DATA SHEET

Zscaler Professional Services

Attack Surface Discovery Report

As organizations look to accelerate Digital Transformation, they need a new model for securing access to private applications. Traditional, network-centric, technologies require companies to expose services to the Internet. This creates a larger attack surface, and leaves them vulnerable to Internet-based attacks, port scanning and ransomware.

Understanding what their attack surface is, and taking steps to reduce it, are both critical to minimizing business risk. Our tool provides analysis to discover your Internet facing attack surface and delivers the findings within a consolidated report. It does an extensive subdomain search on public sources and queries third-party databases to assess known vulnerabilities to build a comprehensive report. With this report you'll be able to identify any unintended public network exposure. Zscaler will then work with you to embrace a zero-trust network access (ZTNA) strategy to mitigate these vulnerabilities and strengthen your overall security posture.

Benefits of Professional Services:

- **Real World Experience** Our Deployment consultants bring deep architectural and operational experience, bolstered by thousands of implementations, that help you reduce risk and increase project success
- **Bridge Resources and Knowledge Gaps** Access Zscaler's expertise to efficiently fill potential skill or resource gaps, without having to hire additional resources
- **Leading Practice Guidance** Achieve your business objectives quickly by leveraging our years of experience and knowledge of leading practices
- **Accelerate ROI** Feel confident knowing your deployment has been set up for success, by relying on Zscaler's proven project methodology

©2024 Zscaler, Inc. All rights reserved.

Focus of the Attack Surface Discovery Report

The detailed report includes five main categories:

- **Known Vulnerabilities:** The report uses the industry standard Common Vulnerability Scoring System (CVSS) and will display each server that has known Common Vulnerabilities and Exposures (CVEs) associated with it. CVSS scoring is provided and is based on the criticality of these CVEs.
- **SSL/TLS Weaknesses:** All services supporting TLS will have their TLS versions reported if they support any protocol version that is TLS1.1 or earlier. Even though these services support the recommended protocol versions (TLS1.2, TLS1.3) clients can negotiate to the lower supported TLS version and exploit known weaknesses.
- **Exposed Servers:** These are ALL the servers that are exposed to the internet and publicly accessible.
- **Namespace Exposure:** The namespace exposure has a list of all services which have a matching keyword or an exposed DNS entry.
- **Public cloud Instances:** Provides insight into the number of applications running on public cloud platforms like AWS, Azure, GCP.

The benefits of receiving this comprehensive report are:

- You learn about your organization's current internet attack surface posture
- You can minimize the risks to your business by implementing applicable recommendations

Use the Attack Surface Discovery Report to identify which internal applications and servers are unintentionally exposed to the internet. Use ZPA to put these resources in the dark.

©2024 Zscaler, Inc. All rights reserved.

Attack Surface Discovery Report			PS Credits = 12
Stage	**Scope**	**Include**	**Description**
Attack Surface Posture Analysis	A Zscaler Account Representative will run the Internet attack surface discovery report for one (1) domain across these areas of focus:	✓	Known Vulnerabilities
		✓	SSL/TLS Weakness
		✓	Exposed Servers
		✓	Namespace Exposure
		✓	Public Cloud Instances
Recommendations	The Attack Surface Discovery report results will be mailed to you and a meeting to discuss the outcomes is recommended.	✓	The tool queries for information that is publicly available without sending any active traffic to your environment. Findings are analyzed and consolidated into a comprehensive report.
		✓	Review and meet to discuss how we can help you reduce your attack surface, and minimize risk to your business
Engagement	A remote Zscaler resource will run this report on your behalf once the request has been received.		
Delivery Method	Your Attack Surface Discovery Report will be sent to you via email within 5 days from request.		
Prerequisites	• Customer must provide their domain name to run the report		
Note on Sensitivity of Data:	Due to the sensitive nature of data involved please note: • The tool does NOT touch or scan any part of the customer's infrastructure • The tool only analyzes publicly available information, and centralizes it in a way that makes it easy for customers to see where they are exposed • The tool only shows what is visible to anyone on the Internet		
Terms and Conditions	Zscaler Deployment and Professional Services Terms and Conditions		

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform.
Learn more at zscaler.com or follow us on Twitter @zscaler.

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com