

Attack Surface Report

Sample Report

About This Report

An Attack Surface is the number of points, or attack vectors, across your IT network where unauthorized users could exploit vulnerabilities to gain access to systems, extract confidential data, and stage an attack.

As new technologies, services, and connections are introduced, your Attack Surface expands, increasing the number of attack vectors and the overall risk for your business. By taking the time to understand, measure, and reduce your attack surface, you can improve your cyber security posture and prevent attacks.

This report leverages open-source data to measure your External Attack Surface, including possible attack vectors externally accessible to the internet. You can complement this report by increasing your situational awareness across your entire IT network, including endpoints, network, and cloud environments.











About Field Effect

Field Effect, a global cyber security company, is revolutionizing the industry by bringing advanced cyber security solutions and services to businesses of all sizes. After years of research and development by the brightest in the business, we have pioneered a holistic approach to cyber security.

Our complete Managed Detection and Response (MDR) solution, flexible simulation-based training platform, and expert-led professional services form a unified defence that results in superior security, less complexity, and immediate value. We build solutions that are sophisticated, yet easy to use and manage, so every business owner can get the hands-free cyber security they expect. For more information, visit fieldeffect.com.



Table of Contents

 Executive Summary.....	3
 1. End of Life (EOL) Software.....	4
 2. End of Life (EOL) Operating Systems.....	5
 3. Potentially Vulnerable Systems.....	6
 4. Remote Access	7
 5. Email (SPF and DMARC)	8
 6. Industrial Control Systems (ICS)	9
 7. Internet of Things (IOT).....	10
 8. Insecure Protocols	11
 9. Transport Layer Security (TLS)	12
 10. Certificates	13
 11. Databases	14
 12. Other Issues.....	15
About the Data Source	16
Full Logs (Annex A)	17

Executive Summary

Overall Risk: High



A high number of security issues were noted in the automated analysis of your organization's Internet-facing IP addresses. It is recommended that your organization develop a plan (including necessary resources) to remediate the most serious issues asap.

Next Steps

The following actions are recommended to improve your organization's cybersecurity posture:

1. Upgrade end-of-life software and/or operating systems to supported versions asap.
2. One or more open ports were detected that should never be available from the Internet. Firewall rules should be added immediately to correct the issue. See Section 12 of this report for more details.
3. Disable all default webpages as these websites are highly vulnerable.
4. Ensure IPs flagged with possible vulnerabilities are fully patched.
5. Consider installing a holistic cyber security monitoring product such as Field Effect's Covalence on your organization's network, to increase visibility of your entire attack surface and stop cyber threats.

1. End of Life (EOL) Software

An EOL product is a software application which is at the end of its product lifecycle and is no longer receiving updates, including security updates. EOL products are particularly vulnerable to hacking as they often have publicly known exploits for which there is no patch.

Analysis Results



- The following EOL software products were found in your organization's Internet-facing IP space:

-lighttpd

It is recommended that these applications be upgraded as soon as possible.

2. End of Life (EOL) Operating Systems

An EOL operating system is at the end of its product lifecycle and is no longer receiving updates, including security updates. EOL operating systems are particularly vulnerable to hacking as they often have publicly known exploits for which there is no patch.

Analysis Results



- No Internet-facing EOL operating systems were noted during the analysis.

3. Potential Vulnerabilities

Hackers and security researchers are constantly looking for new vulnerabilities in computer systems and software. When new vulnerabilities are disclosed publicly they are given a designator under the Common Vulnerabilities and Exposures (CVE) system to track them.

Analysis Results



- A total of 36 known vulnerabilities (CVEs) for 2 IP(s) were noted on your Internet-facing infrastructure. See Annex A for more details.

These IPs warrant special attention for patching and Covalence protection.

4. Remote Access

Remote Access includes protocols like RDP, VNC, and TeamViewer that allow remote administration of computers. It could also include the administration interface of an important network device like a firewall or router.

Analysis Results



- The following remote access issues were detected during the automated analysis:

- Cisco Web VPN
- Fortinet Login
- Tandberg Admin Console

It is recommended that the necessity of having these services available from the Internet be assessed. See Annex A for more details.

5. Email (SPF and DMARC)

SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting and Conformance) are security configurations that are added to servers to increase the security of email.

SPF and DMARC help protect your domain against spoofing and decrease the chances that messages originating from your organization will be marked as spam.

Analysis Results

DMARC

- Record not found for domain: example.com

SPF

- Record found for domain: example.com

6. Industrial Control Systems (ICS)

ICS devices are used for industrial processes or building automation. They should never be positioned to allow inbound connections from the Internet because they typically have no or weak authentication and were not designed with security as a top priority.

Analysis Results



- No ICS systems were noted during the analysis.

7. Internet of Things (IOT)

IOT devices such as smart lightbulbs and door locks should never allow inbound connections from the Internet due to their simple design and lack of security. IOT devices provide an excellent entry point for threat actors, who can then move laterally to internal IP addresses.

In 2018 hackers were able to steal customer data from a casino database server by first gaining access to their network via an internet-connected aquarium thermometer ([Link](#)).

Analysis Results



- No IOT systems were noted during the analysis.

8. Insecure Protocols

Older Internet protocols such as FTP and POP3 are plaintext and typically only protected with a single factor of authentication (password). Their use should be limited and reviewed frequently with the goal of complete removal.

If your organization is still running insecure websites on TCP/80 (HTTP) we recommend moving to TLS (HTTPS) only.

Analysis Results



- The following insecure protocols are likely in use on your network:

- FTP (TCP/21)
- HTTP (TCP/80)
- HTTP (TCP/88)
- HTTP (TCP/9000)
- SNMP (UDP/161)

See Annex A for more details.

9. Transports Layer Security (TLS)

Transport Layer Security (TLS) is a critical security protocol used to protect web traffic. It provides confidentiality and integrity of data in transit between clients and servers exchanging information.

Several encryption standards in the TLS/SSL families have been deprecated since 2011. The driving force behind the deprecation process was the large number of attacks which impacted the cryptographic algorithms at the base of the two protocols. This included attacks such as [BEAST](#), [POODLE](#), and [LUCKY 13](#), all of which showed how attackers could take advantage of weaknesses in both SSL and TLS 1.0/1.1 to compromise encrypted communications and attack organizations.

Analysis Results



- The following deprecated encryption protocols were noted during the analysis:

- TLSv1
- TLSv1.1

It is recommended that the necessity of having these protocols available be assessed. See Annex A for more details.

10. Certificates

SSL Certificates are files used to establish secure communications channels between servers and visitors (clients). Without certificate-based encryption, Internet traffic is vulnerable to eavesdropping and man-in-the-middle attacks.

Expired certificates, the use of wildcard certificates, and self-signed certificates can increase your organization's level of risk and impact your reputation.

Analysis Results



- The following certificate issues were noted during the analysis:

- Self-signed Certificates
- Wildcard Certificates

See Annex A for more details.

11. Databases

Organizations should be wary of directly connecting database servers to the Internet, as they typically lack multifactor authentication and present an enticing target to cybercriminals. These criminals are increasingly stealing the records from databases to extort their victims into large payments.

Analysis Results



- No database servers were noted during the analysis.

12. Other Issues

Other security issues were noted on your network during the automated analysis. These issues may impact the privacy of your organization or increase the chances that an attacker can gain control of one of your Internet-facing devices.

Analysis Results



- The following additional issues were noted:
 - LDAP server directly connected to the Internet
 - Open Directory Listing
 - Windows IIS Server Default Page

Analytic Observations

- One or more Windows webservers running IIS Version 8.5 were noted for your organization. Security updates and other support for this software will cease in October 2023.
- One or more Fortinet devices are noted in this report. These devices should be regularly patched and used with caution as they have had numerous serious security issues over the last 5 years.

About the Data Source

The data for this report was retrieved from Shodan (www.shodan.io), and other publicly available sources. The Shodan service regularly scans the entire Internet on well-known ports looking for connected devices. It is used extensively by security researchers like those at Field Effect but has been dubbed “The World’s Most Dangerous Search Engine” because it is also heavily leveraged by hackers to find exploitable networks.

At no point during this analysis were any penetration testing activities directed at your organization’s networks. All the data contained in this report is publicly available to both security researchers and hackers alike.

Annex A: Full Output Logs

See an IP you don't recognize? This could be the result of stale Domain Name System (DNS) records. DNS records should be regularly audited to ensure they are still required and only point to trusted infrastructure.

No Log Output Selected