BISHOPFOX

DATA SHEET

COSMOS Application Penetration Testing (CAPT)

CAPT is a fully managed service that extends the coverage of the Cosmos Continuous Threat Exposure Management to strengthen the security of business-critical custom applications. CAPT delivers authenticated assessments through a user-friendly interface, with expert analysis to uncover high-risk exposures, real-time insights, and ongoing threat surveillance for sustained resilience.

MEET THE SECURITY DEMANDS OF YOUR MOST CRITICAL APPS

In-depth Testing for Subsurface Threats

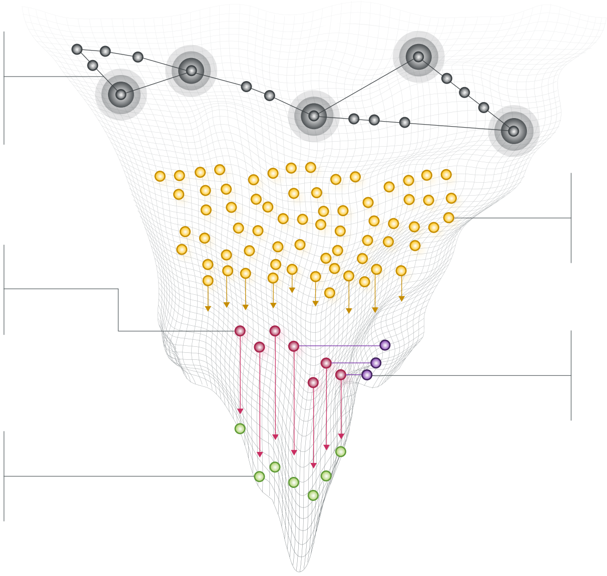
Cosmos Application Penetration Testing (CAPT) offers an innovative approach to application security, prioritizing and protecting the custom applications that are critical to your business.

CAPT is a fully managed service offering in-depth assessments to uncover the full spectrum of threats, from surface vulnerabilities to deeper risks associated with authenticated access, leaving no stone unturned. Our expert-led testing rigorously validates each vulnerability for real-world exploitability, and our findings are directly linked to activities that threaten essential systems, data, and services. As a result, your teams can focus on the threats that pose a genuine risk and prioritize remediation based on the actual business impact.

In the time sensitive and rapidly changing world of cyber threats, CAPT keeps you ahead of attackers and your defenses resilient. Real-time expert guidance and on-demand remediation testing let you quickly close the window of vulnerability. By monitoring for emerging threats and revisiting previous indicators of vulnerability, CAPT ensures your defenses remain strong as the threat landscape and your applications evolve.

KEY OUTCOMES

- **Gain Confidence in the Security of Your Key Applications ›**
- **Uncover the Full Spectrum of Exposures Above and Below the Surface ›**
- **Eliminate Noise, Act Only on Exploitable Threats ›**
- **Prioritize Remediation on Issues That Are Business Impacting ›**
- **Quickly Close the Window of Attacker Opportunity ›**
- **Maintain Defensive Resilience ›**



APPLICATION IDENTIFICATION

Provides a flexible model to nominate targets from Cosmos Attack Surface Management discovered assets or self-submission of applications.

VALIDATION OF EXPLOITABILITY

Eliminates noise by highlighting only high-risk threats confirmed to be exploitable in real-world attack scenarios.

ACCELERATED REMEDIATION

Closes the window of exploitability with access to testers & on-demand remediation testing.

APPLICATION MAPPING & VULNERABILITY IDENTIFICATION

Maps the application and identifies concealed risks inherent with authorized user access.

ONGOING ACTIVITIES

Monitors the threat landscape for emerging threats or classes of previously unknown vulnerabilities that put the application at risk.

Separating Cosmos from the Competition

Experience the Difference

Don't settle for partial solutions that leave your key applications at risk. CAPT offers a fully managed service that combines in-depth testing with the latest technology to proactively address critical, business-impacting exposures while maintaining application resilience against evolving threats.

	Depth of Assessment	Vulnerability Identification	Exposure Validation	Meaningful Severity	Retesting & Support	Ongoing Activities
CAPT	✓ Extends the scope of assessment to encompass authorized user risk.	✓ Maps the complete application attack surface, ensuring all exposures are brought to light.	✓ Verifies all findings are exploitable under real-world attack conditions.	✓ Ties exposure severity to real business impact, confirming that every alert requires action.	✓ Closes the window of vulnerability with live-tester access and on-demand remediation testing.	✓ Preserves resilience by tracking new and evolving threats that endanger your application.
OTHER SOLUTIONS	✗ Only scratches the surface, leaving deeper issues unaddressed.	✗ Neglects key areas, allowing exposures to remain hidden in the shadows of your applications.	✗ Places the responsibility of triage and validation on your security team.	✗ Ties findings to theoretical risk, diverting attention from the exposures that matter most.	✗ Imposes significant strain on your already overstretched resources to analyze outcomes and execute remedial measures.	✗ Restricts the length of evaluation, leading to a gradual weakening of defenses against the evolving threat environment over time.

CLIENT SATISFACTION

82%
Reduction in critical exposure timeframes

5,000+
Hours saved yearly identifying & triaging

93%
Reduction in resource investment

95
Net Promoter Score

Trusted by Industry Leading Organizations

amazon EQUIFAX SONOS

august CHANGE HEALTHCARE Google

Recognized as a Leader in Offensive Security

Best Workplaces for Innovators

Attack Surface Management Market Leader

Product Innovation, Thought Leadership, & Web Design

Security Product for Large Enterprise

Hot Company in ASM

SC 2021 awards BEST EMERGING TECHNOLOGY

About Bishop Fox

Bishop Fox the leading expert in offensive security, providing comprehensive assessment of modern environments with continuous attack surface management, red teaming, and penetration testing for applications, cloud, network, and products. We've worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security. Our Cosmos platform won six awards for innovation in 2022 from programs including SC Media, The American Business Awards, The Globees, and Cyber Defense Magazine and was named an ASM Fast Mover and Leader in both 2022 and 2023 by GigaOm. We've been actively contributing to and supporting the security community for almost two decades and have published more than 16 open-source tools and 50 security advisories in the last five years.

Learn more at bishopfox.com
Follow us on X