Accenture Federal Services | servicenow

Assessing Security with Zero Trust 360°

Today's security landscape requires agencies to view threats in a more holistic way to mitigate risks to organizational assets. Zero Trust is a proactive security approach that emphasizes continuous monitoring and risk-based access controls. The Zero Trust Security Framework assumes that these **security risks can come from both inside and outside of an organization's perimeter**. Shifting to this model requires visibility into the readiness of the environment, prioritization areas, and guidance for managing the ecosystem once Zero Trust is in place.

Accenture's Zero Trust Maturity Model

Accenture has defined a Zero Trust Maturity Model based on the combined Cybersecurity and Infrastructure Security Agency (CISA) 2.0, Department of Defense (DOD), and National Institute of Standards and Technology (NIST 800-207) Zero Trust frameworks and architectures. This model, built on the pillars described on the next page, helps agencies understand their Zero Trust maturity and identifies gaps that need to be addressed.

Why Zero Trust?

Due to Executive Order 10428, the US federal government is prioritizing strengthening cybersecurity with a move towards a mature Zero Trust Architecture (ZTA).

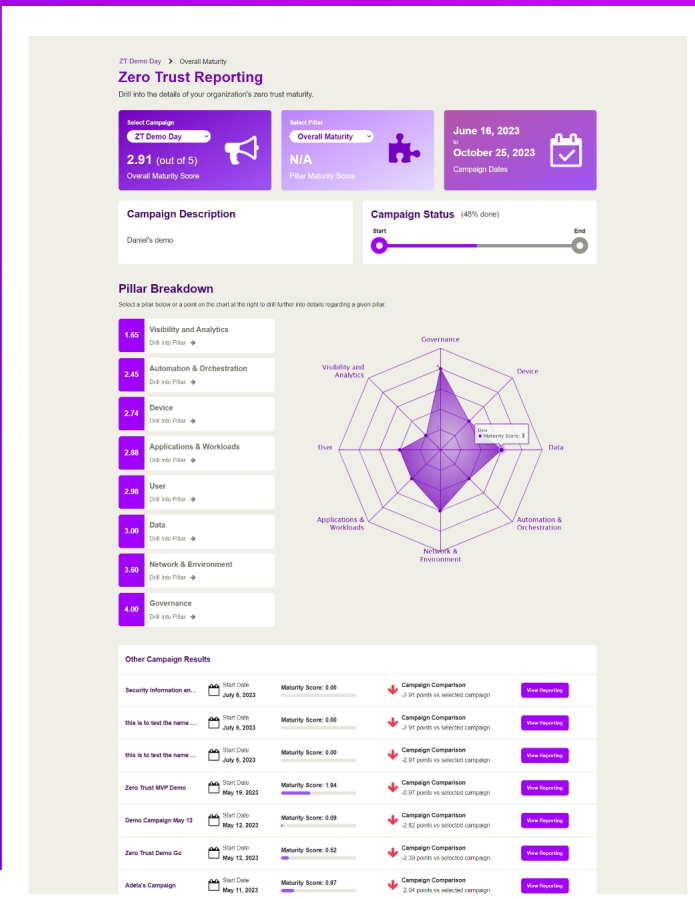
Traditional security relies on perimeter defense but is outdated in today's dynamic IT landscape.

Hackers and cyber threats are more sophisticated and complex, making traditional security insufficient.

Zero Trust is a proactive, holistic security model that continuously monitors all people, processes, and systems.

Pillars of Zero Trust

- **Identity:** Strong identity verification, credential management, and access controls.
- **Devices:** Protecting devices, such as laptops, mobile phones, and IoT devices.
- **Networks:** Securing network traffic and detecting abnormal behaviors.
- **Applications & Workloads:** Defensive coding practices, application vulnerability testing, and container security.
- **Data:** Robust encryption, data loss prevention, and access controls.



Our Zero Trust Assessment: ZT360

Using the Accenture Zero Trust Maturity Model, we have developed Zero Trust 360° (ZT360), a comprehensive security assessment powered by ServiceNow.

ZT360 evaluates an organization's security posture by assessing every component of the model to produce a ZT Maturity Score.

This score helps organizations understand their current maturity level and provides a baseline for measuring progress.

The assessment also generates a tailored ZT Strategic Planning Roadmap that prioritizes security solutions, technology upgrades, and process improvements to help organizations achieve optimal Zero Trust maturity.

What's Next?

Defining a Goal

Evaluate the agency's current security posture and visualize the steps needed to achieve a ZTA that complies with Executive Order 10428.

Developing and Executing a Framework

Determine and prioritize Zero Trust maturity recommendations by using our ZTA Assessment Framework.

Optimizing an Established Infrastructure

Assess the agency's current ZT Strategic Planning Roadmap to continue tracking and enhancing Zero Trust maturity.

Contact

Will Coffey | Senior Manager, Platforms
Gino Sferra | Managing Director, Platforms
Accenture Federal Services
digital.platforms@afs.com