits
- Audits via Resources

SOD RULES

- SOD Rules

WORKFLOWS

- Event Triggers
- Delegation Workflow
- Access Request

SOURCES

- On-prem Active Directory
- Cloud Integrations

SETTINGS

ARCHIVES

- First
- Second
- 2021
- My Account

Home > Identity Trust Score > Group Anomaly

Risk Score Reassessment in Next 4 day(s)

Group Anomaly

Search here...

High Medium Low

| Sr. No | Username | Email | Group Name | Status | Risk Level | Risk Calculation Date |
|--------|----------------|---------------------------|---------------------|--------|------------|-----------------------|
| 1 | Muhammad Qasim | sqasim@mailinator.com | Developer Group | Closed | High | 01-02-2024 10:06:20 |
| 2 | Muhammad Qasim | sqasim@mailinator.com | Finance Group2 | Closed | Medium | 01-02-2024 10:06:20 |
| 3 | Muhammad Qasim | sqasim@mailinator.com | Finance | Closed | Medium | 01-02-2024 10:06:20 |
| 4 | Azhar Sial | asialokta@mailinator.com | Finance | Open | Medium | 01-02-2024 10:06:20 |
| 5 | Muhammad Qasim | sqasim@mailinator.com | Administrator Group | Open | High | 01-02-2024 10:06:20 |
| 6 | Naveed Ali | naveed.ali@mailinator.com | Developer Group | Open | High | 01-02-2024 10:06:20 |
| 7 | Azhar Sial | asialokta@mailinator.com | Finance Group2 | Open | Medium | 01-02-2024 10:06:20 |

Properties
Report Date : 01-02-2024 10:06:20 Severity : Medium Status : Open [Close incident](#)

Description
A user exhibiting deviation between 45%-90% compared to other users within a group based on their assigned applications.

Remediation
Remove user from Application(s): YouAttest Saml V3

1 - 7 of 7

YouAttest in Comparison to Competition – Customer Review

Access Review Platforms

| | |
|--|--|
| Option 1. Microsoft Azure Access Reviews (E5 is a Pre-Requisite) | Most painful option. Fully automatable. |
| Option 2. YouAttest Access Review Platform | Most cost effective option. Fully automatable. |
| Option 3. Vanta Platform Compliance Platform | Access Reviews Are Not Automatable. |
| Option 4. Drata Platform Compliance Platform | Access Reviews Are Not Automatable. |
| Option 5. Gathid Access Review Platform | Access Reviews Are Not Automatable. |
| Option 6. Okta Platform (Includes Access Reviews) | Most expensive option. Most features. |
| Option 7. Quest One Identity | Heavily focused on provisioning and identity. |

YouAttest is Built For Multi-Tenant Management

Direct

One Agency

Single Customer
Tenant



GRC Service Agency

Cust. #1

Cust. #2

Cust. #3

**Single Mgmt Console
(GRC / Audits)**









On-Demand Reviews



YOUATTEST

YouAttest MSP Offering is ideal for the e-ICAM solution

Competitors/Alternatives

| Competitor Segment | Legacy IGA Products | IAMs | GRC Dashboards | Spreadsheets |
|----------------------|--|---|---|--|
| Products |   |   |    |  |
| UAR Support: | Add On | Add-On | Add-On or NOT Available | Manual, Ad-Hoc |
| Key Weaknesses | <ul style="list-style-type: none"> • Complex 12-24 months to deploy • OpEx: 100x Deploy \$ • CapEx: 25x License \$ | <ul style="list-style-type: none"> • Incomplete • Not designed for non-IAM integrated resources • Poor reported workflow | <ul style="list-style-type: none"> • Incomplete • Either poor or limited UAR support • Not all identity resources | <ul style="list-style-type: none"> • Unreliable • 60% <u>error</u> rate • Slow, unreliable |
| MSP Story | <ul style="list-style-type: none"> • Not Realistic, Requires License/Deployment per site | <ul style="list-style-type: none"> • Not Designed for full identity audits • Leaves MSPs to do manual audits for IAM gaps | <ul style="list-style-type: none"> • No Pay-as-Go UAR Usage model for MSPs | <ul style="list-style-type: none"> • Not a reliable practice for MSPs |
| YouAttest Advantage: | UARs (User Access Reviews) for All-Sized Enterprises | YouAttest is ONE tool for all identity UARs – not just IAM resources. | YouAttest is a complete UAR solution. Output exported to these tools. | YouAttest is ideal improvement over manual processes |

Questions & Discussion

YouAttest

info@youattest.com

877.452.0496

<https://youattest.com>





Backing Materials

**YouAttest mapped to key
D.o.D. mandates, frameworks,
guidances and controls**



DoD INSTRUCTION 8520.03

IDENTITY AUTHENTICATION FOR INFORMATION SYSTEMS

DoD Instruction 8520.03

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf>

| Phase | Section | Control Description | How YouAttest Helps |
|---|---|--|---|
| Risk Management and System Owner Responsibilities | Section 1.2 (Policy) | Requires information system owners to evaluate risks to determine and document authentication requirements for their systems, in accordance w/ DoDI 8510.01 (Page 5) | System owners must assess and manage access risks, which include reviewing entitlements to ensure they align with current security priorities |
| DoD Component Responsibilities | Section 2.8 (OSD and DoD Component Heads) | Mandates that DoD Components establish governance for identity, credentialing, and authentication. This includes integrating with DoD enterprise ICAM services and ensuring compliance with authentication policies. | All systems must meet the DoD mandates on identity governance, which means entitlements must be reviewed. |
| Define Roles & Responsibilities | 3.2 (General Authentication) | Information systems must authenticate all entities using approved credentials before granting access to resources (Page 18) | Approved credentials are reviewed and approved accounts. |

| Phase | Section | Control Description | How YouAttest Helps |
|---|-----------------------------------|---|---|
| Credential and Authentication Management | Section 3.5 (CSP Requirements) | CSPs are responsible for credential maintenance, involving updating and based on changes in user roles and access needs (Page 31) | UARs verify that only appropriate identities have access. |
| Identity Provider (IdP) and Security Auditing | Section 3.6 (IdP Requirements) | CSPs are responsible for credential maintenance, involving updating and based on changes in user roles and access needs (Page 31) | IdPs need be reviewed, including entitlements granted. |



DoD INSTRUCTION 8520.04

ACCESS MANAGEMENT FOR DoD INFORMATION SYSTEMS

DoD Instruction 8520.04

<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852004p.pdf>

DoD Instruction 8025.04

| Section / Ref | Control Description | How YouAttest Helps | Notes / Rationale |
|---------------------------------|--|--|---|
| 2.2.2 – Accountability | DoD Components must ensure traceability of identity lifecycle events (provisioning, use, deprovisioning), especially for privileged access and system changes. | YouAttest creates auditable reports of access reviews (UARs), supporting lifecycle traceability from assignment to revocation. | Enforces identity traceability across systems, meeting audit and accountability needs. |
| 2.2.2.2 – Access Review | Identity data, group memberships, and access privileges must be reviewed periodically to confirm appropriateness. | YouAttest automates periodic User Access Reviews (UARs) to validate access assignments across systems. | Directly satisfies this control by enabling repeatable, documented access certifications. |
| 4.2.3 – Privileged Access | Organizations must identify, authorize, and review elevated access to ensure only authorized users perform privileged functions. | YouAttest enables tagging and tracking of privileged accounts, supports targeted attestations for elevated access. | Aligns with least privilege principle and enforces privileged access governance. |
| C.2.2 – Closing Capability Gaps | Gaps in identity governance must be identified and remediated, especially where manual, ad hoc, or legacy methods are in use. | YouAttest replaces spreadsheets/manual tools with automated workflows, enabling remediation of process gaps. | Facilitates modernization and gap closure in legacy IGA practices. |



CLEARED
For Open Publication

May 30, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Continuous Authorization to Operate (cATO) Evaluation Criteria

Continuous Authorization to Operate (cATO)

<https://dodcio.defense.gov/Portals/0/Documents/Library/cATO-EvaluationCriteria.pdf>

Continuous Authorization to Operate (cATO)

| Phase | Section | Control Description | How YouAttest Helps |
|--|---|--|--|
| Appendix D: 1.0 Continuous Monitoring | Business Rules (Page 11): | <ul style="list-style-type: none"> - <i>"Define and assign cybersecurity roles and responsibilities."</i> - <i>"Identify, assess, prioritize, and share risk information in real time."</i> | Associates must both have access to reviews of entitlements and be able to execute these reviews on an ongoing basis. |
| Appendix D: 3.0 Secure Software Supply Chain (SCCS) and DevSecOps | Cloud Native Application Protection Platform (CNAPP): | "Cloud Infrastructure Entitlement Management (CIEM) for management of access rights, permissions, or privileges for the identities of a single or multi-cloud environment." | CIEM involves periodic validation of identities and their associated permissions to ensure least privilege and compliance, which is a core component entitlement data reviews. |
| Appendix D: 3.3 Authorize the People | Verification of Training and Roles | <ul style="list-style-type: none"> - <i>"Provide an organization chart showing the roles within the DSO Team."</i> - <i>"Demonstrate appropriate separation of duties and least privilege are applied to all personnel."</i> | YouAttest Users Access Reviews automate the process of role review and automate Segregation of Duties evaluations. |

Continuous Authorization to Operate (cATO)

| Phase | Section | Control Description | How YouAttest Helps |
|--------------------------|---------|--|--|
| Insider Theat Monitoring | Page 17 | <ul style="list-style-type: none"> - <i>"The below concepts can be used to protect against insider threats: Separation of Duties, Paired programming, Least privilege management with respect to containers/cloud environments,</i> | <p>YouAttest provides an automated process to ensure users are removed from resources - identifying ghost/orphaned accounts and enacted S.o.D. rules</p> |

NIST

800 - 53

"Security and Privacy Controls for Information Systems and Organizations"

NIST 800-53

<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

Regulations - NIST 800-53 | FedRAMP

| Description | 800-53 Control ID | YouAttest | FedRAMP | | |
|---------------------------------------|-------------------|---|---------|-----|------|
| | | | Low | Mod | High |
| Account Management | AC-2 | Automates the UAR process to ensure group and role-based access is set up properly. | y | y | y |
| Access Enforcement | AC-3 | Allows for access revocations. | y | y | y |
| Separation of Duties | AC-5 | Helps manage groups and roles to enforce the separation of duties. | | y | y |
| Least Privilege | AC-6 | Automates the UAR that is done to verify least privilege is in-place. | | y | y |
| Remote Access | AC-17 | Can help ensure remote access group and role-based privileges are set properly. | y | y | y |
| Auditable Events | AU-2 | Offers attestation of assigned user privileges. | y | y | y |
| Audit Review, Analysis, and Reporting | AU-6 | Creates the audit evidence required by regulations. | y | y | y |
| Protection of Audit Information | AU-9 | Helps protect audit information by managing group and role-based access to this data. | y | y | y |
| Audit Generation | AU-12 | Can show if group and role changes have been made since the previous audit. | y | y | y |

Regulations - NIST 800-53 | FedRAMP



| Description | 800-53 Control ID | YouAttest | FedRAMP | | |
|--------------------------------|-------------------|---|---------|-----|------|
| | | | Low | Mod | High |
| Continuous Monitoring | CA-7 | Contributes to continuous monitoring efforts through UARs. | y | y | y |
| Access Restrictions for Change | CM-5 | Helps manage group and role-based accesses for personnel authorized to make changes. | y | y | y |
| Least Functionality | CM-7 | Assists in enforcing least privilege by conducting automated UARs. | y | y | y |
| Configuration Change Control | CM-12 | Helps manage group and role-based access for personnel authorized to make changes. | | y | y |
| Nonlocal Maintenance | MA-4 | Provides a method to manage group and role-based access for nonlocal maintenance. | y | y | y |
| Maintenance Personnel | MA-5 | Provides a method to manage group and role-based access for maintenance personnel. | y | y | y |
| Media Access | MP-2 | Helps control group and role-based access to group policy privileges used to enable or disable the use of external media. | y | y | y |
| Physical Access Controls | PE-2 | Indirectly supports physical access control through managing electronic access. | y | y | y |
| Personnel Termination | PS-4 | Assists in revoking access privileges during the personnel termination process. | y | y | y |

| Description | 800-53 Control ID | YouAttest | FedRAMP | | |
|--|----------------------|--|---------|-----|------|
| | | | Low | Mod | High |
| Personnel Transfer | PS-5 | Helps track and manage privileges as part of the personnel security process. | y | y | y |
| Personnel Screening | PS-7 | Assists with managing privilege changes related to the screening process. | y | y | y |
| Authority to Process Personally Identifiable Information (PII) | PT-2 | Helps manage group and role-based access to PII. | | | |
| Application Partitioning | SC-2 | Provides a method to manage group and role-based access to each application. | | y | y |
| System Monitoring | SI-4 | Supports system monitoring of groups and roles between one audit and the next. | y | y | y |



"Cybersecurity Framework 2.0: A Framework for Managing Cybersecurity Risk"

NIST CSF 2.0

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

| UAR Lifecycle Phase | NIST CSF 2.0 Control | Control Description | How YouAttest Helps |
|-------------------------------------|----------------------|---|--|
| Define Roles & Responsibilities | GV.RM-03 GV.SP-01 | Roles and responsibilities are clearly defined and aligned internally and externally. | UARs validate that role/group assignments align with responsibilities. |
| Access Governance & Risk Management | GV.RM-01 GV.RM-02 | Risk processes address identity-related risks and governance structures. | Access reviews provide visibility into group and role risk. |
| Issue & Manage Credentials | PR.AA-01 | Identities and credentials are issued, managed, verified, and audited. | UARs verify that only appropriate identities have access. |
| Enforce Least Privilege & SoD | PR.AA-02 PR.AA-05 | Access is managed using least privilege and separation of duties. | UARs enforce and validate these principles through reviews. |
| Control Remote Access | PR.AA-03 | Remote access is managed according to policies. | UARs ensure proper privileges for remote access users. |

| UAR Lifecycle Phase | NIST CSF 2.0 Control | Control Description | How YouAttest Helps |
|--------------------------------|----------------------|---|---|
| Monitor for Changes | DE.CM-04 | Personnel activity is monitored for unauthorized access or changes. | UARs identify changes in group/role membership since last review. |
| Audit & Accountability | PR.AU-01 | Audit logs are maintained and reviewed per policy. | UARs generate logs and audit trails for identity governance. |
| Deprovisioning | GV.WM-01 | HR practices include deprovisioning (e.g., employee offboarding). | UARs help ensure timely revocation of access for departed users. |
| Access to Sensitive Data | PR.DS-01 | Data-at-rest is protected through access controls. | UARs confirm that only authorized roles have data access. |
| Configuration & Change Control | PR.CM-01 PR.CM-02 | Access to system configuration is limited to authorized personnel. | UARs validate that only correct personnel have elevated privileges. |