COALFIRE

DATA SHEET

Web application perimeter mapping

Without a clear understanding of the attack surface, how can you minimize it?

Given the speed at which enterprises must build and deploy software, they're likely only able to scale regular testing efforts to a small percentage of external web applications and cloud services. With an ever-increasing presence of continuously deployed, publicly accessible assets, the weakest links won't necessarily be found in business-critical applications, but rather in neglected, forgotten, unknown, legacy, or unintentionally public applications and servers.

As a result of shadow IT, M&A activity, and marketing campaigns, gaining and maintaining visibility of your external web footprint can be a constant struggle. Further complicating the situation are ongoing attacks that leverage marketed vulnerabilities – many of which have had patches available for years. Organizations with large web footprints created by the ongoing presence of outdated, weak, misconfigured, or leaky applications and servers are particularly at risk.

Through web application perimeter mapping, Coalfire creates a baseline inventory of your unique web application perimeter. Through subsequent mapping on a monthly, quarterly, or as-needed basis, you can ensure that any changes to the available attack surface are quickly recognized and tracked.

Leverage meaningful insight to make informed, scalable risk decisions

Mapping your organization's external web application perimeter may not involve any testing activities, but the output will yield critically valuable data. From the information uncovered, you can generate instant awareness of risks and justify easy follow-up fixes, including:

- Patching vulnerable web servers
- Standardizing ports in use
- Identifying applications with basic authentication
- Decommissioning forgotten or legacy applications
- Implementing or fine-tuning defensive layers like runtime application self-protection (RASP) or a web application firewall (WAF)

Address modern security considerations

Whether part of preacquisition due diligence or post-close integration activities, perimeter mapping rapidly discovers web assets owned by and related to the target entity while simultaneously reducing the inherent risk and operating costs created by their public exposure.

Why Coalfire

- Our AppSec consultants have experience in both software engineering and security consulting, which means we're able to deliver modern, actionable guidance on all aspects of application security.
- We conduct more than 1,000 complex projects each year for clients in the technology, healthcare, financial, manufacturing, energy, and retail industries.
- Our team comprises experienced testers of the world's largest cloud service providers, including Amazon, Google, IBM, Microsoft, Oracle, and Salesforce.
- For the past 10 years, we have trained and educated security professionals at Black Hat in the advanced tradecraft we developed.

Attain critical visibility and actionable insight into your web application perimeter.

Learn more about Coalfire's web application perimeter mapping solution.

Coalfire.com | 877-224-8077

COALFIRE

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

DS_WAPM_01212022