maximus

Implementing Zero Trust Architecture to Improve Cybersecurity Defenses at the IRS

The Internal Revenue Service (IRS) processes sensitive personal data and taxpayer information for millions of Americans each year. The agency must continuously safeguard this data, in addition to maintaining the availability and security of critical IRS IT systems, applications, and infrastructure. Working with Maximus, the IRS successfully transitioned to a Zero Trust Architecture (ZTA), significantly improving cybersecurity posture across the agency.

Challenge

In its journey to ZTA, the IRS encountered challenges in technology, processes, and culture. While the agency's IT infrastructure had been maintained, many of its decades-old legacy systems were not designed with modern cybersecurity principles in mind. In addition, change management processes needed expansion to introduce cyber modernization plans that would mitigate disruption to processes that support the agency's core activities of processing taxpayer information. Finally, internal culture change was needed to instill a higher level of cyber savviness and a security mindset across the agency – enabling adoption of repeatable and enforceable security processes and a comprehensive understanding of security vulnerabilities.

Approach

Starting with a thorough assessment of the IRS's existing network infrastructure, Maximus worked closely with agency stakeholders to identify potential vulnerabilities and areas for improvement as part of a comprehensive ZTA strategy. This ensured that the resulting strategy not only aligned with the

Services Provided:

- Comprehensive and tailored Zero Trust Architecture strategy
- Deployment of DHS's Continuous Diagnostics and Mitigation Program (CDM)
- Information security continuous monitoring
- Cybersecurity risk assessments
- Development of incident response dashboards
- Advanced identity and access management, network segmentation, and security analytics
- Development of comprehensive incident response plans
- Design of cybersecurity training and awareness programs

Success Achieved:

- Reduced attack surface across the agency's networks
- Significantly improved security defenses and network visibility
- Improved incident response capabilities
- Improved FISMA compliance
- Alignment with the 2021 Executive Order on Cybersecurity
- Improved cybersecurity mindset and stakeholder involvement

agency's specific needs but that it also maximized the IRS's security, efficiency, and adaptability to the evolving cyber threat landscape.

Improving security processes and compliance

Key to the ZTA transition, Maximus experts applied the Continuous Diagnostics and Mitigation (CDM) Program established by the Department of Homeland Security (DHS) to lay the groundwork for modern tools, integration services, and dashboards that improve IRS security processes and provide deeper insight to:

- Reduce agency threat surface
- Increase network and security posture visibility
- Improve Federal Information Security Modernization Act (FISMA) reporting and compliance

Maximus also implemented process improvements and support for continuous monitoring, risk assessments, and cyber threat response capabilities using dashboards – all instrumental in adhering to ZTA principles.

Leveraging modern technology to address security gaps

Our experts deployed advanced solutions and technologies, including identity and access management; robust network segmentation; security analytics; and continuous monitoring of network traffic, user behavior, and system logs. These capabilities enable the agency to:

- Ensure that only authorized personnel can access sensitive systems and data
- Isolate potential attacks and prevent them from gaining access to the entire network
- Detect and respond to threats in real time

> *"[The IRS] is already well underway in the world of Zero Trust Architecture implementation for sure."*
>
> – Jena Whitley, Director of Enterprise Services, U.S. Treasury Inspector General for Tax Administration [Federal News Network, Federal Insights, October 2023]

Instilling culture change and cyber savviness

To increase the agency's cybersecurity mindset overall, Maximus worked closely with IRS stakeholders to conduct extensive employee training and awareness programs. This comprehensive education on the principles and benefits of ZTA helped to:

- Mitigate any internal resistance to new processes and tools
- Empower employees to actively participate in maintaining a more secure IRS enterprise
- Provide personnel reporting tools to enable prompt alerts to any suspicious activities

Maximus also worked alongside IRS IT teams to develop and implement ZTA-aligned, comprehensive incident response plans. These plans outline steps to be taken in the event of any security incident, helping to ensure that reporting diligence is followed up with standardized response protocols.

Results

These efforts to transition the IRS to ZTA have significantly strengthened its cybersecurity posture and defenses. The partnership between Maximus and IRS has made the agency better positioned to detect and respond to threats and has served as a model for other agencies to progress toward ZTA. Maximus' expertise and commitment to providing innovative solutions to protect critical government systems and data has elevated the IRS as a leader in cybersecurity best practices within the federal government.