Government Agencies Deserve A Better Way To Pentest

A Synack Perspective for the Public Sector

Kim Crawley

Executive Summary

State governments' security and risk teams across the public sector are feeling the squeeze between an increase in cyber attacks and a lack of resources to keep up. In a recent survey conducted on behalf of SolarWinds, public sector respondents reported an increase in concern over ransomware, malware and phishing from the previous year, but time to detection and resolution had not improved for the majority.

To bolster application security, the Office of Management and Budget (OMB) issued a memorandum directing agencies to identify critical software and implement the latest protections outlined by the National Institute of Standards and Technology (NIST). Another OMB memorandum presented a federal zero trust architecture (ZTA) strategy that requires agencies to meet specific cybersecurity standards and objectives by end of FY2024.

These and other security mandates underscore heightened concerns about cyberattacks on governments, which are escalating due to several factors: an expanded attack surface (e.g., home and mobile workers); adoption of cloud computing; accelerated software development and deployment cadence; and a severe shortage of security professionals. Countering this threat requires a multi-pronged approach, including dedicated and continuous application security testing.

Many government agencies already use annual penetration testing (pentesting) to identify issues and comply with regulations. However, traditional pentesting falls short in today's complex and rapidly changing threat landscape. First, legacy pentests often fail to replicate highly sophisticated cyberthreats. They may miss vulnerabilities in cloud and hybrid cloud environments. And, testing once a year provides only a single point-in-time snapshot of security while the attack surface and attacker continuously change.

According to Bryson Bort, a senior fellow in the Cyber Statecraft Initiative at the Atlantic Council, “CISOs on average have 30,000 vulnerabilities. The problem is, they have no context. Do those vulnerabilities actually matter? Are they critical to our security?”

In this paper, we discuss the importance of pentesting, highlight the drawbacks of traditional pentesting and describe a new approach that addresses these shortcomings. Better pentesting involves continuous testing of web and mobile applications by a team of expert, ethical security researchers, combined with a secure, dynamic pentesting platform. It can surpass legacy pentesting in scope, speed and scalability. This innovative solution can help federal agencies protect critical software, platforms and APIs more effectively while meeting increased security requirements.

Pentesting deficiencies analysis

Using antiquated pentesting methodology in today’s cyber threat landscape is like sending a tortoise out in pursuit of a cheetah. Here’s a point-by-point analysis of why and how old-school pentesting is no longer up to the challenges we face today:

- **Too slow and static for the cloud era.** A traditional, annual pentest misses critical cloud risks and assets. It targets only one point in time, must cover a vast landscape and doesn’t adequately convey the state of the environment. A zero day vulnerability or misconfiguration can occur at any time, regardless of defenses in place (e.g., Apache Log4j). Adversaries can and will exploit ephemeral cloud assets exposed on the internet (e.g., containers, buckets, etc.).

- **Inadequate flexibility and scalability**. Traditional pentesting cannot scale in government agencies with tens of thousands of assets. Frustrations include extended wait times for testing, inadequate coverage and the lack of insight into what was actually tested - all resulting in a lack of assurance and trust.

- **Security on paper, not in the wild.** Regulatory compliance is a vital baseline for any government security program, but it’s not sufficient in measuring security posture over time or in communicating resilience. When exploitable vulnerabilities are disclosed, malicious hackers immediately begin to identify targets. Attackers won’t wait for your team to patch or update your applications.

- **Disruptive to security and development workflows.** A traditional pentest creates anxiety and unnecessary work for security teams. Results are not actionable, as they lack context and rarely integrate with existing vulnerability management or ticketing systems. Most vendors won't re-test, measure security improvements or provide real-time analytics.

- **Falls short in creativity and resources.** We're living in a ransomware-as-a-service era, where malware delivery has become a business model. Attackers have a wide range of other tactics, techniques and procedures (TTPs) that pentests need to replicate. Two consultants armed with a checklist can't and won't prepare you for what's coming.

Your security team has an essential role in protecting mission-critical agency applications, and they deserve to be informed about every vulnerability that matters – without creating more work or risk.

Traditional pentesting is too slow and static for the cloud era

In accordance with the 2019 Federal Cloud Computing Strategy (Cloud Smart), federal agencies are migrating applications and data to cloud services authorized by the Federal Risk and Authorization Management Program (FedRAMP). The fact that cloud-hosted assets are elastic and growing faster than ever places new demands on pentesting:

- Containers and virtual machines can have life spans of mere days.
- Cloud resources can double and halve in size in the blink of an eye.
- With agile release methodologies, daily application updates can introduce new vulnerabilities.
- Case in point: According to research from Palo Alto Networks, large organizations add 1,300 new publicly accessible cloud services per year on average.

Additionally, old fashioned pentesting deployments fail at meeting scalability and flexibility requirements of modern development or security teams.

Mere compliance should not be a security baseline

Regulatory compliance is an important component of a federal security program, but **compliance checklists fall short**:

- Pentesting periodically to meet compliance makes measurements of security posture and risk difficult over time.
- The inconvenient truth is that cyber threat actors are testing you every day, much faster than the bureaucratic pace of HIPAA, Sarbanes-Oxley or GDPR requirements. Point-in-time reporting, or testing once per year, fails to provide timely assessments of new and exploitable vulnerabilities.
- When zero day vulnerability information is released, malicious hackers can immediately begin their enumeration process to identify targets.
- If your agency's sensitive data is breached in the months it took to find a vulnerability, the result may be negative publicity, citizen complaints and compliance violations.

Traditional pentesting disrupts security and development workflows

One reason why many agencies don't pentest more frequently or continuously is that **traditional pentesting is disruptive**:

- Many scanners used in pentests produce noisy results, distracting from fixing the higher priority vulnerabilities.
- A pentest can cause an application, network segment or department to go offline.
- Sometimes pentests need to be repeated to gather more information. But when pentesting is disruptive, repeating an exploit can become aggravating.
- Vendors may send pentest reports in formats that are not actionable (e.g., PDFs, Excel sheets).
- A security team member must spend valuable time copying and pasting report information into ticketing or collaboration tools like Jira, ServiceNow or Slack.

In addition to the aforementioned points on workflows, security leaders recognize that faster remediation is more important than ever, as hackers will prioritize externally facing vulnerabilities like misconfigured S3 buckets or supply chain vulnerabilities.

Traditional pentesting fails to match the creativity and resources of adversaries

Simply put, **traditional pentesting** does not measure up to the inventiveness, agility and skill of threat actors because:

- It can be difficult to find top pentesting talent, especially testers with specific specializations.
- Inevitably, the knowledge and skills of a few pentesters are limited compared to those of hundreds or even a thousand pentesters.
- Collective intelligence is a measurable phenomenon that can be highly inventive and effective in discovering vulnerabilities and exploits.
- Traditional pentesting engagements are limited in scope by design, to avoid disruption and due to limited time and resources.
- Today's cloud and hybrid networks are elastic and dynamic. You can't counter a dynamic threat with a static tool like traditional pentesting.

The reality is that attackers are scanning you every day, you just don't get the report.

Pentesting needs to change

Simply conducting more pentests in the traditional manner is not the answer. While missing all kinds of critical vulnerabilities, traditional pentests can even make it difficult to keep up with the ones that are found and reported.

Roman Medina, CISO at Jefferson Bank in Texas, said, "I do think we may miss critical issues or vulnerabilities if we stick to the same annual pentest year after year. The way we pentest has to evolve. I am looking at starting a continuous pentest service next year."

Staffing a team that is large enough to perform traditional, ongoing pentests is not feasible for most government agencies. Instead, it's time to reimagine pentesting.

Government agencies are adopting modern, on-demand pentesting solutions by crowdsourcing talent. These solutions add a rigorous vetting process for security researchers and combine human testing with sophisticated technology. This approach gives you access to diverse skills and knowledge in many different security areas. It

also permits continuous testing, seamless scalability of assets, ease of scheduling and guidance on remediation.

Ask your cybersecurity leadership how they plan to pentest better, today!