RAPID7

SOLUTION BRIEF

IT Security in the Public Sector:

Building the Ultimate Strategy and Toolkit with Rapid7

Government agencies are increasingly becoming targets for cyberattacks and espionage. As custodians of public data, you have a mission to protect confidentiality above all other security concerns. That requires continuous monitoring, analysis, and remediation.

Meanwhile, the public sector faces a highly-controlled environment with a growing number of regulations. Staying on top of compliance requirements while safeguarding confidential information and evolving infrastructure isn't easy.

Rapid7 solutions simplify security and compliance and give you the tools and proof necessary to prove potential threats and motivate action. Nexpose and AppSpider hunt down and remediate vulnerabilities in the organization, while Metasploit Pro bolsters security posture through simulated attacks.

Leave No App Untested: AppSpider

Today's organizations in the public sector rely on a vast and ever-evolving array of custom web, mobile, and cloud applications. With the application environment in constant flux, no team can sustainably monitor and test all apps manually. Attackers know this: The applications that power organizations are their preferred channel of attack.

You need a security solution to find and test vulnerabilities in web apps in an automated way. While there's no shortage of Dynamic Application Security Testing (DAST) tools on the market, most are unfit to secure modern application architectures, data formats, and other underlying technologies.

Rapid7 AppSpider is the on-premises solution that provides the flexibility required to secure a complex, modern environment. With AppSpider, you can dynamically assess for vulnerabilities across all modern frameworks and technologies, speed up remediation, and monitor applications for changes.

Maximize Test Coverage

New technologies for web applications are being developed and implemented all the time. This rapid evolution is a boon for end users, but it can be a headache for security testers. Traditional web crawling simply doesn't cut it anymore.

AppSpider can still crawl traditional formats like HTML and Javascript, but with its Universal Translator feature, it can also interpret the modern technologies being used in today's web and mobile applications such as SPAs, AJAX, REST, JSON, and more. It does so by decoupling the discovery and attack engines so that all attackable inputs identified by the discovery engine are translated and normalized into a common universal format; this makes it possible for the same set of attacks to be applied to multiple input and data format types.

In addition, AppSpider offers the flexibility to select which portions of an app to scan, when to scan them, and which attack policies to use.

Customize Attack Modules

AppSpider comes equipped with a variety of predefined procedures and attacks with which to test applications, while our team continually monitors the threat landscape and deploys new modules.

However, like many organizations in the public sector, you're probably working with systems bespoke to your industry. AppSpider lets you build custom attack modules, ensuring that your application security testing solution is right for your unique environment.

Act at the Moment of Impact: Nexpose

Cyberattacks on federal agencies are increasingly sophisticated and frequent. To combat breaches, you need to be able to continually monitor environments and respond before impact. Nexpose is your on-premises solution for assessing vulnerabilities—and fixing them as soon as they arise.

Old data is your enemy. New vulnerabilities pop up daily due to network changes, new devices, improved attack strategies, and more. Nexpose is continuously monitoring and analyzing the network in real time, so you won't miss new or existing risks.

Remediate Quickly and Easily

In order to provide actionable recommendations, you need to know which high-risk vulnerabilities to prioritize. Nexpose provides an actionable risk score based on CVSS, vulnerability age, the availability of exploits for those vulnerabilities, and which malware kits use them.

Rather than the impossibly long static reports you're likely to receive from other solutions, Nexpose remediation reports include the top 25 actions that will reduce the most risk. You'll also be provided with clear instructions on exactly what to do about each issue to make sure vulnerabilities you identify are dealt with. You can make sure the remediation suggestions get to the right people by creating asset groups based on how remediation duties are divvied up.

Customize to Your Requirements

The robust APIs of Nexpose make it easy to build in your own customer toolkits and create custom automation. Have an air-gapped network? No problem. Unlike many vulnerability management solutions that can't function without an internet connection, Nexpose's flexible deployment and update options make offline scans easy.

As a government agency, a security solution is only worthwhile if it simplifies compliance with a variety of regulations. Nexpose provides integrated policy scanning to help you benchmark your systems against popular standards like CIS and NIST. Intuitive remediation reports give you step-by-step instructions on which actions can make the biggest impact on improving compliance.

Benefit from World-Class Support

As the premier solution for public sector vulnerability assessments, Rapid7 continuously works to keep Nexpose at the cutting edge of the threat landscape. Our support team is ready to collaborate with you to more effectively reduce vulnerabilities and combat attacks.

Stay Ahead of the Enemy: Metasploit Pro

You've identified vulnerabilities with Nexpose and they've been remediated—now what?

Test the results by simulating attacks with Metasploit Pro.

Metasploit Pro is the commercially-supported edition of Metasploit, the world's leading penetration testing solution. Metasploit Pro lets you turn attackers' techniques against them. Leverage a database of exploits backed by a community of over 200,000 global users and contributors to safely simulate real-world attacks on your network.

You can even go beyond your technological landscape and assess another leading source of vulnerabilities—people. Use Metasploit Pro to test employees with phishing and USB drop campaigns so you know they'll be ready for the real thing.

Leverage Advanced Features

Metasploit Pro is based on the trusted Metasploit Framework, but also provides features ideal for the public sector. You won't need to turn to outside sources for help with the software—Metasploit Pro comes with knowledgeable technical support.

You don't have time to run a long list of manual tests or compile endless reports. The automated features in Metasploit Pro make penetration testing efficient and easy. Have a sequence of repetitive tasks you run regularly? Automate them using Task Chains.

Government is a compliance-heavy environment where you may find yourself having to submit reports in duplicate or triplicate. Metasploit Pro has a powerful reporting engine with a variety of pre-configured standard reports, as well as the ability to build your own.

Double the Power: How Nexpose and Metasploit Pro Work Together

Nexpose reaches deep into the nooks and corners of networks and finds potential vulnerabilities. In some cases, these vulnerabilities might be a security breach waiting to happen. In others, maybe another app or procedure is preventing the vulnerability from being a true risk. Metasploit Pro works with Nexpose to make sure your resources are being funneled to the highest priority risks. Once Metasploit Pro has exploited vulnerabilities, they are considered validated, and this information is sent to Nexpose so that issues can be prioritized.

When you're working with other teams to clean up their internal vulnerabilities, you'll need to prove the impact of the issue. By simulating attack with Metasploit Pro, you can demonstrate exactly why a vulnerability requires remediation.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.

Ready to develop your complete security toolkit?

Reach out to sales@rapid7.com to get started.