CYBER RATINGS.ORG

Introducing Spot Check

We Test. You Trust.

January 2024

The Challenge: Security Verification

In the realm of Security Service Edge (SSE), the transition from operational management to strategic oversight presents new challenges for organizations.

This involves:

- Ensuring the SSE provider maintains the system effectively.
- Assessing the impact of policy changes on security.
- Verifying the effectiveness of the SSE solution within the organization's security framework.

Cybersecurity is a black box; Security Service Edge is a black box in a black box.

- It is a lot harder to test SSE than traditional network security products.
- Enterprises don't always have the time or expertise to build a test environment.
- Many of the tools required to test SSE are not yet commercially available.

How Do You Know? Verify with Spot Check.

Introducing Spot Check

Trust but Verify: A Timeless Principle Applied to Cybersecurity

CyberRatings “**Spot Check”** is a service designed to provide organizations with the assurance they need. Spot Check doesn't just test; it verifies. It provides an independent evaluation of SSE solutions, verifying that they are delivering on their promise of protection.

- **Objective Assessment**: "Spot Check" evaluates your SSE's ability to defend against the latest threats, offering an objective assessment of your cybersecurity posture.
- **Real-World Scenarios**: By testing your actual deployments, "Spot Check" ensures that your SSE solutions are battle-tested and ready for the challenges they will face.
- **Policy Change Evaluation**: When policies change, "Spot Check" helps you understand the security implications, ensuring that your modifications don’t adversely impact your security posture.

Confidence comes from verification.

Unique Features

Cipher Suite Support

Testing will determine which cipher suites are supported.

False Positive Rate

The rate at which the SSE blocks legitimate traffic.

Exploits & Malware Delivered Over HTTP

The rate at which exploits & malware delivered over HTTP are blocked.

Exploits Delivered Over HTTPS

The rate at which exploits & malware delivered over HTTPS are blocked.

Evasions

Threat actors use evasion techniques to disguise and modify attacks at the point of delivery to avoid detection by security products.

Version	(Value)	Cipher Suites	Prevalence
TLS 1.3	(0x13, 0x02)	TLS_AES_256_GCM_SHA384	66.51%
TLS 1.2	(0xC0, 0x30)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	11.85%
TLS 1.2	(0xC0, 0x2F)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	9.26%
TLS 1.3	(0x13, 0x01)	TLS_AES_128_GCM_SHA256	8.07%
TLS 1.2	(0xCC, 0xA8)	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	1.72%
TLS 1.2	(0xC0, 0x28)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	0.68%
TLS 1.3	(0x13, 0x03)	TLS_CHACHA20_POLY1305_SHA256	0.55%
TLS 1.2	(0xC0, 0x2C)	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0.42%
TLS 1.2	(0xCC, 0xA9)	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0.27%
TLS 1.2	(0xC0, 0x2B)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0.20%

- **HTTP Evasions**
  - HTTP Headers
  - HTTP Chunked Encoding
  - HTTP Compression
- **HTML**
- **XML**
- **JSON**
- **Multipart/form-data**
- **Portable Executable**
- **Layered Evasions**

4,000+ Exploits

10,000+ Malware Downloads

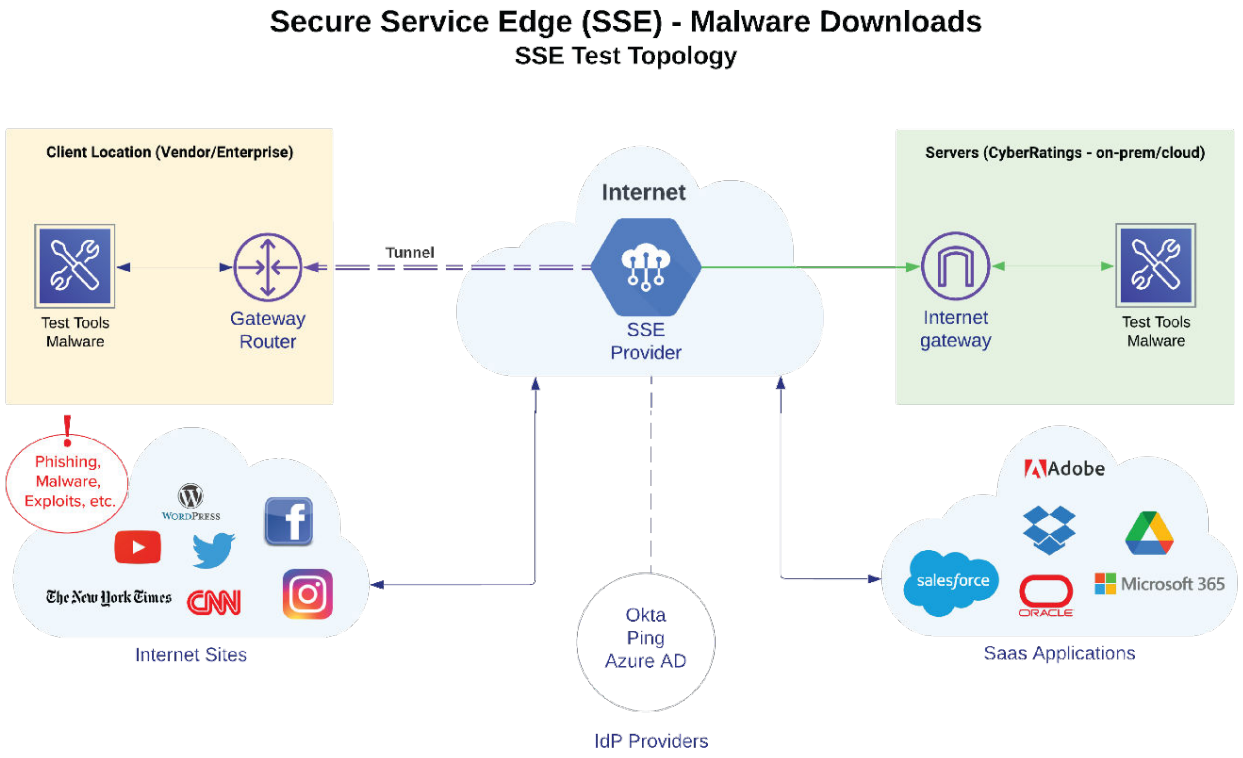
12,000+ Evasions

Customer's SSE configuration

CRO Live Network & Targets

Technical Overview

- TLS/SSL Functionality
- Protection vs Malware Download
- Protection vs. Exploits
- Resistance to Evasions
- False Positive Rate



CYBER RATINGS.ORG — SSE Spot Check for <Company Name>

<Vendor><Product/Service> <Date>

OVERVIEW

On *January 22, 2024* CyberRatings.org conducted an independent spot check for <Company Name> of the <Vendor> <Product/Service> from our cloud testing facility in Austin, Texas. <Vendor> was tested to measure the effectiveness of its protection against #,### exploits, ##,### malware samples, and whether any of ##,### evasions could bypass defenses. CyberRatings.org also tested to determine whether the service provided functional support for TLS/SSL 1.2 and 1.3 encrypted traffic using the most prevalent cipher suites.

100% SECURITY EFFECTIVENESS

Exploit Protection	100%
Malware Protection	100%
Resistance to Evasions	100%
False Positive Testing	100%
TLS/SSL Functionality	100%

Threat Prevention		Samples Tested	Samples Blocked	Blocked %
Exploit Protection		###	###	###%
Wild Exploits		###	###	###%
Exploit Library		###	###	###%
Critical	9.0-10.0	###	###	###%
Very High	8.0-8.9	###	###	###%
High	7.0-7.9	###	###	###%
Medium	6.0-6.9	###	###	###%
Malware Protection		###	###	###%
Wild Malware		###	###	###%
Malware Library		###	###	###%
Resistance to Evasions		###	###	###%
HTTP Evasions		###	###	###%
HTML Evasions		###	###	###%
XML Evasions		###	###	###%
JSON Evasions		###	###	###%
Multipart/Form-Data Evasions		###	###	###%
Portable Executable (packed, archived, etc.)		###	###	###%
Layered Evasions		###	###	###%
False Positive Rate		###	###	###%

SSL/TLS Functionality

Version	Prevalence	Cipher Suites	Results
TLS 1.3	66.51%	TLS_AES_256_GCM_SHA384 (0x13, 0x02)	Pass/Fail
TLS 1.2	11.85%	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)	Pass/Fail
TLS 1.2	9.26%	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)	Pass/Fail
TLS 1.3	8.07%	TLS_AES_128_GCM_SHA256 (0x13, 0x01)	Pass/Fail
TLS 1.2	1.72%	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA8)	Pass/Fail
TLS 1.2	0.68%	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28)	Pass/Fail
TLS 1.3	0.55%	TLS_CHACHA20_POLY1305_SHA256 (0x13, 0x03)	Pass/Fail
TLS 1.2	0.42%	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C)	Pass/Fail
TLS 1.2	0.27%	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA9)	Pass/Fail
TLS 1.2	0.20%	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2B)	Pass/Fail

Getting Started with Spot Check

How does it work?

Spot Check operates as a virtual employee that is added to the SSE policy being used by an organization. If the organization has multiple policies based on roles (e.g., Sales, Marketing, Engineering, Accounting, Executives) we recommend doing a Spot Check virtual employee for each user type.

Signing up for Spot Check is easy.

All you need to do is email us at spotcheck@cyberratings.org.

Confidence comes from verification.

About Us

We Test. You Trust.

CyberRatings.org (CRO) is a non-profit member organization dedicated to providing confidence in cybersecurity products and services through our research and testing programs.

3,200+ members from around the world include:

- Security Vendors
- Technology Companies
- Financial Services
- IT Services / MSPs
- International, Federal / State / Local Governments
- Healthcare
- Oil & Gas
- Retail
- Entertainment
- Manufacturing

We are a world-class lab you can hire and a non-profit dedicated to sharing our knowledge of how to build, manage, and apply testing to answer the tough questions.