WHITE PAPER

Flexible Web Application Security Testing Deployments

FOR GOVERNMENT AGENCIES

Invicti

Executive summary

This document demonstrates how decentralized deployments with internal scanning agents can provide consistent vulnerability scanning results with centralized visibility in a wide variety of environments. By decoupling the scanning engine from the management and reporting systems, agencies can deploy Invicti's industry-leading dynamic and interactive application security testing (DAST+IAST), Acunetix and Netsparker, to match internal application development infrastructure and integrate it into existing workflows. Highlights from this technical white paper include:

- The challenges of ensuring consistent and accurate vulnerability scanning and enforcing web security policies and compliance in distributed and highly dynamic application environments.
- How Invicti products use scan agents to combine distributed vulnerability scanning with centralized security management.
- The benefits of deploying one of Invicti's products, Acunetix or Netsparker, with scan agents, such as maximized security testing coverage, centralized visibility, improved operating efficiency, and automatic scaling.
- Typical use cases and deployment scenarios with network diagrams, including an agency-wide deployment with thousands of web assets to secure.

Invicti helps organizations to centrally secure and manage multiple web applications in a variety of deployment scenarios.

The challenges

Ensuring consistent web application security testing across multiple environments, deployments, and locations poses a major technological challenge for government entities. Every organization is different and one-size-fits-all solutions inevitably require trade-offs between coverage, effectiveness, and workflow efficiency. While the ultimate goal is the same – to measurably improve web application security – the sheer variety of application deployment architectures leaves organizations struggling to get tangible results.

SECURING DISTRIBUTED APPLICATION ENVIRONMENTS

To be effective at scale, security solutions and workflows need to be automated as much as possible. The growing complexity and scale of web application environments combined with a rapidly changing cybersecurity landscape means that code-level (static) security testing is not enough to prevent vulnerabilities. Organizations have come to realize that automated dynamic testing is crucial to any web application security program, but implementing scanning effectively in complex environments is not an easy task. What's more, scanning is just the beginning. To improve security, you need to get accurate and timely vulnerability information to your developers so they can fix the issues. You also need centralized visibility across the entire security workflow, no matter how complex the underlying infrastructure.

For large application environments with hundreds of web assets spread across multiple sites, handling vulnerability scanning and management manually is simply not effective. To complicate the picture even more, what if some of the application environments you want to scan are internal and not accessible from the Internet, perhaps for compliance reasons? What if they reside in separate networks or even different physical locations across the world? How do you ensure that all assets are scanned on a regular basis and vulnerabilities are fixed before they can be exploited by attackers? How can you centrally manage security across distributed teams? How do you keep track of all the security workflows so you know if you are making progress?

Organizations realize that automated dynamic testing is crucial to any web application security program, but implementing scanning effectively in complex environments is not an easy task.

KEEPING PACE WITH CHANGE AND GROWTH

Compounding the problem is the fact that web application environments are highly dynamic. New sites and applications appear on what seems a daily basis, high-profile applications are under constant development, and new technologies are readily brought on board to keep ahead of the competition. Because it has become so easy to spin up a new website or expand an existing one, many agencies don't know exactly what web assets they have and what they need to secure.

Software architecture is changing, too. Monolithic applications are now a rare sight outside legacy environments and organizations increasingly favor service-oriented designs, with software commonly split up into dozens or even hundreds of microservices. Coupled with the flexibility and convenience of cloud computing and virtualization, this results in web application environments made up of ever-changing collections of containerized web services that are spun up and torn down depending on current business needs and workloads.

Facing this moving and ever-expanding target are small security teams that don't have the resources or technical capabilities to manually keep up with all the changes and centrally manage security. If you have a dozen geographical locations with separate web application development programs, staying in control of all the changes becomes exponentially more difficult. When you also need to scale security to match the pace of organizational growth while still maintaining visibility of the overall security posture, it is clear that conventional approaches are not going to work.

New sites and applications appear on what seems a daily basis, high-profile applications are under constant development, and new technologies are readily brought on board to keep ahead of the competition.

The solution: Flexible scan agent deployment

To address these challenges across the huge variety of deployment models and use cases, web application security solutions need to be highly configurable and support a variety of deployment models. This allows organizations to smoothly incorporate security into their existing environments and workflows to ensure consistency and central visibility.

Invicti's solutions, Acunetix and Netsparker, have a modular architecture that offers extremely flexible deployment options, from a fire-and-forget, all-cloud on-demand deployment to advanced on-premises setups across isolated internal networks. With this model, you can take advantage of Invicti's industry-leading vulnerability detection and management features in a way that best suits your infrastructure and business requirements.

Vulnerability scanning with Invicti's products is based on the idea of decoupling the scan process from the central server by using scan agents to run scans and report results back to the server. For maximum flexibility, you can deploy scan agents in any target environment – on-premise (on Windows and Linux, but also wherever a Docker image can be deployed), in the cloud, and in any hybrid configurations in between. The goal of deploying one of Invicti's products with a customized scan agent setup is to decentralize scanning and align it with the application environment while still reaping the benefits of centralized scan and vulnerability management.

Invicti's solutions have a modular architecture that offers extremely flexible deployment options, from a fire-and-forget, all-cloud deployment to advanced on-premises setups across isolated internal networks.

The benefits

By matching the deployment model of the web application security solution to your agency's specific environment, you can take full advantage of the Invicti products' workflow integration and optimization capabilities. Let's take Netsparker as an example. After setting up scan agents and automation, a small security team can easily manage thousands of assets across multiple locations and add agents as necessary to seamlessly scale scanning without additional manual configuration. Combined with Netsparker's extensive internal API, this also opens the way to fully automated security testing integration in custom environments.

With multiple scan agents, agencies can divide and conquer application security challenges by maximizing coverage and making full use of Netsparker's proprietary Proof-Based Scanning™ technology. This translates to rapid security improvements with minimized communication overhead, shorter time-to-fix, and automated fix retesting across all web application environments.

With multiple scan agents, agencies can divide and conquer application security challenges by maximizing coverage and making full use of Netsparker's proprietary Proof-Based Scanning™ technology.

CENTRALIZED VULNERABILITY SCANNING AND MANAGEMENT

Results from multiple Netsparker scan agents can be combined in a single easy-to-use management interface for full visibility and control over web application security across any number of environments. Crucially, this is possible regardless of the internal deployment architecture and organizational structure. After all, a large organization can have dozens of development teams, each with its own unique tasks, capabilities, and needs. Without centralized web application security management, there is no way to define and apply security policies, enforce SLAs or identify opportunities for improvement.

Centralized management is especially challenging across local environments. While organizations worldwide continue moving to the cloud, there are still many situations where data and applications must reside on local systems, for example due to compliance concerns. By deploying Netsparker scan agents in each environment, agencies can scan internal applications and manage vulnerabilities from a central interface just like in an all-cloud setup. Combined with automation and API integration, this provides a unique solution to detect vulnerabilities and maintain web application security across multiple logical and physical locations, no matter if you are using Netsparker via the user interface or integrating its scanning capabilities into your own management systems.

By deploying Netsparker scan agents in each environment, you can scan internal applications and manage vulnerabilities from a central interface just like in an all-cloud setup.

AUTOMATIC SCALING IN THE CLOUD

For cloud-based deployments[1], you can use Netsparker scan agents to improve scalability and performance. If you set a Netsparker scan agent to cloud mode and enable automatic scaling in the cloud, a new cloud agent will be automatically created every time a scan is launched and automatically destroyed when the scan ends. This eliminates the need to manually configure additional agents as scanning needs grow – when a new website, web service or application environment instance goes live, you can automatically fire up one or more agents to test it.

The ability to spin up scan agents on demand is especially important in containerized environments where the number and type of services and applications that are running at any given time may vary depending on the current workload. Agent scalability extends scan automation to ensure scanning coverage across the entire web application environment currently in use. This provides a realistic view of the current web security posture and, if necessary, allows you to reduce scanning time by using multiple agents to scan many environments in parallel.

[1] *Currently supported on Amazon Web Services.*

Whenever a new website, web service or application environment instance goes live, you can automatically fire up agents to test it.

Selected deployment scenarios

To ensure that all users can integrate industry-leading vulnerability scanning capabilities into their environments, Invicti developed Netsparker and Acunetix with flexibility in mind. Depending on their individual needs, agencies can use any combination of built-in and custom integrations and management capabilities to launch scans and collect results. Below are just a few deployment scenarios that use scan agents to maximize effectiveness and coverage.

AGENCY-WIDE DEPLOYMENT ON-PREMISES

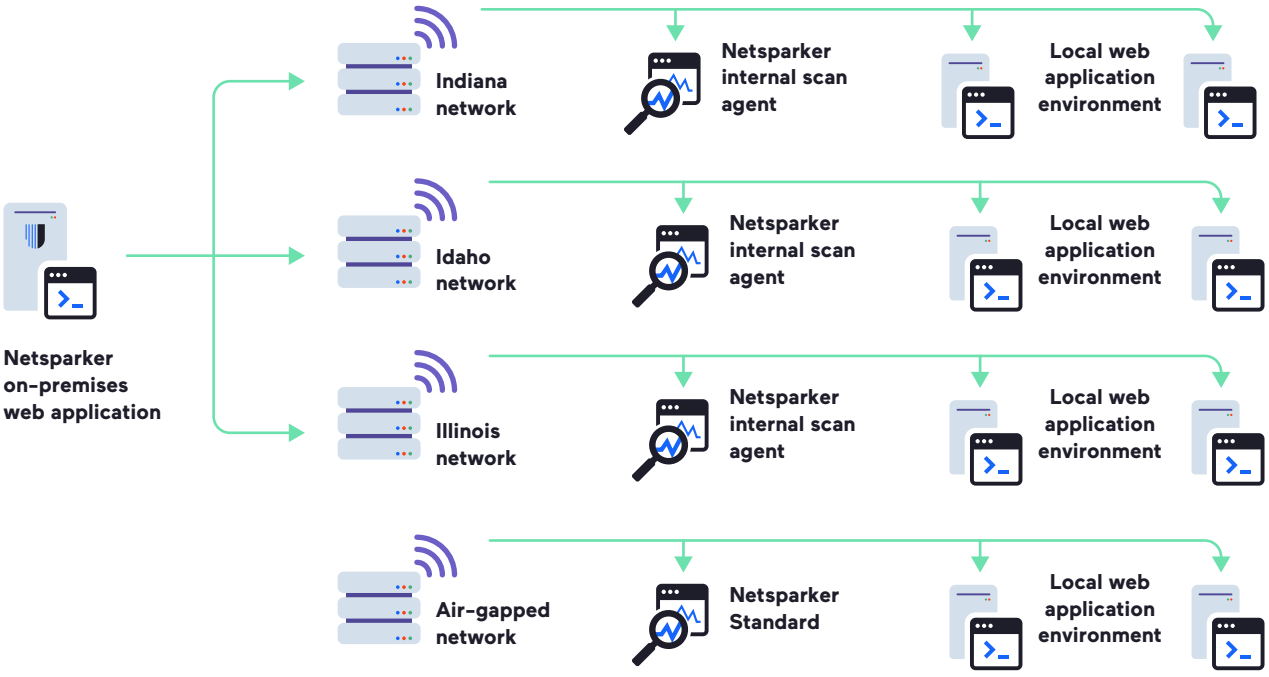
A federal agency maintains and develops dozens of web applications for multiple states. Development is spread across some 30 separate teams, each with its own development, staging, and production environments. Each team has its own virtual network within the wider agency infrastructure. For compliance reasons and to protect citizens' personal information, data storage and application development must be isolated from the public web.

For ad-hoc scans and manual testing in air-gapped networks, the security team uses Netsparker Standard, which is included with the Enterprise edition. Scan results from Netsparker Standard are then uploaded to the on-premises Netsparker server.

SOLUTION – Netsparker on-premises with local scan agents in each team's virtual network, managed by a Netsparker server deployed on-premises. Each team has one virtual machine that runs a scan agent to test selected web assets in the team's local network, with scans triggered automatically via a Jenkins integration. Scan results from each agent are sent to the on-premises Netsparker application server. The web security teams use Netsparker's vulnerability classification and management features to assign issues to developers.

SCENARIO 1

NETSPARKER ON-PREMISES WITH LOCAL SCAN AGENTS IN VIRTUAL NETWORKS AND ON-PREMISES MANAGEMENT



AGENCY-WIDE ON-PREMISES DEPLOYMENT IN THE PRIVATE CLOUD

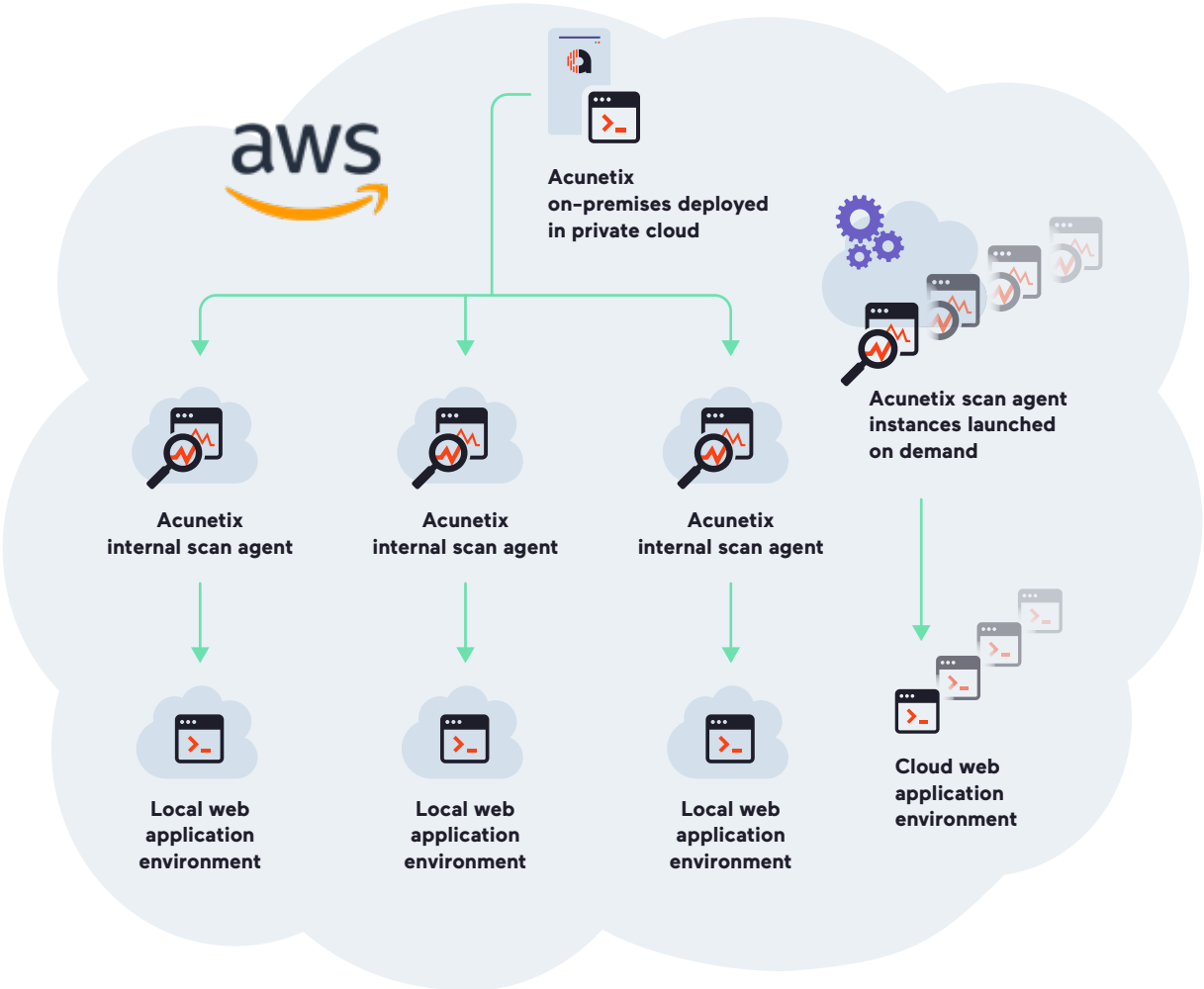
A government department agency runs a constantly growing all-cloud environment based on Amazon Web Services, with hundreds of services and applications developed and maintained both for citizens and for internal use. Web application environments change on a daily basis as new functionality is rolled out in CI/CD pipelines and existing containerized services and applications are spun up depending on demand.

Automatic scan agent scaling in the cloud provides a unique solution for securing environments that are spun up automatically, where it is impractical to deploy scan agents manually.

SOLUTION – Acunetix on-premises deployed to a private AWS cloud with cloud scan agents and automatic agent scaling on AWS. Every time a scan is launched, Acunetix creates a new agent instance, runs the scan, collects the results, and destroys the instance. Scans are triggered automatically for each build, so the number of scan agents varies to match the current testing workload. Results are sent back to the central server and accessible to the security team in the regular Acunetix user interface. All vulnerabilities confirmed with Proof of Exploit and classified as High or Critical severity are automatically assigned to developers to fix via a Jira integration.

SCENARIO 2

ACUNETIX ON-PREMISES DEPLOYED TO A PRIVATE AWS CLOUD WITH AUTOMATIC SCAN AGENT SCALING



AGENCY-WIDE DEPLOYMENT IN THE CLOUD

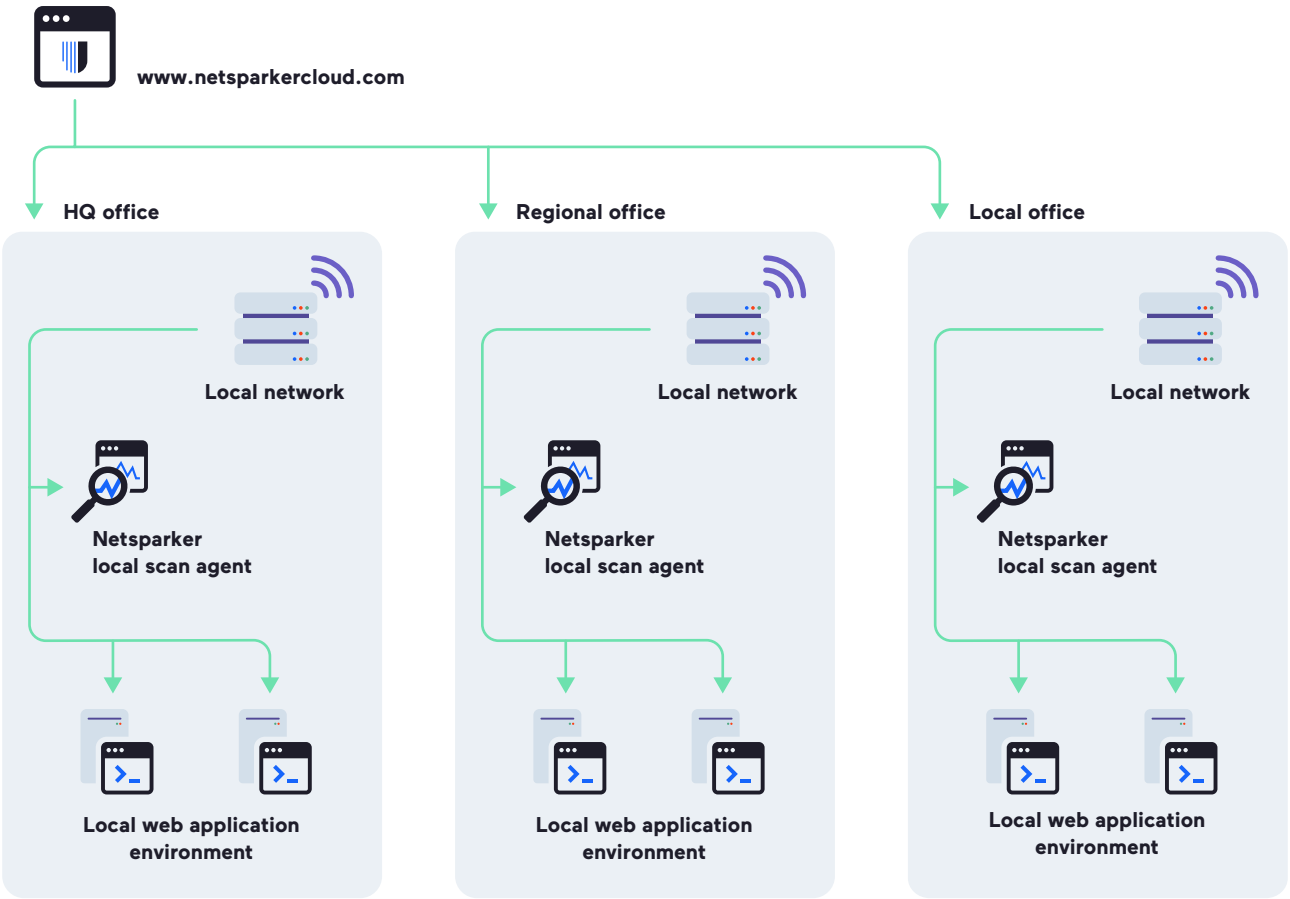
An independent executive agency has web development teams spread across a number of separate physical sites in multiple locations, using a mixture of Windows and Linux environments. To protect intellectual property, development and staging environments must be isolated from the public Internet. At the same time, the agency needs to uniformly enforce strict web application security policies to meet regulatory requirements for information security.

Internal scan agents allow the organization security team to scan non-public development and staging environments. Once deployed to production, the live applications are scanned directly using Netsparker on-demand.

SOLUTION – Netsparker on-demand with local scan agents at each site, managed centrally by the Netsparker server in the cloud. Each team has one machine that runs a scan agent to test selected web assets in the team's local network, with scans triggered automatically via a custom IDE integration using the Netsparker API. Scan results from each agent are sent to the central Netsparker server where the web security team can use Netsparker's vulnerability classification and management features to assign issues to developers.

SCENARIO 3

NETSPARKER ON-DEMAND WITH LOCAL SCAN AGENTS AT EACH SITE AND CENTRAL MANAGEMENT IN THE CLOUD



Conclusion

An effective web application security program relies on accuracy, consistency, and maximum automation. For large organizations, applying consistent vulnerability scanning policies across multiple environments poses a major challenge. They need a solution that will allow them to distribute scanning and provide centralized results and visibility, regardless of the specific architecture and technologies.

Invicti's application security testing solutions, Acunetix and Netsparker, were designed with precisely this goal in mind, using a modular architecture that decouples vulnerability scanning and management. Agencies can align scanning to their internal structures and workflows by deploying Acunetix or Netsparker scan agents in all their web application environments, whether on-premises or in the cloud, but still reap the benefits of centralized security management. Combined with the benefits of extensive integration and customization, this translates into improved coverage, compliance and, ultimately, more secure web applications.

Agencies can align scanning to their internal structures and workflows by deploying Acunetix or Netsparker scan agents in all their web application environments.

Invicti

ABOUT INVICTI SECURITY

Invicti Security is changing the way web applications are secured. A global leader in web application security for more than 15 years, Invicti's dynamic and interactive application security products help government entities scale their overall security operations, make the best use of their security resources, and engage developers in helping to improve their overall security posture. Invicti's products **Acunetix** and **Netsparker**, automate application vulnerability identification, confirmation, and management to keep public information and critical infrastructure secure. Designed with the government in mind, Invicti's products meet all federal mandates, including FISMA, NIST and STIG compliance requirements.

fedgov@invicti.com **www.invicti.com/fed-gov**