Outpost24

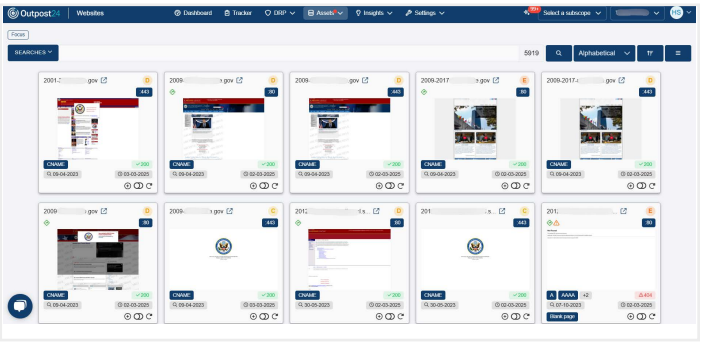
CyberFlex

Implementing comprehensive application security strategy for the evolving attack surface

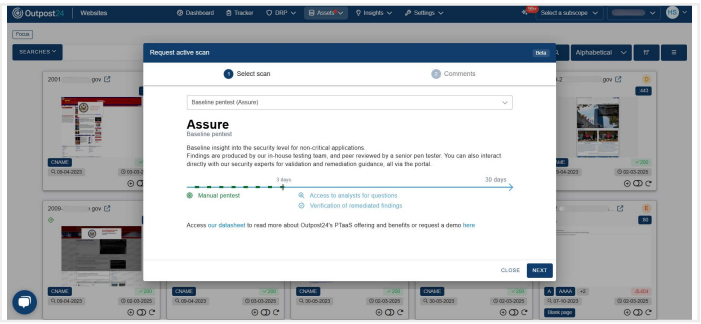
As the application attack surface grows, many organizations struggle to efficiently connect attack surface data to their pen testing planning. A lack of visibility and understanding of the application inventory can lead to a false sense of security, as both known and unknown applications introduce new vulnerabilities and risks. Access to meaningful and actionable insights is crucial for effective remediation and reducing the risk of data breaches.

With Outpost24 CyberFlex, we play a critical role in supporting the execution of your application security strategy, preventing unauthorized access, and maintaining the integrity and availability of applications. By implementing thorough application security measures, you can mitigate risks, protect your reputation, and ensure the trust of your customers and stakeholders.

Enhance your application security strategy with our complete attack surface management and on-demand PTaaS solution. Our service enables your team to focus on what matters most by sifting through your attack surface to identify the riskiest apps for further assessment. Our scalable and flexible solution helps you maximize your pen test spend throughout the annual engagement without slowing you down. With CyberFlex you get the tools, expert guidance, and strategic insights needed to optimize your security efforts and mitigate risks, all in one place.



Application inventory



Application PTaaS

Key Use Cases

Continuous App Discovery & Monitoring
We analyze your application inventory, whether known and unknown and provide context and recommendations for vulnerabilities and potential severity impact.

Attack Surface Scoring & Prioritization
Rates the attack surface across the entire scope, on applications and exposure and provides in-depth insights to prioritize remediation efforts.

Comprehensive Risk Assessment
We provide detailed risk categorization and security ratings, considering factors such as usage, ownership and location. This consolidated PTaaS assessment helps you manage application risk more effectively.

Remediation & Compliance
Maintain complete visibility and identify unpatched software to eliminate unused entry points, reducing your attack surface. As your company grows, expedite future remediation to ensure ongoing compliance.

Guiding you through attack surface management and penetration testing

- Which known and unknown applications are currently exposed?
- What applications do I own that carry the highest risk?
- Which application vulnerabilities should I prioritize to reduce the risk of a breach?
- How effective is my penetration testing process?
- How can I monitor new applications as they enter the attack surface?
- Can I identify all risky applications to expedite further testing?
- How can I detect and manage shadow IT?
- How can I maximize the value of my penetration testing investments?
- Can I be confident that I will remain compliant with new regulations?

Comprehensive application security strategy

SecOps
Gain a comprehensive understanding of your entire estate and application security posture to keep security at the forefront. Our in-depth insights empower your development teams and enhance your Appsec programs, ensuring that business-critical applications are released free of vulnerabilities. This protects your brand reputation and supports company growth without slowing you down. With our flexible consumption-based pricing and integrated platform, you can have complete peace of mind knowing that all issues are identified for further testing, driving ROI and ensuring compliance.

DevSecOps
Our Appsec experts offer a continuous feedback loop and in-depth recommendations, enabling developers to proactively fix critical issues before moving onto the next stage. By building a comprehensive application inventory and providing recommendations for further pen testing, we help catch vulnerabilities early. We also generate a prioritized list for developers to address critical issues first, enabling you to make better informed decisions and save money.

M&A
During M&A it's crucial to understand the new company's application landscape, assessing the associated risks, and making informed recommendations on next actions. Manually trying to identify and test all your applications can be time-consuming and error-prone, often leading to missed vulnerabilities. We provide comprehensive, automated insights and detailed reports, ensuring that you have a clear and complete risk assessment, which is essential for making strategic decisions and mitigating potential security threats.

GET A DEMO

Key Product Features

24/7 monitoring
Continuous attack surface monitoring and application risk categorization to identify potential threats and defend your apps against adversaries before they strike.

Comprehensive discovery
Automatically maps and analyzes your external facing apps and even those you don't know about.

Interactive dashboard
In-depth recommendations about your application attack surface allowing you to drill down to all details and expedite apps for further assessment.

Actionable results
Our Appsec experts will analyze and review your application risks for complete security peace of mind.

Custom alerts and reporting
Fully configurable alerting and reporting to fit your needs.

Flexible consumption agreement
Better-informed, consumption-based pricing ensures you test the riskiest apps, saving you time and money.

About Outpost24

The Outpost24 group is pioneering cyber risk management with vulnerability management, application security testing, threat intelligence, and access management – in a single solution. Over 2,500 customers in more than 65 countries trust Outpost24's unified solution to identify vulnerabilities, monitor external threats, and reduce the attack surface with speed and confidence.
Delivered through our cloud platform with powerful automation supported by our cyber security experts, Outpost24 enables organizations to improve business outcomes by focusing on the cyber risk that matters.