



WHITE PAPER

GOVERNMENT AGENCIES DESERVE A BETTER WAY TO PENTEST

A Synack Perspective for the Public Sector

By Kim Crawley





Executive Summary

The public sector is feeling the squeeze between an increase in cyber attacks and a lack of increased resources to keep up. In a recent survey conducted on behalf of SolarWinds, public sector respondents reported increased concern over ransomware, malware and phishing the most over the previous year, but time to detection and resolution had not improved for the majority.¹ 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 the end of FY2024.

These and other security mandates underscore heightened concerns about cyber attacks 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 cyber threats. 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. This new solution offers continuous pentesting of web and mobile applications by a crowdsourced team of expert, ethical security researchers, combined with an enabling pentesting platform. It can surpass legacy pentesting in scope, speed and scalability. Further, it provides valuable insights and context about vulnerabilities that are uncovered. This innovative solution can help federal agencies protect critical software, platforms, and APIs more effectively while meeting increased security requirements.

A better pentest provides continuous penetration testing of web and mobile applications by a crowdsourced team of expert, ethical security researchers on an enabling pentesting platform.

1. <https://www.businesswire.com/news/home/20220111005056/en>

Pentesting deficiencies analysis

As a security leader, you know that legacy tech is often unsecure, inadequate and difficult to administer. These caveats also apply to legacy pentesting practices. 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, storage 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. The cumulative effect of these gaps are a lack of assurance and trust in the agency's security posture.



- **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 their enumeration process to identify targets. Attackers don't care about rules of engagement, and they certainly 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 don't typically integrate to existing vulnerability management or ticketing systems. Most vendors won't re-test, measure security improvements or provide real-time analytics. Further, poor pentesting skills can lead to disruption and downtime, for example, if pentesters accidentally take applications or network segments offline.



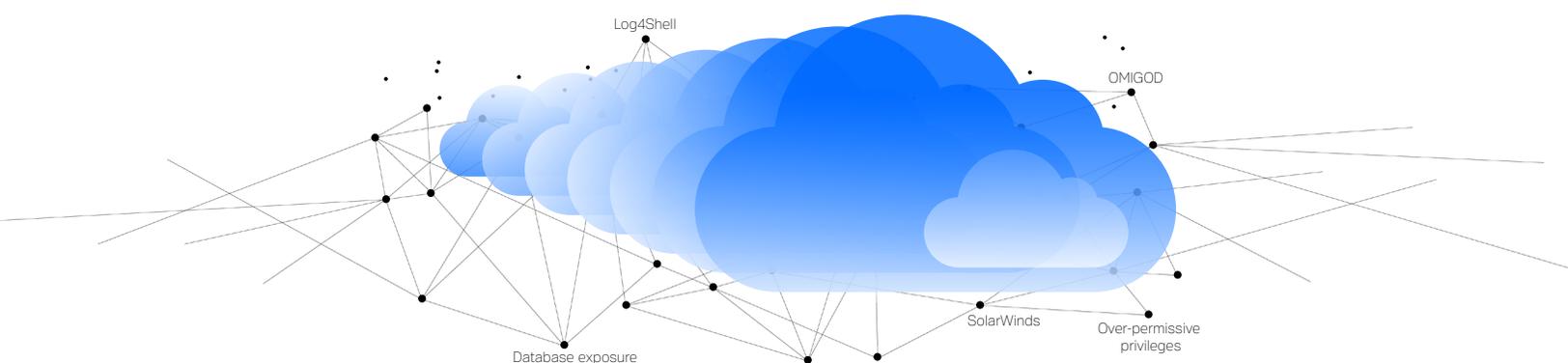
- **Falls short in creativity and resources.** We are living in the ransomware-as-a-service (RaaS) era, where malware delivery has become a business model. Attackers have a wide range of other tactics, techniques and procedures (TTPs) that pentests need to replicate. Two consultants armed with a checklist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

Your security team has an incredibly important 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, dynamic 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 modern 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.¹



Old fashioned pentesting deployments fail at flexibility and scalability

Deployments **may take weeks or months to schedule**, which significantly delays the testing process:

- When a new exploitable vulnerability appears on Twitter or Reddit, agencies often don't have the flexibility to check for that specific CVE on demand.
- A recent research report examining software vulnerabilities on social media found that on average they are discussed on Twitter, Github and Reddit for 87 days before being added to the National Vulnerability Database (NVD).²
- It's impossible to scale manual testing deployments from one to tens of thousands of assets.
- Pentests require the work of specialists with different skill sets, and it's difficult to schedule them if you plan engagements in the traditional way.



1. [Cortex Xpanse Research](#)

2. Shresthra et al. "Multiple social platforms reveal actionable signals for software vulnerability awareness: A study of GitHub, Twitter and Reddit." March 24, 2022.

Mere compliance should not be a security baseline

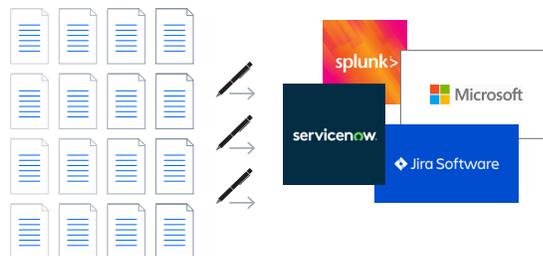
Regulatory compliance is an important component of a federal security program, but **compliance checklists fall short**:

- If you're pentesting periodically according to compliance rather than pentesting continuously, it's difficult to measure security posture and risk 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 (e.g., Microsoft Exchange).
- 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, a network segment or a department to go offline.
- Sometimes pentests need to be repeated to gather more information. But when pentesting is disruptive, repeating an exploit can be messy and aggravating.
- Vendors may send pentest reports in formats that are not actionable (e.g., PDFs and Excel sheets).
- A security team member must spend valuable time copying and pasting report information into ticketing tools like Jira, ServiceNow or collaboration tools like Slack.

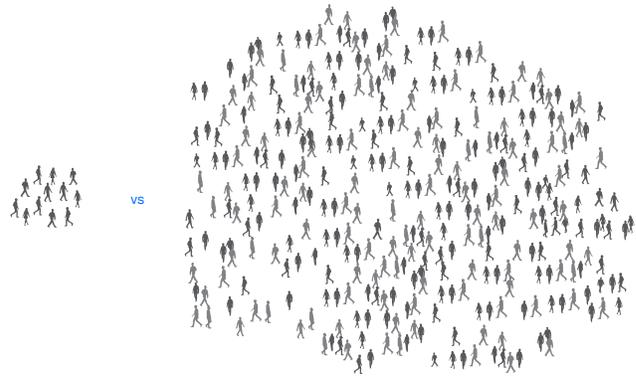


In addition to the aforementioned points on workflows, security leaders recognize that faster remediation is more important than ever, as hackers will prioritize externally facing vulnerabilities like misconfigured S3 buckets or supply chain vulnerabilities.

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, partly to avoid disruption and partly due to limited time and resources.
- Today's cloud and hybrid networks are elastic and dynamic, as are modern cyber threats. 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.

Collective intelligence is a measurable phenomenon that can be highly inventive and effective in discovering vulnerabilities and exploits.

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. It's frustrating to think of all the money, labor and other resources that are being spent on pentesting by security teams and their contractors, only to fall short in response to current and future cyber threats.

“

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.

ROMAN MEDINA - CISO, JEFFERSON BANK

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 based on crowdsourcing talent. These solutions add a rigorous vetting process for security researchers and combine human testing with sophisticated technology tools. 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.

For tips on what features to expect from an on-demand pentest, schedule a demo with the Synack team.

