Synack

Government Agencies Move to a Zero Trust Model with Application Security Testing

Modernize to better protect your agency

Government mandates direct federal agencies to adopt Zero Trust Architecture to modernize and improve cybersecurity defenses. Increased incidents, from the SolarWinds and Colonial Pipeline breaches to the Log4j vulnerability, have pushed the White House, Office of Management and Budget and the Department of Homeland Security to address cyber risks by modernizing U.S. cybersecurity systems and pushing for closer collaboration between government and the private sector. Advancing Zero Trust principles is a critical piece of these mandates.

The mandate for application security in your Zero Trust approach

With mandates moving the U.S. government to a Zero Trust Model, where no user or system is automatically trusted, federal agencies need to consider dedicated application security testing in addition to ongoing compliance requirements. The checklist below highlights certain requirements for agencies and defense industrial base (DIB) organizations to reach compliance with recent mandates. These requirements include:

- **Memorandum M-22-09, Section D: Applications and Workloads**
  The memorandum states "agencies must operate dedicated application security testing programs" and that they must utilize high-quality firms specializing in application security for independent third-party evaluation.
- **Binding Operational Directive 22-01**
  It requires federal civilian agencies to remediate vulnerabilities that are being actively exploited by known adversaries and to report back to CISA.
- **Binding Operational Directive 20-01**
  Agencies are required to maintain effective public vulnerability disclosure programs (VDPs).
- **FISMA, CMMC and NIST Compliance**
  Federal organizations must comply with FISMA to ensure NIST standards are adhered to, and defense organizations must adhere to the CMMC framework, which protects sensitive unclassified information shared with DOD contracting partners. Organizations in many cases are also required to support specific control guidelines including NIST SP 800-207 and NIST SP 800-53.

Background: OMB document M-22-09 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Achieve Zero Trust and compliance with dedicated application security testing

Synack provides dedicated application security testing and external attack surface discovery, enabling federal agencies to adhere to mandates while advancing their moves toward Zero Trust principles. Agencies that select Synack will also benefit from its FedRAMP Moderate Authorized designation, indicating that 325 security controls were met to enhance security for users working in Synack's FedRAMP environment. Synack's dedication to data security provides federal practitioners with a layer of trust needed while utilizing services in the cloud.

Synack, as the premier security testing platform, is proud to have worked with more than 30 government organizations on application security testing capabilities with capacity to deliver better results at scale than traditional methods. Synack365, a year-round continuous penetration testing engagement, reduces risks to federal agencies by external and internal assets alike, improving their organizational security posture. Backed by a vetted community of researchers for continuous penetration testing and vulnerability management, Synack is committed to helping agencies protect citizens and their data by bridging the cybersecurity skills gap, giving organizations on-demand access to the most-trusted worldwide network of security researchers.

> *"Synack is essential to my vulnerability management processes. It provides some of the greatest ROI I have. With Synack, you increase the trust with your IT Operations team."*
>
> MIKE BAKER - CISO, GDIT

Talent augmentation with the Synack Red Team

The Synack offering is empowered by the Synack Red Team (SRT), an elite community of highly-vetted global security researchers that represent the top talent in cybersecurity today. By utilizing the SRT community, you reap the benefits of a diverse set of skills and perspectives, allowing for more creativity and comprehension in penetration testing as well as skill and talent augmentation for specific security tasks.

Improve mean time to value & security posture

With new progress observed in allocating funds to meet increasing cyber challenges and requirements, Synack can help you scale your red team efforts, showing immediate impact with an effective offensive security augmentation that enables meeting the mandates now in place. The SRT can be activated to quickly begin work on a target, with multiple researchers engaged at a time as needed. Talk to Synack today to build better application security testing to identify vulnerabilities and ensure your authentication is secure.

Speak with your Synack representative or drop a line to government@synack.com to learn more.