Sassie

Company Overview Report

760

SECURITY RATING

Date Created

2023-02-21

BitSight Technologies Inc.

https://www.bitsight.com/

BITSIGHT

TABLE OF CONTENTS

* Risk vector does not currently affect Security Ratings
** Informational risk vector (will never affect Security Ratings)

This report was created for Sassie, by BitSight Technologies. It is a snapshot of the company's BitSight Security Rating performance during the past year, as of **February 20, 2023**.

BitSight Security Rating

760 ADVANCED

Rating Related Risk

Ransomware Incidents vs a **< 750** company

Half as Likely

Data Breach Incidents vs a **< 700** company

Half as Likely

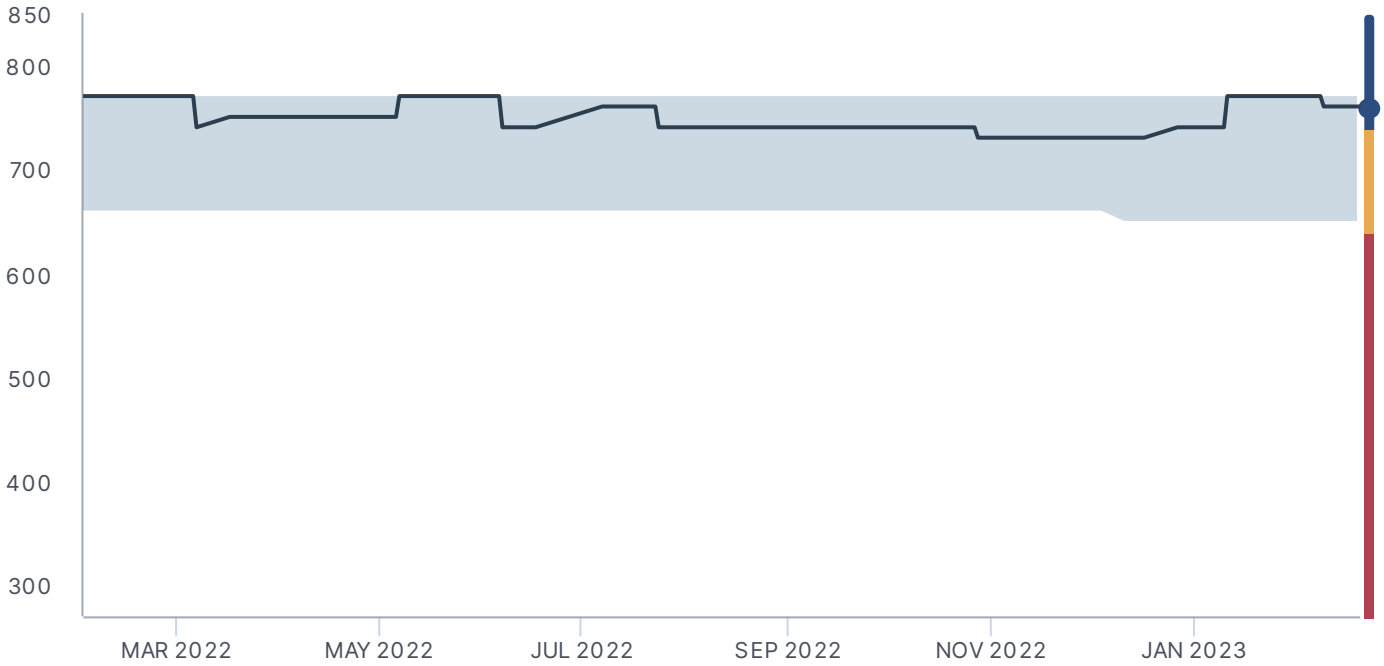
Company Info

Subscription	**Total Risk Monitoring**
Relationship	**My Company**
Monitored by	**1 company**
Homepage	**sassieshop.c...**
Industry	**Technology**
IP addresses	**6**
Searched by	**58 users**
Company ID	**Unassigned**

Security Ratings

770
Highest on 8 Feb 2023

730
Lowest on 28 Oct 2022



Technology Industry Range

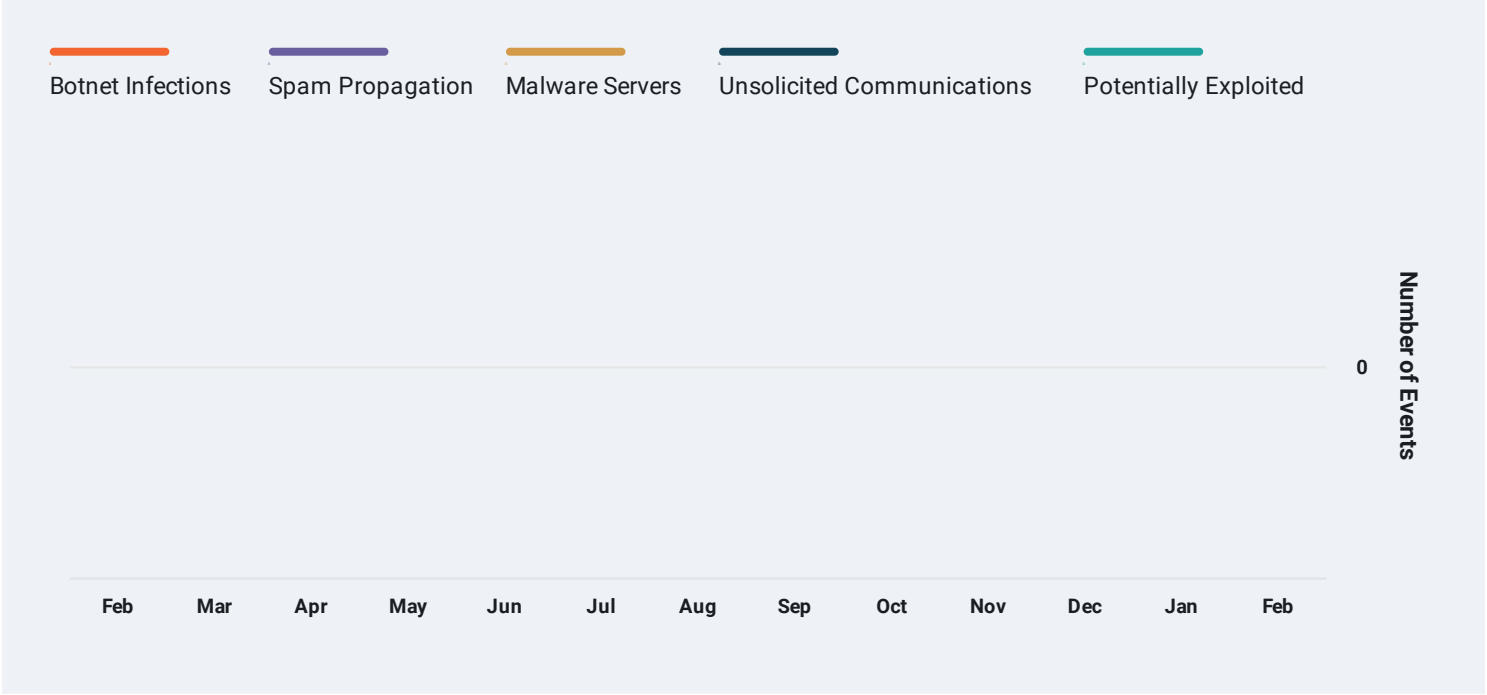
BASIC 250-630 INTERMEDIATE 640-730 ADVANCED 740-900

Compromised Systems

Compromised Systems are devices or machines in an organization's network that show symptoms of malicious or unwanted software. These compromises can disrupt daily business operations and can increase an organization's risk of breach.

Compromised Systems are evaluated based on the number and type of malware, the severity, and the duration. For each risk vector, an overall letter grade is calculated from evaluations of each instance of compromise.

For example, an organization could have an "F" for botnet infections, if they either had many botnets in a short period, or a few persistent botnets over months.



A Botnet Infections

Top 10%

Botnet Infections

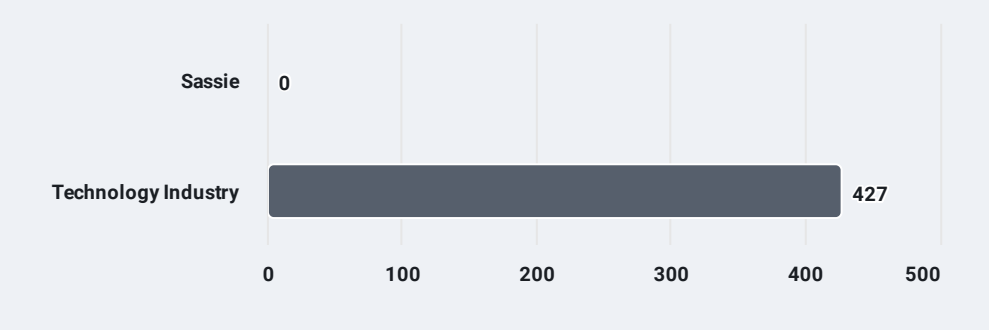
Botnet Infection events indicate that devices on a company's network were observed participating in botnets as either bots or Command and Control servers. Botnets can be used to exfiltrate corporate secrets and sensitive customer information, repurpose company resources for illegal activities, and serve as conduits for other infections.

Remediation Suggestions

- Conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

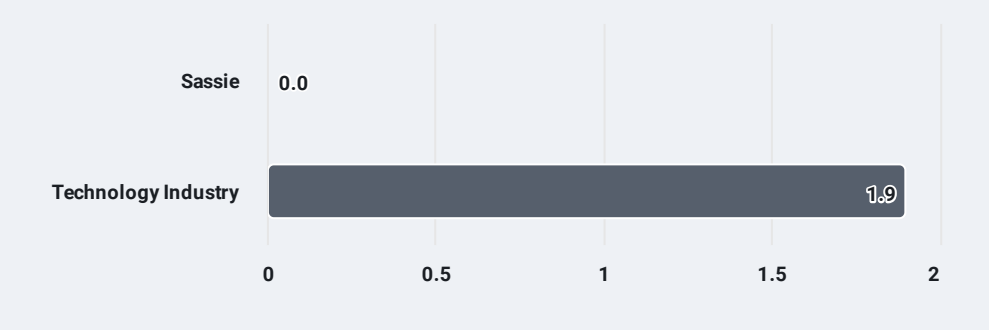
Event Counts over past year

No data to compare with the Technology industry.



Average Days to resolve events over past year

No data to compare with the Technology industry to resolve events.



Top Findings

Identifier	First Seen	Last Seen	Duration	Severity	Details

There are no findings currently affecting this risk vector.

A Spam Propagation

Top 10%

Spam Propagation

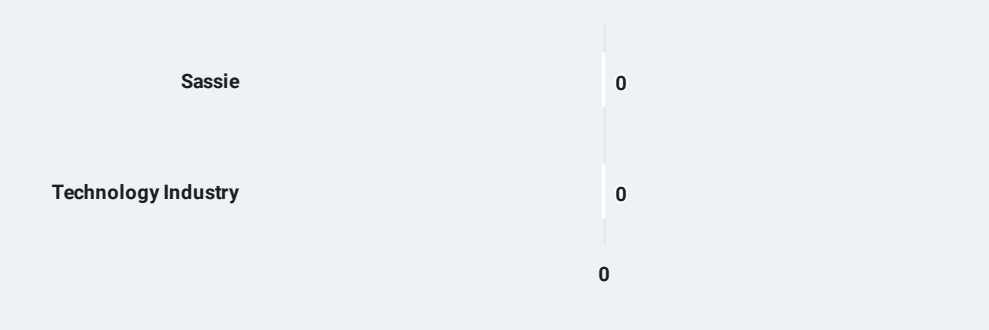
Spam Propagation events are observed when devices on a company's network are sending unsolicited commercial or bulk email. This type of activity can damage a company's reputation and cause legitimate company email to be caught in spam filters.

Remediation Suggestions

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

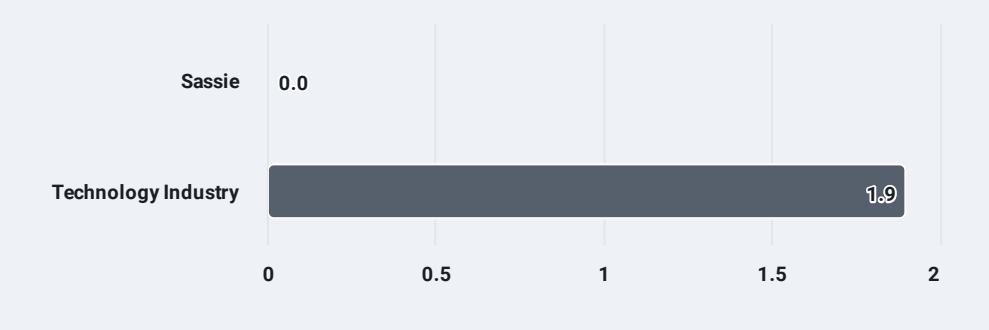
Event Counts over past year

No data to compare with the Technology industry.



Average Days to resolve events over past year

No data to compare with the Technology industry to resolve events.



Top Findings

Identifier	First Seen	Last Seen	Duration	Severity	Details

There are no findings currently affecting this risk vector.

A Malware Servers

Top 10%

Malware Servers

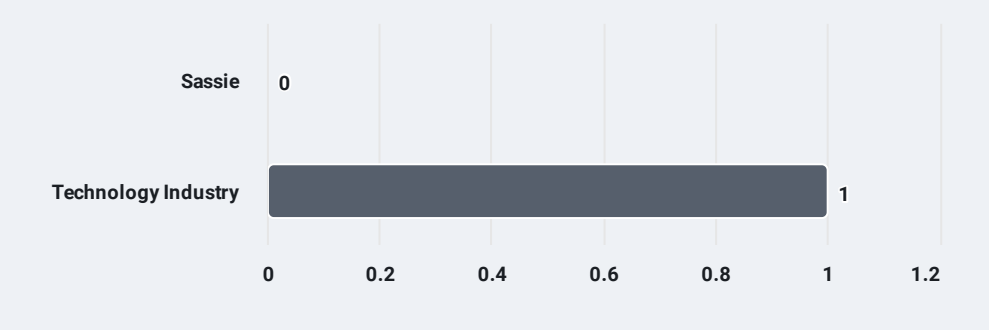
Malware Server events occur when servers are observed engaging in malicious activity, such as hosting phishing, fraud or scam sites. Compromised servers can put employees and customers at risk by infecting devices that connect to company resources.

Remediation Suggestions

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

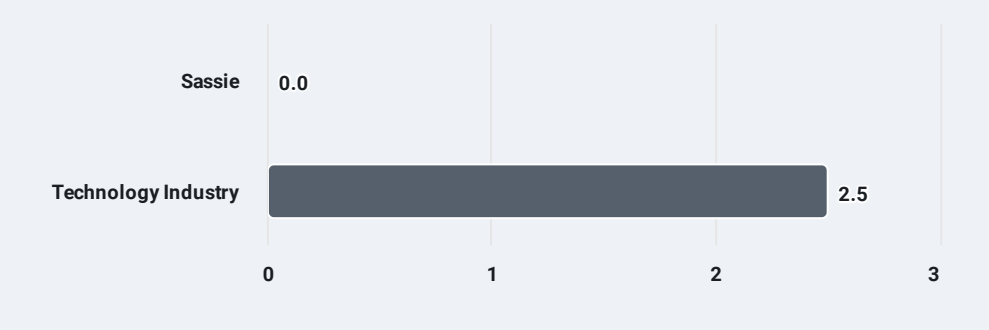
Event Counts over past year

No data to compare with the Technology industry.



Average Days to resolve events over past year

No data to compare with the Technology industry to resolve events.



Top Findings

Identifier	First Seen	Last Seen	Duration	Severity	Details

There are no findings currently affecting this risk vector.

A Unsolicited Communications

Top 10%

Unsolicited Communications

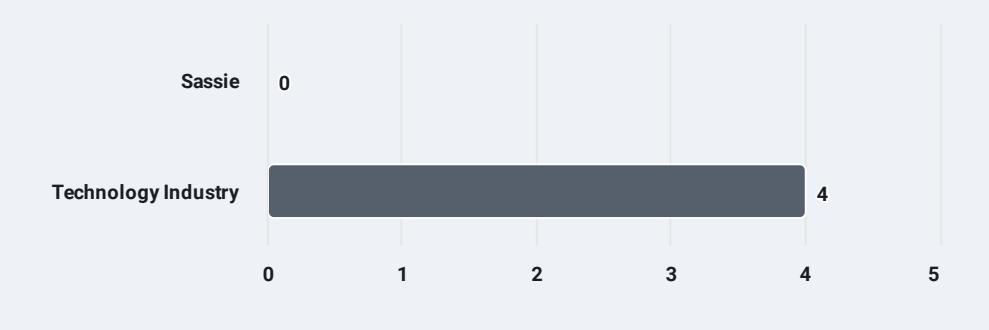
Unsolicited Communications events occur when devices attempt to communicate with servers that are not hosting any useful services. This type of activity not only shows that a device is compromised, but that it is actively seeking other devices to infect.

Remediation Suggestions

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

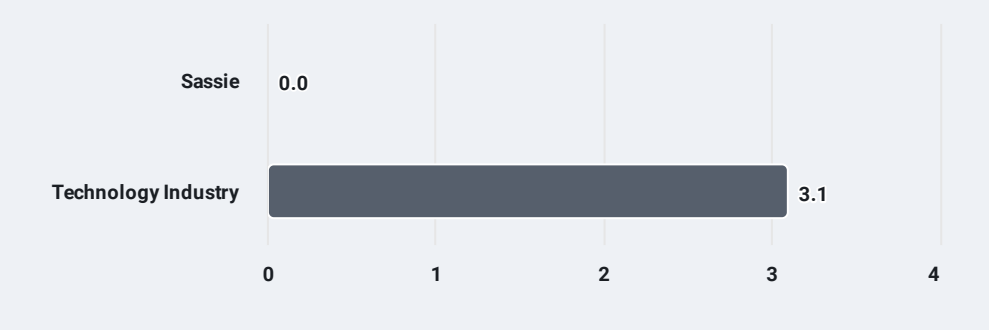
Event Counts over past year

No data to compare with the Technology industry.



Average Days to resolve events over past year

No data to compare with the Technology industry to resolve events.



Top Findings

Identifier	First Seen	Last Seen	Duration	Severity	Details

There are no findings currently affecting this risk vector.

A Potentially Exploited

Top 10%

Potentially Exploited

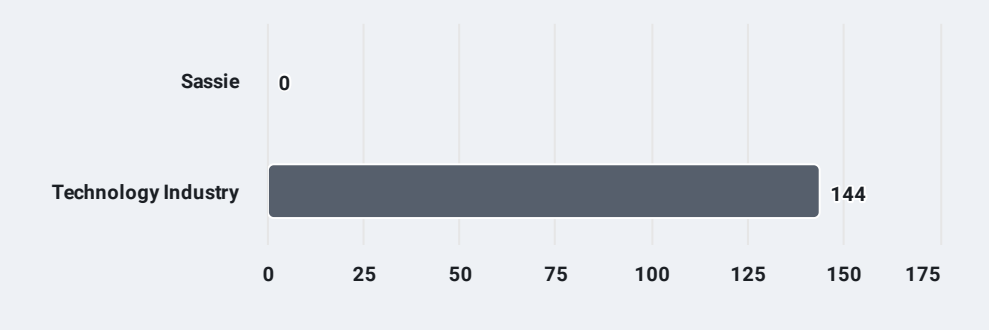
Potentially Exploited events occur when browsers on a company's network are infected with malware that is altering the user's experience, such as adware. These events are often indicative of other infections.

Remediation Suggestions

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

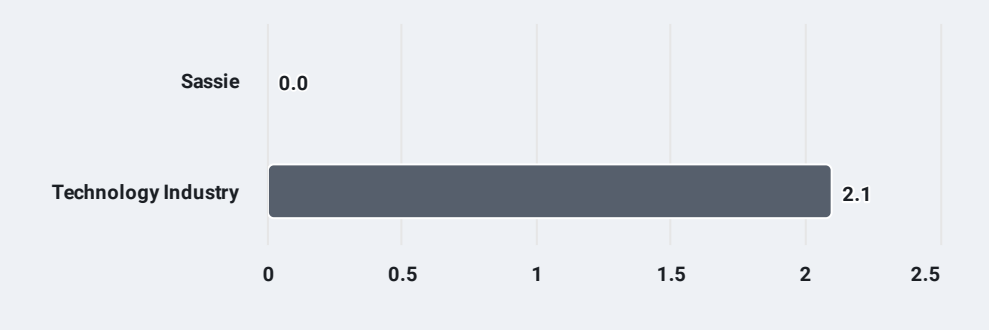
Event Counts over past year

No data to compare with the Technology industry.



Average Days to resolve events over past year

No data to compare with the Technology industry to resolve events.



Top Findings

Identifier	First Seen	Last Seen	Duration	Severity	Details

There are no findings currently affecting this risk vector.

Diligence

Diligence risk vectors show steps a company has taken to prevent attacks. BitSight currently evaluates SPF, DKIM, TLS/SSL, Open Port and DNSSEC information in assessing a company's security diligence.

All diligence records are evaluated as one of the following: Good, Fair, Warn, Bad or Neutral. Records are assessed using industry-standard criteria. For each diligence risk vector, an overall letter grade is calculated using the evaluations of each individual record.

For example, if a company has three domains, and each of them has an effective SPF record, their overall SPF grade would be an "A". Likewise, if none of the three domains have SPF records, their overall SPF grade would be an "F".

Records older than 60 days will not affect a company's Security Rating.

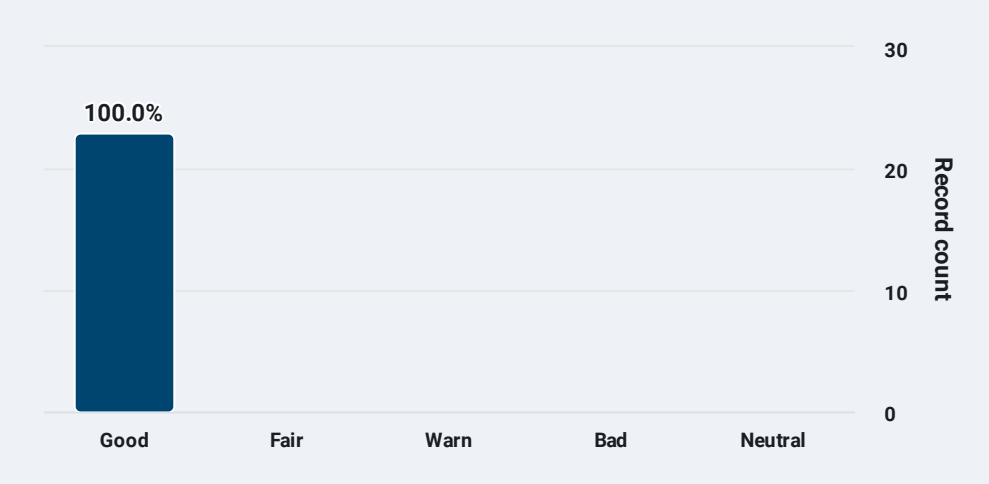
A SPF Domains

Top 10%

SPF Domains

Properly configured SPF records help ensure that only authorized hosts can send email on behalf of a company by providing receiving mail servers the information they need to reject mail sent by unauthorized hosts. BitSight verifies that a company has SPF records on all domains that are sending or have attempted to send email, and that they are configured in a way that helps prevent email spoofing.

Grade Distribution: **23** records



Remediation Suggestions

- Create an SPF record. and conduct a thorough security review of the machine (malware & antivirus sweep).
- Check for common mistakes in your SPF record.
- All domains should have SPF records, even SMTP servers and those that aren't configured to send mail. If a company does not intend to send mail from a domain, an attacker can still use that domain to spoof email.

Identifier	First Seen	Last Seen	Grade	Severity	Details
_spf.sassieshop.com	2022-10-25	2023-02-20	GOOD	Minor	
mail.sassieshop.com	2022-02-15	2023-02-20	GOOD	Minor	
surfrelay.sassieshop.com	2021-12-05	2023-02-20	GOOD	Minor	
bems-prod-1.sassieshop.com	2021-11-29	2023-02-20	GOOD	Minor	
bems-prod-9.sassieshop.com	2021-11-29	2023-02-20	GOOD	Minor	
bems-prod-10.sassieshop.com	2021-12-04	2023-02-20	GOOD	Minor	
bems-prod-bare-2.sassieshop.com	2022-03-14	2023-02-20	GOOD	Minor	
bems-prod-2.sassieshop.com	2021-11-30	2023-02-19	GOOD	Minor	
sassieshop.com	2022-02-17	2023-02-18	GOOD	Minor	

bems17.sassieshop.com	2022-04-11	2023-02-18	GOOD	Minor

Showing 10 out of 23 findings.
This risk vector has 23 total findings, in order to view them all please login to BitSight.

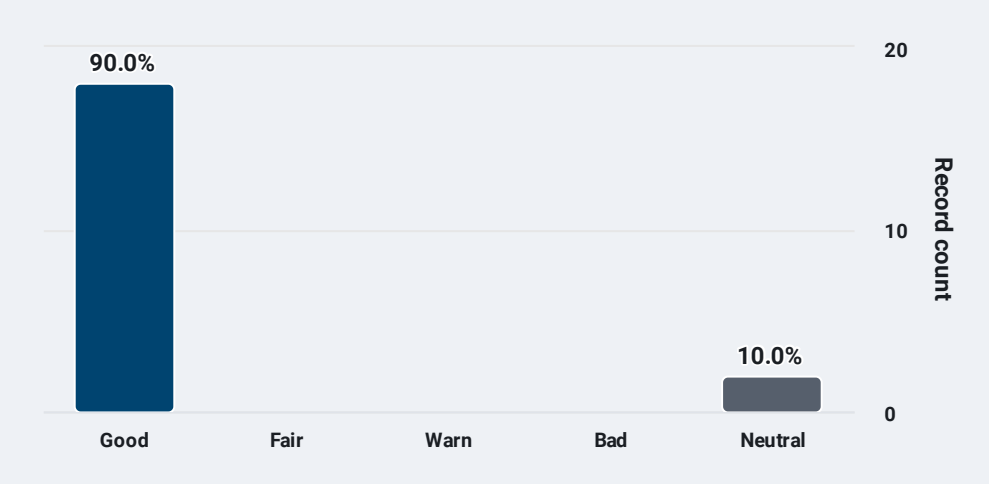
A DKIM Records

Top 10%

DKIM Records

Properly configured DKIM records can help ensure that only authorized hosts can send email on the behalf of a company. BitSight verifies that a company uses DKIM and has configured it in a way that prevents email spoofing.

Grade Distribution: **20** records



Remediation Suggestions

- Search for Diligence records and then implement an effective DKIM record if one does not already exist. Please see our comprehensive article on How to create a DKIM record.
- Generate a new RSA keypair, specifying a bit strength of 2048 or larger. For elliptic curve keys, a length of 224 bits is recommended. Refer to the recommended key length. We follow NIST recommendations regarding key length.
- Refer to the recommended key rotation for how often to generate a new RSA keypair.
- Check that your keys are properly stored and the DKIM record has the correct key.

Identifier	First Seen	Last Seen	Grade	Severity	Details
dkim.sassieshop.com	2021-12-04	2023-02-20	GOOD	Minor	
surfrelay2048._domainkey.sassieshop.com	2021-11-30	2023-02-20	GOOD	Minor	
sassieshop._domainkey.bems-prod-1.sassieshop.com	2022-01-07	2023-02-20	GOOD	Minor	
sassieshop._domainkey.bems-prod-9.sassieshop.com	2022-01-07	2023-02-20	GOOD	Minor	
sassieshop._domainkey.bems-prod-10.sassieshop.com	2022-01-07	2023-02-20	GOOD	Minor	
sassieshop._domainkey.bems-prod-bare-2.sassieshop.com	2022-03-15	2023-02-20	GOOD	Minor	

sassieshop._domainkey.bems-prod-2.sassieshop.com	2022-01-07	2023-02-19	GOOD	Minor
sassieshop._domainkey.bems-prod-bare-1.sassieshop.com	2022-03-23	2023-02-17	GOOD	Minor
default._domainkey.europe.sassieshop.com	2022-02-07	2023-02-13	GOOD	Minor
dkim2.sassieshop.com	2022-01-18	2023-02-11	GOOD	Minor

Showing 10 out of 20 findings.
This risk vector has 20 total findings, in order to view them all please login to BitSight.

A TLS/SSL Certificates

Top 10%

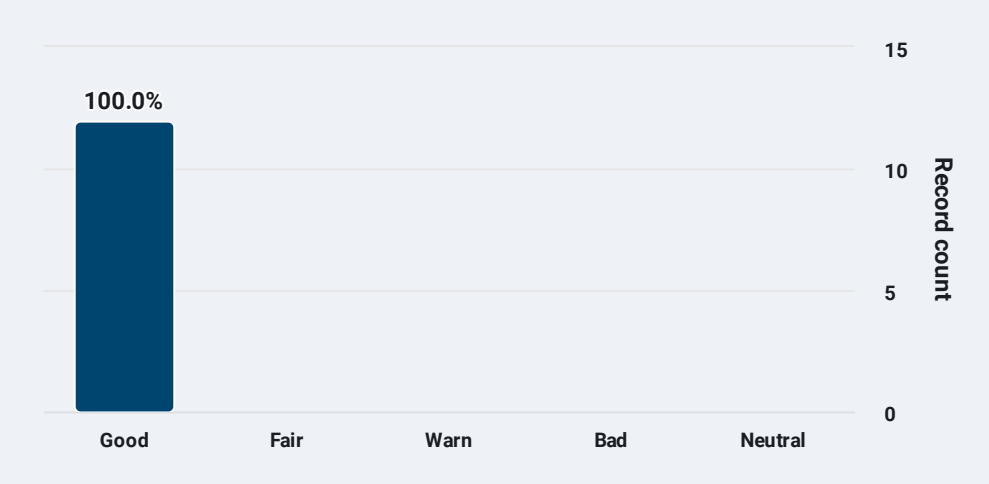
TLS/SSL Certificates

TLS/SSL certificates are used to encrypt traffic over the Internet. BitSight analyzes TLS/SSL certificates and provides information about their effectiveness. Certificates are responsible for verifying the authenticity of your company servers to your associates, clients, and guests, and serve as the basis for establishing cryptographic trust.

Remediation Suggestions

- Review the Certificate Authority Best Practices and implement effective TLS/SSL certificates.
- Obtain valid and up-to-date TLS certificates from an industry certificate authority.
- Select a stronger signature algorithm (like SHA-256).

Grade Distribution: **12** records



Identifier	First Seen	Last Seen	Grade	Severity	Details
*.europe.sassieshop.com	2022-12-24	2023-02-20	GOOD	Minor	
*.sassieshop2.com	2022-12-30	2023-02-20	GOOD	Minor	
great-mayer.54-251-213-121.plesk.page	2023-01-25	2023-02-19	GOOD	Minor	
site.sassieshop.com	2023-02-09	2023-02-15	GOOD	Minor	
mail.45-56-99-139.cprapid.com	2023-01-28	2023-02-05	GOOD	Minor	
site.sassieshop.com	2022-12-03	2023-01-22	GOOD	Minor	
great-mayer.54-251-213-121.plesk.page	2022-11-26	2023-01-20	GOOD	Minor	
bems10.sassieshop.com	2023-01-17	2023-01-18	GOOD	Minor	
inbake.com	2023-01-04	2023-01-14	GOOD	Minor	
*.sassieshop2.com	2022-10-29	2022-12-28	GOOD	Minor	

Showing 10 out of 12 findings.
This risk vector has 12 total findings, in order to view them all please login to BitSight.

A TLS/SSL Configurations

Top 10%

TLS/SSL Configurations

Evaluates TLS/SSL server configurations, which includes whether a company's servers have correctly configured security protocol libraries, and support strong encryption standards when making encrypted connections to other machines. Incorrect or weak configurations may make servers vulnerable to certain attacks (POODLE, Heartbleed).

Grade Distribution: **16** records

Remediation Suggestions

- Update and keep server implementations of TLS/SSL (OpenSSL, LibreSSL, etc); latest versions are patched against known vulnerabilities and they have countermeasures for other attacks.
- Refer to the TLS 1.0 and 1.1 deprecation schedule to see how this risk vector will be affected. Disable SSL v2, SSL v3, TLS 1.0, and TLS 1.1. Migrate to a minimum of TLS 1.2. Migrating to a later version (TLS 1.2 or TLS 1.3) is strongly encouraged.
- Regenerate Diffie-Hellman primes to be 2048 bits.
- Refer to the Guide to Deploying Diffie-Hellman for TLS to configure TLS securely.

Identifier	First Seen	Last Seen	Grade	Severity	Details
sassieshop2.com:443	2022-09-14	2023-02-20	GOOD	Minor	
prod.sassieshop.com:443	2022-01-27	2023-02-19	GOOD	Minor	
54.251.213.121:8443	2021-12-05	2023-02-16	GOOD	Minor	
54.251.213.121:443	2021-11-29	2023-02-13	GOOD	Minor	
198.58.119.44:25	2023-01-11	2023-02-04	GOOD	Minor	
45.56.99.139:110	2023-01-28	2023-02-04	GOOD	Minor	
45.56.99.139:443	2023-02-02	2023-02-04	GOOD	Minor	
av.sassieshop.com:443	2022-08-18	2023-02-03	GOOD	Minor	
45.56.99.139:465	2023-01-31	2023-02-03	GOOD	Minor	
45.56.99.139:587	2023-02-03	2023-02-03	GOOD	Minor	

Showing 10 out of 16 findings.
This risk vector has 16 total findings, in order to view them all please login to BitSight.

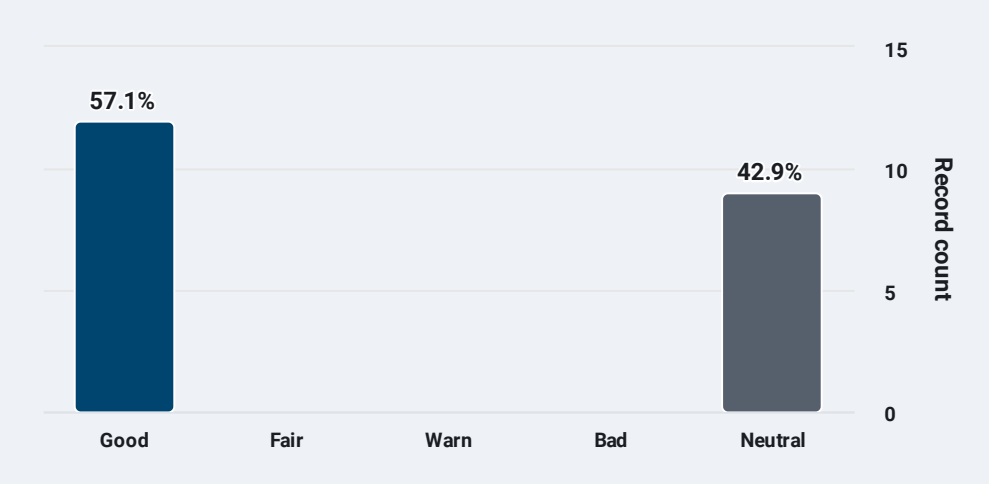
A Open Ports

Top 10%

Open Ports

Open Ports shows which port numbers and services are exposed to the Internet. Certain ports must be open to support normal business functions; however, unnecessary open ports provide ways for attackers to access a company's network.

Grade Distribution: **21** records



Remediation Suggestions

- Embedded in every packet of network communication is the port number for that communication, which can be used to identify and block unwanted attempts to communicate over certain ports or ranges of ports not used by the company. Close unnecessary open ports.
- Audit the services running on a particular machine and ensure only vital services are running.
- Set up access to required services over a Virtual Private Network (VPN).
- Block specific or ranges of ports not used by the company in the company edge network infrastructure. The port number is embedded in every packet of network communication, which can be used for port identification. View the full list of network ports in the IANA Service Name and Transport Protocol Port Number Registry.

Identifier	First Seen	Last Seen	Grade	Severity	Details
54.251.213.121:80	2021-11-28	2023-02-16	NEUTRAL	Minor	Detected service: HTTP
54.251.213.121:8443	2021-12-05	2023-02-16	GOOD	Minor	Detected service: HTTPS
54.251.213.121:443	2022-09-19	2023-02-13	GOOD	Minor	Detected service: HTTPS
54.251.213.121:22	2021-12-20	2023-02-09	GOOD	Minor	Detected service: SSH (OpenSSH_8.2p1)
54.251.213.121:53	2021-11-29	2023-02-07	NEUTRAL	Minor	Detected service: DNS
52.86.30.179:80	2022-05-02	2023-02-07	NEUTRAL	Minor	Detected service: HTTP
45.56.99.139:110	2023-02-03	2023-02-05	GOOD	Minor	Detected service: POP3 with STARTTLS
198.58.119.44:25	2023-01-11	2023-02-04	GOOD	Minor	Detected service: SMTP with STARTTLS
45.56.99.139:443	2023-02-02	2023-02-04	GOOD	Minor	Detected service: HTTPS
45.56.99.139:465	2023-01-31	2023-02-03	GOOD	Minor	Detected service: SMTPS

Showing 10 out of 21 findings.
This risk vector has 21 total findings, in order to view them all please login to BitSight.

D Web Application Headers

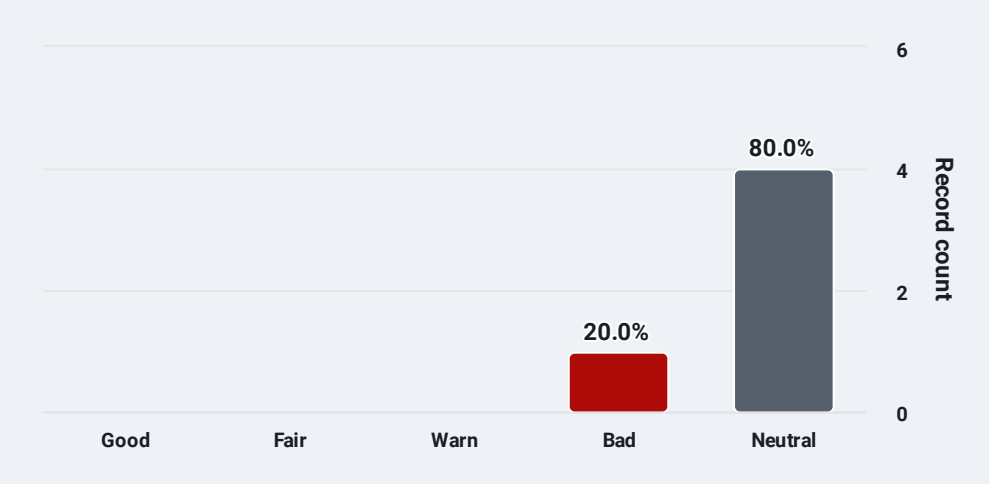
Bottom 30%

Web Application Headers

This risk vector analyzes security-related fields in the header section of HTTP request and response messages. If configured correctly, these fields can help provide protection against malicious behavior, such as man-in-the-middle and cross-site scripting attacks. Different types of headers are required for HTTP/1.0, HTTP/1.1, and HTTPS.

See the Knowledge Base for a list of required headers for each protocol.

Grade Distribution: **5** records



Remediation Suggestions

- Records that affect a company's Diligence grades have messages that provides an explanation and remediation. Refer to the Help and Remediation messages for additional details.
- Implement the required headers from the list of required headers and refer to the configuration requirements.
- Ensure application headers are created correctly and don't contain misspellings (typos).

Identifier	First Seen	Last Seen	Grade	Severity	Details
europe.sassieshop.com:443	2022-07-24	2023-02-20	NEUTRAL	Minor	Redirect
bems10.sassieshop.com:443	2023-01-17	2023-02-02	BAD	Material	No security headers are set
site.sassieshop.com:80	2022-06-11	2023-01-17	NEUTRAL	Minor	Redirect
www.sassieshop.com:443	2022-12-23	2023-01-15	NEUTRAL	Minor	Redirect
uat.sassieshop.com:443	2022-01-13	2023-01-13	NEUTRAL	Minor	Redirect

Showing 5 out of 5 findings.

A Patching Cadence

Top 10%

Patching Cadence

This risk vector evaluates how many systems in an organization's network infrastructure are affected by software vulnerabilities and how quickly the company resolved any issues. Vulnerabilities are publicly disclosed holes or bugs in software that can be used by attackers to gain unauthorized access to systems and data. Patches are updates to the affected software that resolve the vulnerability and close that particular avenue of attack.

Vulnerability Management Performance

Remediation Suggestions

- Conduct general housekeeping on company infrastructure. Keep software, hardware, operating systems, and supporting libraries up-to-date. Doing so can make it easier to patch systems in case vulnerabilities appear in the future.
- Ensure your operating systems and supporting libraries are up-to-date with the latest patches. Implement automatic updates for critical systems.
- Ensure new systems introduced into your corporate network are free of known vulnerabilities. Staying informed on the latest threats is a simple way to be aware of any possible risks your company could acquire when bringing any new devices onto your network.
- Find out how quickly your critical vendors are patching vulnerabilities. Your organization’s security posture may be strong, but even one weak link in your supply chain can pose significant risk.

Identifier	First Seen	Last Seen	Grade	Severity	Details

There are no findings currently affecting this risk vector.

A Insecure Systems

Top 10%

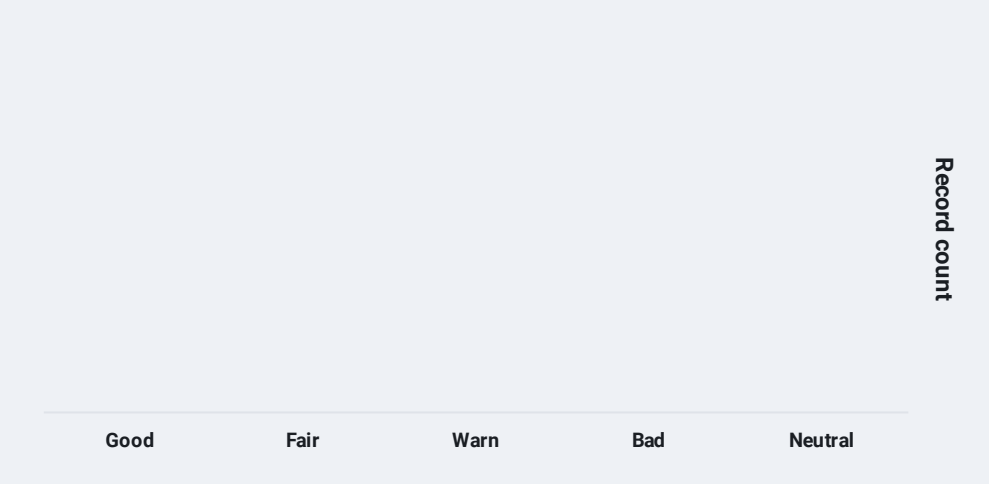
Insecure Systems

Insecure Systems is an indication of the number of an organization's endpoints that are communicating with an unintended destination. The software of these endpoints may be outdated, tampered with, or misconfigured. "Endpoints" refer to any desktop computer, server, mobile device, media system, or appliance that has internet access. A system is classified as "insecure system" when these endpoints try to communicate with a web domain that doesn't yet exist or isn't registered to anyone.

Remediation Suggestions

- Identify known insecure systems and uninstall or update the firmware of insecure applications (endpoints), as outlined in the remediation instructions for the record.

Grade Distribution: **0** records



Identifier	First Seen	Last Seen	Grade	Severity	Details

There are no findings currently affecting this risk vector.

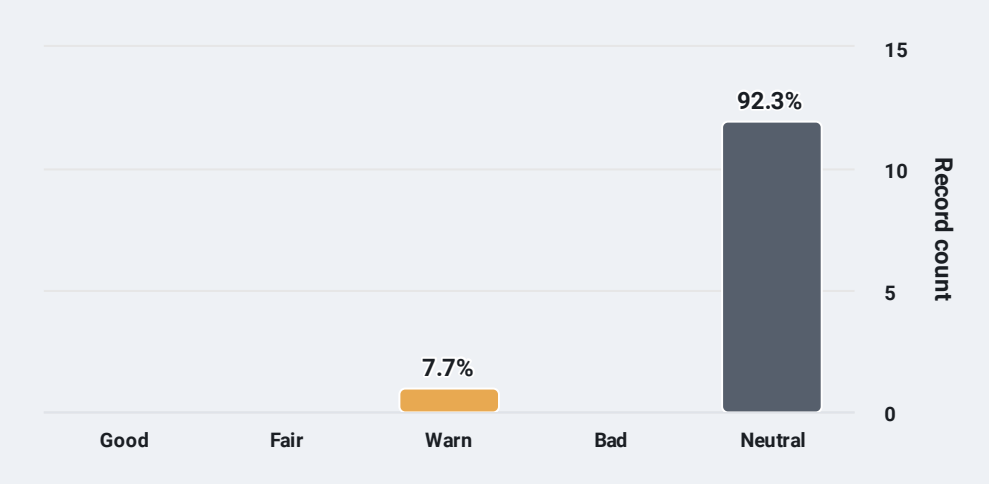
C Server Software

Bottom 50%

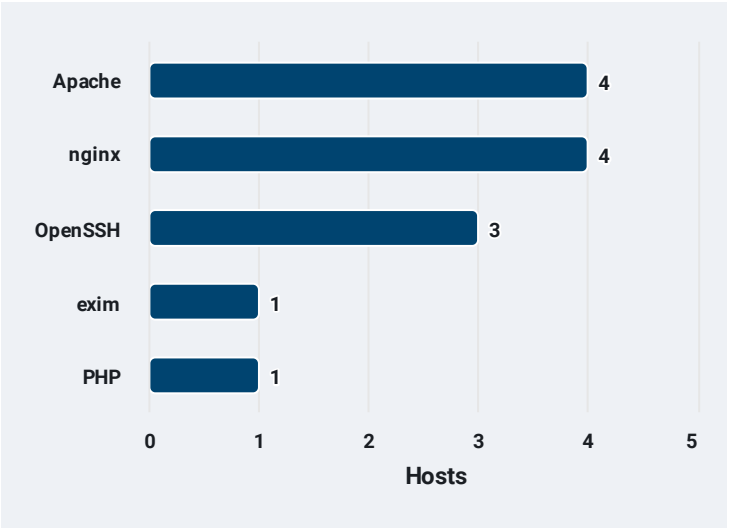
Server Software

The Server Software risk type can be used to create a rich picture about the software used by an organization. It helps track security holes created by server software that is no longer supported by its original developers or has become out-of-date (deprecated).

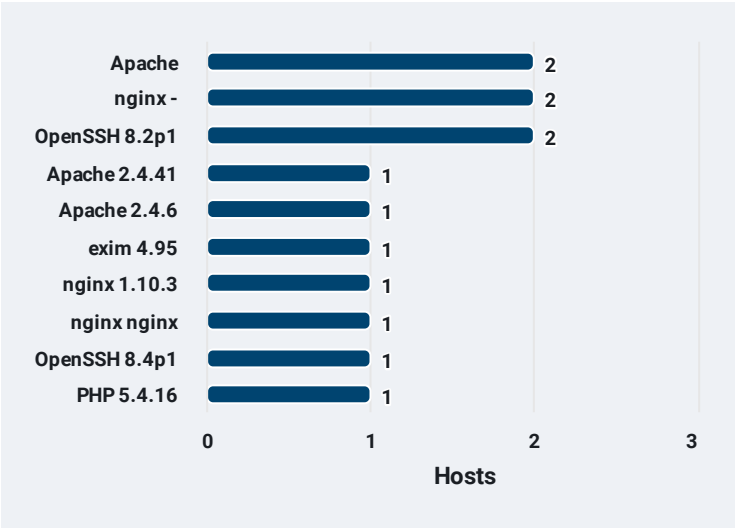
Grade Distribution: **13** records



Top Software Types



Top Software Versions



Remediation Suggestions

- Identify out-of-date server software installations and update them.
- Ensure the organization has critical server software set to auto-update, if applicable, and if some of the organization's production applications depend on certain unsupported versions, their software development teams will need to integrate the newer versions into their code base.
- Consult your operating system vendors' software repositories and release notes for more information on supported server software for your organization.

Identifier	First Seen	Last Seen	Grade	Severity	Details
54.251.213.121	2021-12-06	2023-02-19	NEUTRAL	Minor	Support status is unknown
54.251.213.121	2021-11-28	2023-02-16	NEUTRAL	Minor	Support status is unknown
54.251.213.121	2022-01-21	2023-02-14	NEUTRAL	Minor	Support status is unknown

52.86.30.179	2023-02-09	2023-02-09	WARN	Moderate	Software version is unsupported
45.56.99.139	2023-01-31	2023-02-04	NEUTRAL	Minor	Software version is incomplete
45.56.99.139	2023-01-31	2023-02-03	NEUTRAL	Minor	OS-specific software version is unknown
45.56.99.139	2023-01-26	2023-01-26	NEUTRAL	Minor	OS-specific software version is unknown
45.56.99.139	2023-01-26	2023-01-26	NEUTRAL	Minor	OS-specific software version is unknown
45.56.99.139	2022-11-03	2023-01-16	NEUTRAL	Minor	Support status is unknown
45.56.99.139	2023-01-16	2023-01-16	NEUTRAL	Minor	Support status is unknown

Showing 10 out of 13 findings.
This risk vector has 13 total findings, in order to view them all please login to BitSight.

N/A Desktop Software

Desktop Software

Desktop software are laptops, servers, and other non-tablet, non-phone computers in a company's network which access the internet. Outgoing communications from desktop software include metadata about the device's operating system and browser version; we compare the devices' version of OS and browser with currently released versions and software updates available for those systems, and determine whether those systems are supported or out of date.

Remediation Suggestions

- Search for Diligence records and then identify and update unsupported mobile software.
- Set up auto-update methods for critical desktop software.
- Insufficient information prevents BitSight from identifying unsupported software. The use of software device management systems is recommended, along with integrating human processes that ensures systems in the organization are patched and the software is up-to-date.

No findings available

N/A Mobile Software

Mobile Software

Mobile Software measures mobile devices, such as smartphones and tablets, that are accessing the Internet from an organization's network. Outgoing communications from mobile devices include metadata about the device's operating system, browser version, and applications. The version information is compared with the latest and currently available versions in order to determine if the mobile device is running supported or out-of-date software.

No findings available

Remediation Suggestions

- Search for Diligence records and then identify and update unsupported mobile software.
- Set up auto-update methods for critical mobile software.
- Insufficient information prevents BitSight from identifying unsupported software. The use of mobile device management (MDM) systems is recommended, along with integrating human processes that ensures systems in the organization are patched and the software is up-to-date.

A DNSSEC * Top 10%

DNSSEC *

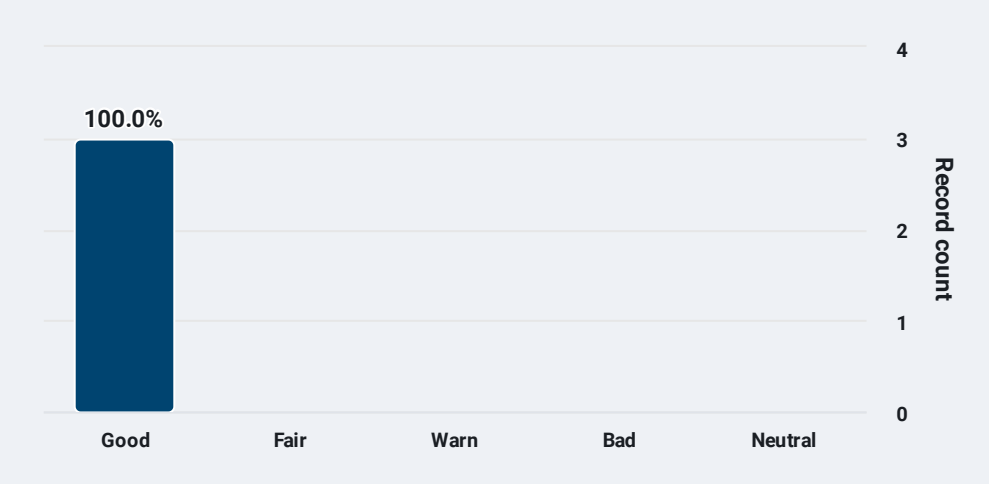
DNSSEC is a protocol that uses public key encryption to authenticate DNS servers. BitSight verifies whether a company is using DNSSEC and if it is configured effectively.

Remediation Suggestions

- Set up DNSSEC for your domain, including generating the appropriate keys and updating DNS zone records.
- Generate a new Zone Signing Key using the RSA or DSA algorithm, with a key of 2048 bits or more.
- Download updated trust anchors and set them to be managed automatically.
- Add your DNSKEY to your DNS records through your registrar's management interface.

* Risk Vector does not currently affect Security Ratings

Grade Distribution: **3** records



Identifier	First Seen	Last Seen	Grade	Severity	Details
sassieshop.com	2023-02-16	2023-02-18	GOOD	Minor	
sassiedev2.com	2023-02-16	2023-02-16	GOOD	Minor	
sassieshop2.com	2023-02-15	2023-02-15	GOOD	Minor	

Showing 3 out of 3 findings.

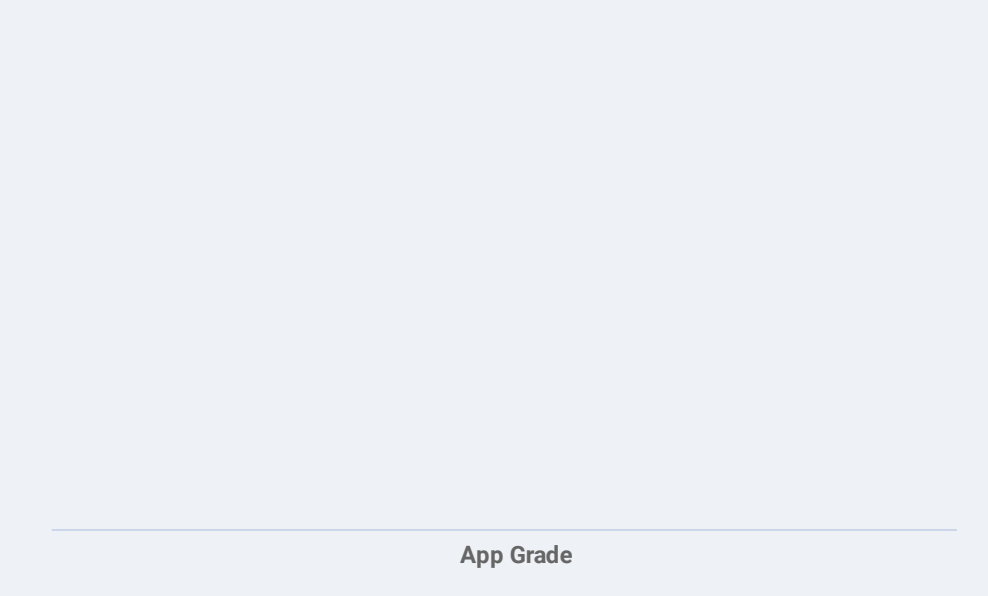
N/A Mobile Application Security *

Mobile Application Security *

This risk vector analyzes the security aspect of publicly available applications in official mobile marketplaces such as Apple App Store and Google Play.

* Risk Vector does not currently affect Security Ratings

Total Mobile Applications: 0



Remediation Suggestions

- Identify mobile applications that are not adhering to application security best practices.
- Verify questionnaire data from vendors. For example, to verify claims that their organization is free of a particular operating system.
- Understand which, if any, applications at an insured present a risk for known vulnerabilities and other threats.
- Verify quality and other contractual agreements with clients or vendors; for example, verify that a client created secure software from a security standpoint and adhered to a policy of keeping end-user operating systems up-to-date.
- If your company is developing and supporting apps for third party customers, please ensure your support emails and support URLs reflect the appropriate ownership information.

N/A Domain Squatting **

Domain Squatting **

Domain squatting reports on the presence of registered domains named similarly to those owned by an organization. Attackers set up malicious software served by similar domain names to take advantage of organization visitors' mistyped URLs, and can trick users to opening malicious email attachment if recipients do not carefully check messages' domain names of origin.

Remediation Suggestions

- Assess potential weaknesses in domain coverage. Work to register any potentially at-risk domains and to trademark your brand assets. Increase domain squatting coverage by requesting the addition of a secondary domain that legitimately belongs in your domain map.
- Implement a policy for domain squatting threats, including process for issuing takedown requests, taking legal action based on trademark infringement, and implementing firewalls/blocking mechanisms to protect against squatted domains.
- Verify completed questionnaires from critical vendors.
- Be wary of suspicious domains that are similar to official domains for a vendor, but not registered to their company.
- Understand if end users at an insured company are at risk for data loss, email phishing attacks, and other threats.

** Informational risk vector (will never affect Security Ratings)

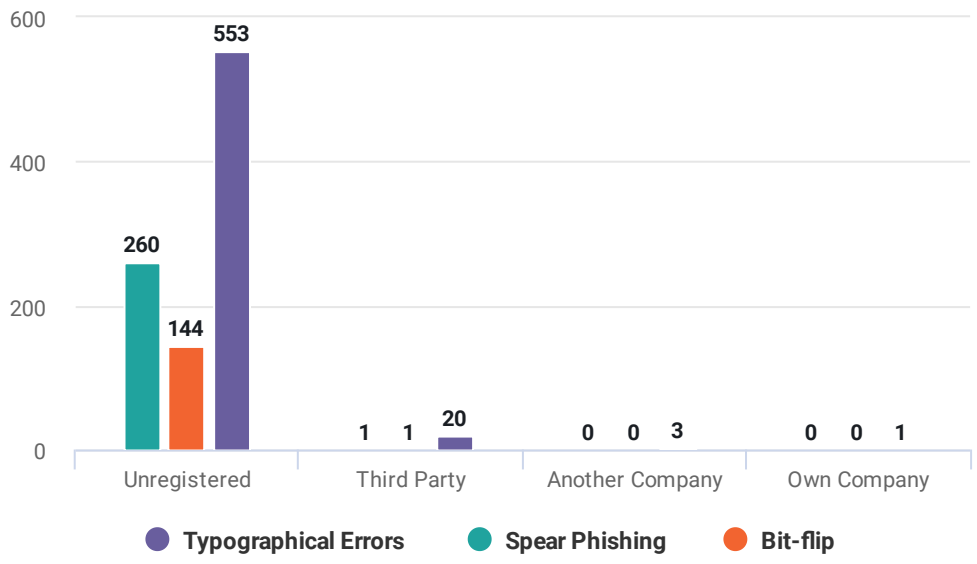
Overview

983 RESULTS

TYPOGRAPHICAL ERRORS
58.7% 577 results

SPEAR PHISHING
26.6% 261 results

BIT-FLIP
14.8% 145 results



Results Matrix for All Domains

	Unregistered	Third Party	Another Company	Own Company
Spear Phishing	**260**	**1**	**0**	**0**
Addition	77	1	0	0
Homoglyph	149	0	0	0
Hyphenation	28	0	0	0
TLD Variant	6	0	0	0
Bit-flip	**144**	**1**	**0**	**0**
Bitsquatting	144	1	0	0
Typographical Errors	**553**	**20**	**3**	**1**
Insertion	287	1	0	0
Omission	24	3	0	1
Repetition	7	0	0	0
Replacement	165	1	0	0
Subdomain	11	14	3	0
Transposition	25	0	0	0
Vowel-swap	22	1	0	0
Various	12	0	0	0
Total	957	22	3	1

User Behavior

User Behavior looks at user file sharing activity that may introduce malicious software into a company, for example, by downloading a compromised file.

User behavior records older than 60 days will not affect a company's grade.

A File Sharing

Top 10%

File Sharing

File sharing is the exchange of media and software, passed through a centralized server (File Transfer Protocol, email, instant messaging), distributed cloud storage services, or direct peer-to-peer channels such as BitTorrent, Gnutella.

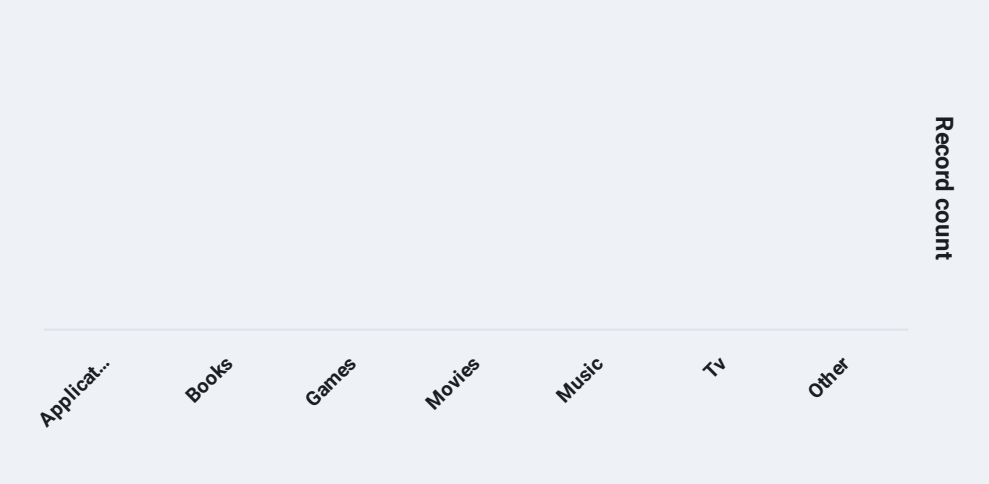
BitSight only tracks file sharing over the BitTorrent protocol, when seen on company infrastructure, and records the sharing of such files as books, music, movies, TV shows, and applications.

Remediation Suggestions

- File Sharing events coming from your company's infrastructure can be found in the My Company ➔ User Behavior tab. The User Behavior Forensics add-on package provides specific details about File Sharing events.
- Use a firewall with Deep Packet Inspection to block torrent activity, as BitTorrent is difficult to block using standard port range rules.

File Sharing over 60 days: 0 events

0 unique IPs observed



IP Address	First Seen	Last Seen	Duration	Severity	File Sharing Category

There are no findings currently affecting this risk vector.

N/A Exposed Credentials **

Exposed Credentials **

The Exposed Credentials risk vector indicates if employees of a company had their information disclosed as a result of a publicly disclosed data breach. Exposed Credentials is an informational risk vector and does not affect a company's Security Rating. Many websites do not validate email addresses, which makes it difficult to assert that certain exposed records are associated with a company's employees. Likewise, BitSight does not test that exposed credentials are valid, for example by trying a username and password exposed from a breached site, in order to preserve business confidence and trust.

Remediation Suggestions

- Use Exposed Credentials as an opportunity to create or re-evaluate policies on information reuse, especially requirements concerning password reuse, password complexity, to address the potential risks associated with Exposed Credentials.
- Consider using 2-factor authentication as part of your organization’s user account security strategy.

** Informational risk vector (will never affect Security Ratings)

Observed Events

Observation Date	Exposure Date	Breached Site	Domains	Records
02/26/2020	02/25/2019	Verifications.io	sassieshop.com	9

Public Disclosures

Public Disclosure events provide information on breaches, general security incidents, and other disclosures related to possible incidents of undesirable access to a company's data.

Only certain events in this category affect a company's rating and only if they occur, as opposed to having a percentage of the rating dedicated to them.

A Security Incidents

Top 10%

Security Incidents

Breaches are publicly disclosed events of unauthorized access, often involving data loss or theft. These events are graded based on several factors, including the number of lost or exposed data records.

Note: Breaches have a negative impact on Security Ratings only if they occur and have a 120-day half-life. For instance, the remaining impact of a breach will be fewer than 20 points after 18 months for severe breaches and under 10 points for moderate breaches.

Public Discovery	Effective Date	Severity	Category

There are no events currently affecting this risk vector

General Security Incidents

General Security Incidents are a diverse range of events related to the undesirable access of a company's data and are considered more severe than Other Disclosures. Some categories of General Security Incidents are Ratings-impacting, while others are informational only and do not impact the rating. These events are graded based on several factors, including the number of lost or exposed data records.

Note: Ratings-impacting General Security Incidents have a negative impact on Security Ratings only if they occur and have a 120-day half-life. For instance, the remaining impact of a General Security Incident will be fewer than 20 points after 18 months for the most severe incidents and under 10 points for moderate ones.

Public Discovery	Effective Date	Severity	Category	Origin

There are no events currently affecting this risk vector

N/A Other Disclosures *

Other Disclosures *

Other Disclosures are considered the least severe group of events within Public Disclosures. This category is used for incidents we learn about via public information, and through other means, that are judged to be minimal in their reflection on security posture. All categories of Other Disclosures are informational only and do not impact the rating.

* Risk Vector does not currently affect Security Ratings

Public Discovery	Effective Date	Severity	Category	Origin

There are no events currently affecting this risk vector

FAQ

What is a BitSight Company Overview Report?

This report was created for Sassie, by BitSight Technologies. It is a snapshot of the company's BitSight Security Rating performance during the past year, as of February 20, 2023. It includes:

- A historical overview of the company's BitSight Security Rating and their overall security performance.
- A summary analysis of the company's observed events by risk vector.

Learn more about this report here:
https://www.bitsight.com/security-ratings

Why am I receiving this report?

A BitSight Company Overview Report is typically shared by BitSight customers with companies in their networks (their third parties). The report is typically sent for various reasons, such as informing their third parties of risks affecting their internet security posture that may need remediation, as a part of the evaluation process for cyber insurance applicants, or to meet regulatory requirements.

If this report is sent by another party, BitSight encourages discussing this report with that party. Access to the BitSight platform can also be granted to the third parties of BitSight customers, where they may view additional details.

Who is BitSight?

BitSight is a company that provides daily security ratings through an automated service via the BitSight Security Ratings Platform.

The BitSight platform continuously analyzes terabytes of external data on the security behaviors of a company in order to help organizations manage third party risk, first party risk, benchmark performance, and assess and negotiate cyber insurance premiums. It's used by the world's largest investment banks, retailers, private equity companies, and insurers to evaluate the security risk of their own organization and their third parties with objective, evidence-based security ratings.

Based in Boston, MA, BitSight is backed by Moody's Corporation, Warburg Pincus, Globespan Capital Partners, Menlo Ventures, GGV Capital, Comcast Ventures, Flybridge Capital Partners, and the National Science Foundation.

For more information about BitSight, visit https://www.bitsight.com or follow @BitSight on Twitter.

Please email BitSight Support at support@bitsight.com regarding additional questions or for more information about this report.

What is a BitSight Security Rating?

A BitSight Security Rating describes a company's cybersecurity posture, serves as a measure of their risk, and transforms how companies manage security risk by using a data-driven, outside-in approach to rate a company's security effectiveness.

A company's rating is presented as a number between 250 and 900. It's an aggregation of the letter grades of all risk vectors (with different weights), that are then normalized for that company. It's based on a 10-point rating system, and then rounded down in 10 point increments. Therefore, if the current rating is 740, this is a representation of the combined assessments of all risk vectors. The rating may be somewhere between 740 and 749 in actuality.

Learn more about the BitSight Security Rating here:
https://www.bitsight.com/security-ratings

How can I discuss information in this report?

This report summarizes the security performance of the company, depicted across the risk categories and the risk vectors within them.

- The Compromised Systems risk category indicates the presence of malware or unwanted software, which is evidence of insufficient security controls.
- The Diligence risk category assesses the steps a company has taken to prevent attacks, their best practice implementation, and risk mitigation (e.g., server configurations) to determine if the security practices of an organization are on par with best practices.
- The User Behavior risk category assesses employee activity, such as file sharing and password re-use. These types of activities can introduce malware to an organization or result in a data breach.
- The Public Disclosures risk category provides information related to possible incidents of undesirable access to a company's data, including breaches, general security incidents, and other disclosures.

Disclaimer

This report and all the data contained herein (the "Information") is the proprietary information of BitSight. Information is provided on an "as is" basis, for an organization's internal use and informational purposes only, and does not constitute investment or financial advice, recommendations to purchase, sell, or hold particular securities. BitSight hereby disclaims any and all warranties whatsoever, including, but not limited to, any warranties of merchantability or fitness for a particular purpose with respect to the Information. BitSight shall not be responsible for any reliance or decisions made based upon Information, and to the extent permitted by law, shall not be liable for any direct, indirect, incidental, consequential, special, or punitive damages associated therewith. Except as otherwise permitted in an applicable underlying agreement, this report may not be reproduced in whole or in part by any means of reproduction.