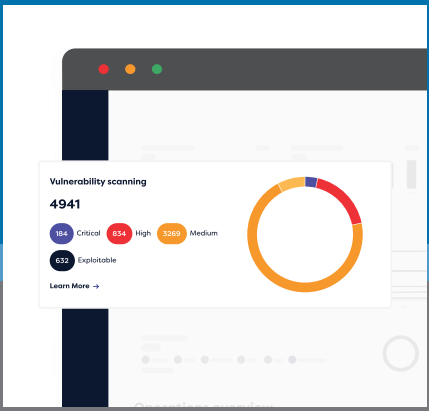
Rootshell External Attack Surface Management



Manage the growing complexities of security perimeters by discovering, monitoring, assessing and reducing external attack surfaces.

Key features

- Identifies unknown risks and exposures
- Maps attack surfaces
- Continuous discovery of digital assets
- Monitors for unauthorised access
- Clear visibility of what's exposed and vulnerable
- Proactively addresses issues before they are exploited
- Contextualised risk scoring, clear reporting & inventory
- Insight into risks from third-party and vendor exposure

About Rootshell EASM

Rootshell External Attack Surface Management (EASM) helps organisations protect their external attack surface, securing any digital assets exposed to the internet. EASM continuously identifies all internet-facing assets, including known and unknown domains, IP addresses, cloud services, third-party assets and shadow infrastructure, providing a comprehensive view of an organisation's digital footprint.

Through this monitoring, potential vulnerabilities and threat vectors that malicious actors can exploit can be detected and secured.

Why we partner with Rootshell?

Rootshell EASM enables organisations to understand and manage risk across a continuously changing digital environment. Rootshell's EASM service proactively manages external risk through continuous monitoring, providing contextual risk scoring and clear, actionable reporting.

By embedding EASM into a security strategy, the most critical exposures can be detected, prioritised and secured - while also supporting compliance and audit requirements. As security and compliance expectations increase and threats grow, Rootshell EASM empowers organisations to stay ahead of threats.

The challenges Rootshell EASM solves

Digital footprints are continuously changing which means one-off attack surface assessments are unreliable making it easy and highly likely to miss exposures. At the same time, attackers continuously scan the internet using automated tools and open-source intelligence to discover exposed assets and vulnerabilities.

Organisations need to maintain a clear, up-to-date view of their external attack surface. Rootshell EASM delivers this, applying the same search techniques as threat actors but from a defensive perspective. By identifying what attackers would see first, Rootshell EASM allows organisations to remediate issues before they can be exploited.

brigantia by ELOVADE

020 3358 0090
partnersupport@brigantia.com
www.brigantia.com

Suite 2.1, Hurstwood Business Centre
York Road, Thirsk
YO7 3BX