Security report for hbpct.co.nz

This report provides a detailed overview of key factors of hbpct.co.nz's overall security posture.

Generated date	Report for	Issued by
Feb 19, 2025	hbpct.co.nz	IAG Assurance (NZ)

Introduction

UpGuard continuously monitors the security posture of hbpct.co.nz using open-source, commercial, and proprietary threat intelligence feeds. Our analysis is centered on objective, externally verifiable information.

This report provides rich context for each identified risk, enabling you to make better decisions faster. We do this by intelligently grouping risks into one of five categories: website security, brand & reputation risk, network security, email security, and phishing & malware. Each identified risk is given a severity, name, risk type, and the number of domains impacted. By default, findings are sorted by severity, with the highest critical severity items at the top.

The results outlined below are based on our assessment on Feb 19, 2025 and are intended to provide an overview of hbpct.co.nz's externally visible attack surface. The results are summarized into a security rating which provides a quantitative measure of hbpct.co.nz's security posture.

In addition to this PDF report, you can find an always up to-date assessment of hbpct.co.nz on the UpGuard platform where additional information, our knowledge base, and other tools are available. To obtain online access to your UpGuard account, please contact your account administrator or reach out to us at support@upguard.com.

How are UpGuard's security ratings calculated?

UpGuard uses advanced algorithms to determine the security posture of millions of organizations every day. As noted above, we use threat signals gathered from trusted commercial, open-source, and proprietary sources. We also support the use of targeted security questionnaires to more deeply assess the posture of an organization. These signals are grouped together to identify threats and issues in an attack surface that could result in a security incident. Signals we pay attention to include things like open ports, DNS configuration, known data breaches, and hundreds of other vectors including:

- Susceptibility to man-in-the-middle attacks
- Insecure SSL/TLS certificates
- SPF, DKIM and DMARC settings
- HTTP Strict Transport Security (HSTS)
- Email spoofing and phishing risk
- Vulnerabilities
- Malware susceptibility
- Open admin, database, and file sharing ports
- Exposure to known data breaches and data leaks
- Secure cookie configuration

Our ability to combine these signals in real-time is what makes UpGuard so effective: cybersecurity is a domain where small improvements can make a big difference. By following our suggestions you can reduce the risk of sensitive data exposures, leaked credentials, and other security incidents.

When assessing your security performance, we recommend beginning with your overall security rating. As a general rule of thumb, here is how our A-F ratings correspond to your security posture:

Our security ratings range from A to F:

A **801-950**
Organization has a robust security posture and good attack surface management.

B **601-800**
Organization has basic security controls in place but could have large gaps in their security posture.

C **401-600**
Organization has poor security controls and has serious issues that need to be addressed.

D **201-400**
Organization has severe security issues and should not process any sensitive data.

F **0-200**
Organization has not invested in basic security controls and should not be used.

Any risks we find are given a severity rating from low to critical:

!!!! **Critical risks**
Critical risks or vulnerabilities that place the business at immediate risk of data breaches.

!!! **High risks**
Severe risks that should be addressed immediately to protect the business.

!! **Medium risks**
Unnecessary security risks that could lead to more serious vulnerabilities.

! **Low risks**
Areas of improvement to reduce risks and improve the business' security rating.

Company profile

Name	hbpct.co.nz
Primary domain	hbpct.co.nz
Industry	-
Tier	Untiered
Portfolios	Quotes
Labels	In-Use

Assessment summary

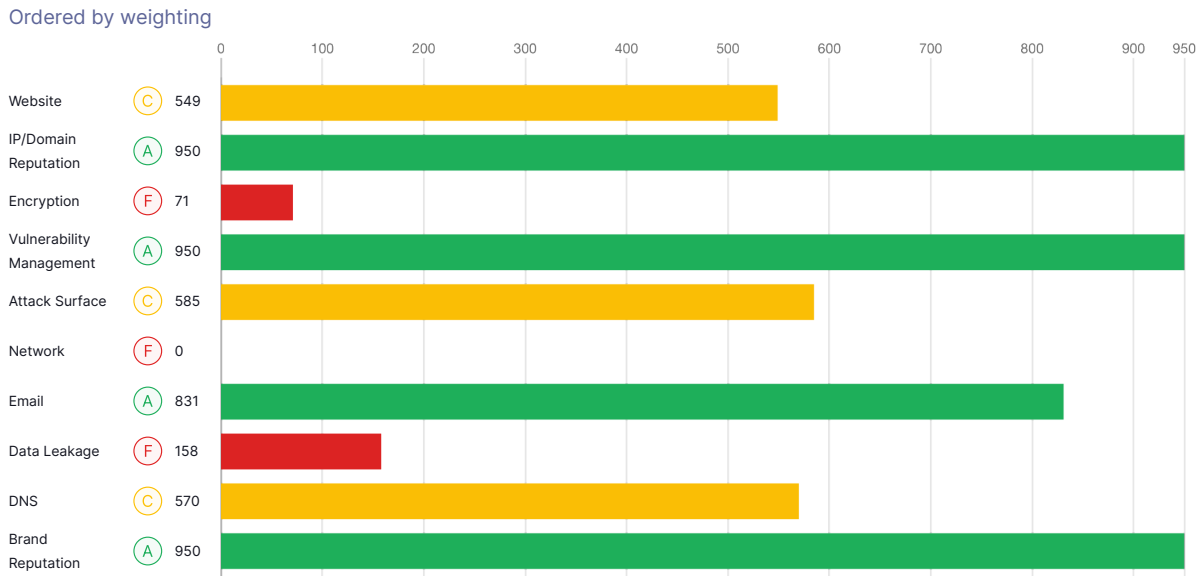
Overall security rating

OVERALL SECURITY RATING

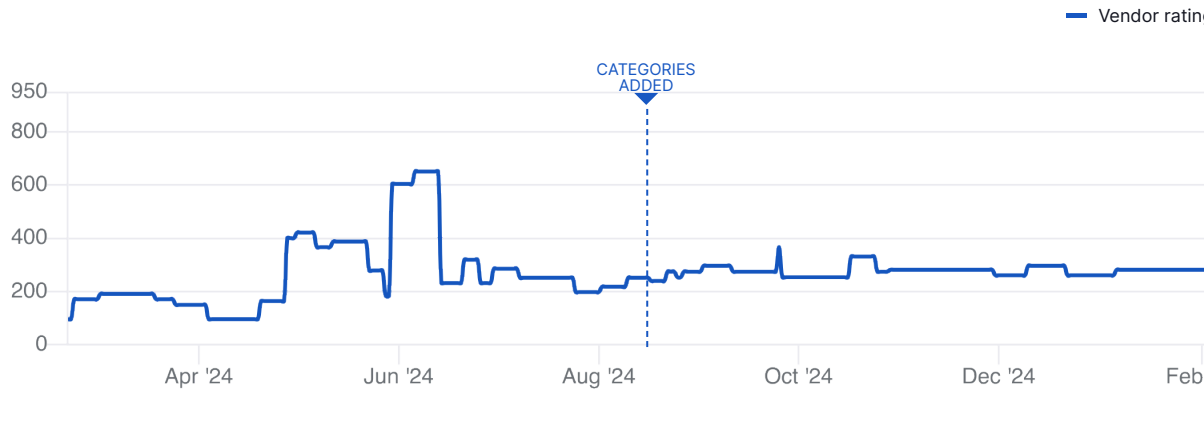
D 281 / 950

hbpct.co.nz has severe security issues and should not process any sensitive data.

Security rating by category



Security rating (last 12 months)



Risk count by severity

Category	Category rating	!!!! Critical	!!! High	!! Medium	! Low
Website	C 549	-	-	3	1
IP/Domain Reputation	A 950	-	-	-	-
Encryption	F 71	1	-	1	-
Vulnerability Management	A 950	-	-	-	-
Attack Surface	C 585	-	-	1	2
Network	F 0	1	-	3	-
Email	A 831	-	-	-	1
Data Leakage	F 158	-	-	1	-
DNS	C 570	-	-	-	1
Brand Reputation	A 950	-	-	-	-

Risk category breakdown

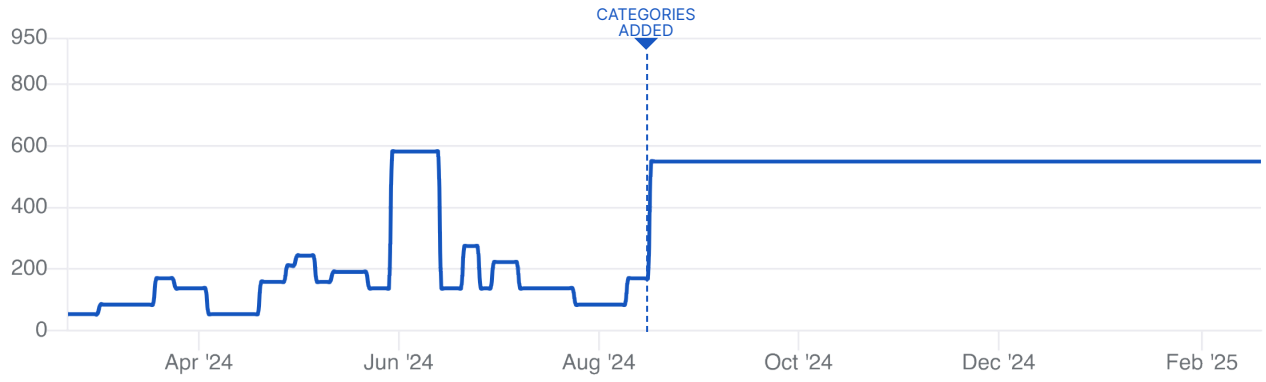
Website

Website security identifies issues with the controls that allow websites to safely be exposed to the untrusted network of the internet. Many of these controls are server security headers that help ensure a site is only serving trusted content.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 3	! 1

CATEGORY RATING C 549 / 950



Website Risk Breakdown

Risk	Affected	Overview	Recommendation
!! Secure cookies not used	1 asset	Cookies are data sent from websites that are stored on your computer. They contain information about your preferences, history and other details. Cookies are used by websites to track users over time, target advertising and personalize the user experience. Some cookies are used in authentication, allowing sessions to be established without re-entering credentials. The Secure cookies attribute restricts the cookie's usability to encrypted channels only, ensuring that cookies are always passed over HTTPS connections.	Applications and web servers that distribute cookies should be configured to include the Secure attribute. The specifics of how to do this differ by technology. For example in ASP.NET, you add <httpCookies requireSSL="true" /> to the web.config file. In Java, you add <secure>`true`</secure> to the cookie-config session of web.xml. Because the Secure attribute requires SSL connections to work, it is important to verify that SSL is properly configured before enabling it.

Asset	Expected	Actual
hbpct.co.nz	`[all set-cookie headers include 'secure']`	`Set-Cookie: whostmgrsession HttpOnly;`

Risk	Affected	Overview	Recommendation
!! X-Frame-Options is not deny or sameorigin	1 asset	X-Frame-Options is a server header that dictates whether a page is allowed to be rendered using the <frame>, <iframe>, <embed> or <object> tags. This measure prevents attackers from rendering a page within a frame they control, where they can then gather inputs to the page like login credentials.	Add a server header for X-Frame-Options with an option of "deny" if there is no need for the site to appear in a frame, or "sameorigin" to restrict this option to other pages on the same domain.

Asset	Expected	Actual
hbpct.co.nz	`[deny or sameorigin]`	`[not set]`

Risk	Affected	Overview	Recommendation
!! CSP is not implemented	1 asset	A Content-Security-Policy header defines directives for server governance on website behaviors through the HTTP header, though you	To create the Content Security Policy for your website, you will need to update the configuration file containing your HTTP Response header.

Website Risk Breakdown (continued)

		can also supply HTML meta tags with a string-matching attribute that sets a CSP for the page. With your CSP, you define the approved origins for content that browsers will load on your website, such as JavaScript, CSS stylesheets, images, and more.	Different server setups and hosting platforms require different approaches to your configuration files. For example, you update the .htaccess or .httpd.conf files for Apache web servers, whereas NGINX servers require modification in the server block.

Asset	Expected	Actual
hbpct.co.nz	`[valid policy]`	`[not set]`

X-Content-Type-Options is not nosniff	1 asset	The X-Content-Type-Options header is not set to "nosniff," an option that prevents MIME type sniffing. This header ensures that the content types defined in the Content-Type header are used and not changed.	In the file that configures your server headers, add the header X-Content-Type-Options: nosniff. You should also ensure that the Content-Type is set correctly for the content you are expecting to server, and test that the site renders as desired after the change.

Asset	Expected	Actual
hbpct.co.nz	`nosniff`	`[not set]`

Risk category breakdown

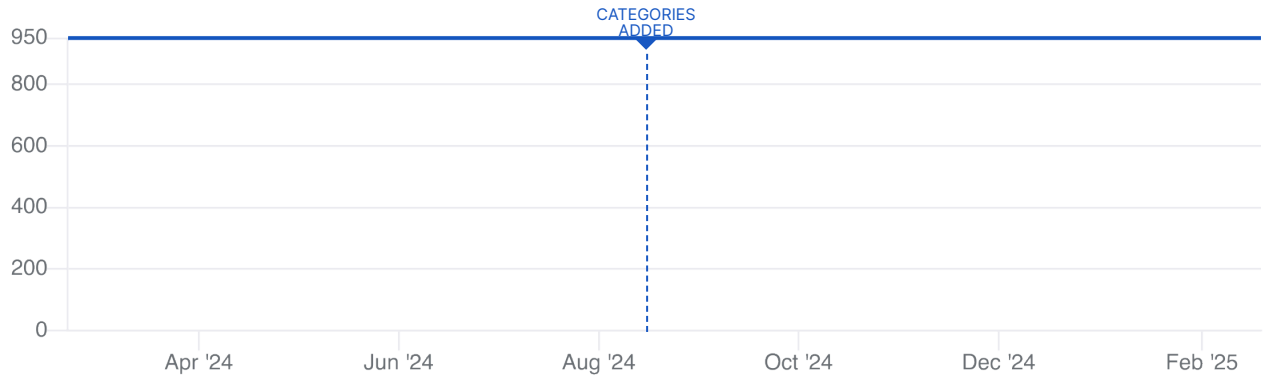
IP/Domain Reputation

IP/Domain reputation indicates reports that a site is suspected of hosting malware, unwanted software, or phishing pages. These risks can indicate that a system has been compromised and may result in the site being blocklisted by other security administrators.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 0

CATEGORY RATING A 950 / 950



IP/Domain Reputation Risk Breakdown

No risks detected in this category.

Risk category breakdown

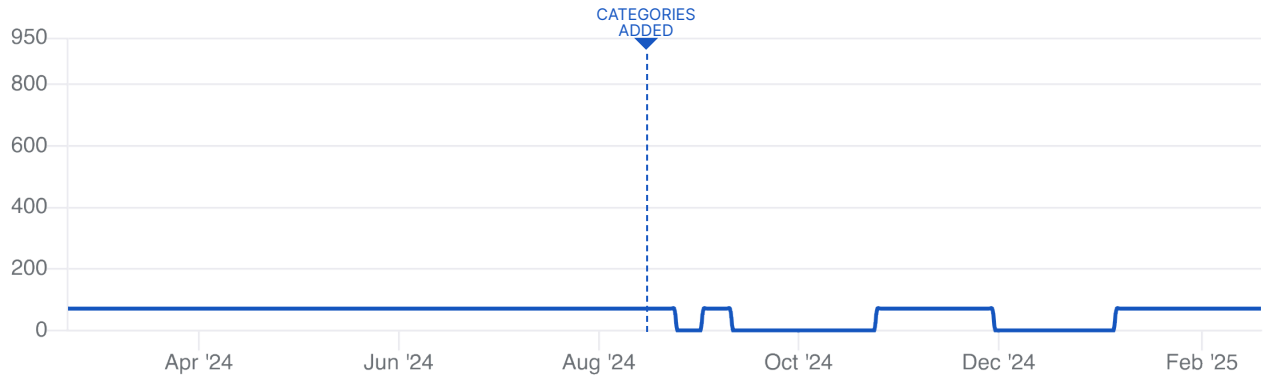
Encryption

Encryption of data in transit is a security measure that prevents adversary-in-the-middle attacks. Data in transit over the internet should always be encrypted, and the encryption methods should be kept up to date to avoid adversarial decryption techniques.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 1	!!! 0	!! 1	! 0

CATEGORY RATING F 71 / 950



Encryption Risk Breakdown

Risk	Affected	Overview	Recommendation
!!!! SSL not available	1 asset	Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. Certificates expire after a set period of time and must be renewed to keep SSL/TLS active. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when necessary.	Valid SSL/TLS certificates with strong encryption algorithms should be obtained from a trusted authority and properly installed and configured on all internet facing systems. Every system must have its name on the certificate to prevent mismatch errors in the browser. HTTPS should be made mandatory, with the necessary redirects and enforcement in place to ensure no plain text connections are possible. Processes should be established to ensure certificates are renewed before they expire.

Asset	Expected	Actual
hbpct.co.nz	`true`	`false`

Risk	Affected	Overview	Recommendation
!! HTTP Strict Transport Security (HSTS) not enforced	1 asset	Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when necessary. HTTP Strict Transport Security (HSTS) ensures that no HTTP connections will be allowed from the server. This forces the use of HTTPS, which maintains encryption at all times.	Enable HSTS on the server. This is done by including the Strict-Transport-Security header on the system. The “includeSubDomains” directive should be specified to ensure all subdomains on the system use HTTPS. Submit your domain to Google’s HSTS preload service. This preload list is included in most browsers and will automatically make all connections to the domain use an encrypted channel.

Encryption Risk Breakdown (continued)

Asset	Expected	Actual
hbpct.co.nz	[header set]	[not set]

Weak cipher suites supported in TLS 1.2 — 1 asset

Transport Layer Security (TLS) 1.2 supports several strong cipher suites, but also includes some that are considered obsolete or weak. Weak encryption algorithms in TLS 1.2 include NULL, RC2, RC4, DES, IDEA, and TDES/3DES, and cipher suites using these algorithms should not be used.

TLS 1.3 no longer includes the weak cipher suites available in 1.2. Upgrading to 1.3 will resolve the issue. Within 1.2, compare the list of cipher suites in use to the list at ciphersuite.info/cs to identify which are insecure.

Asset	Expected	Actual
hbpct.co.nz	[secure ciphers only]	TLSv1.2: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

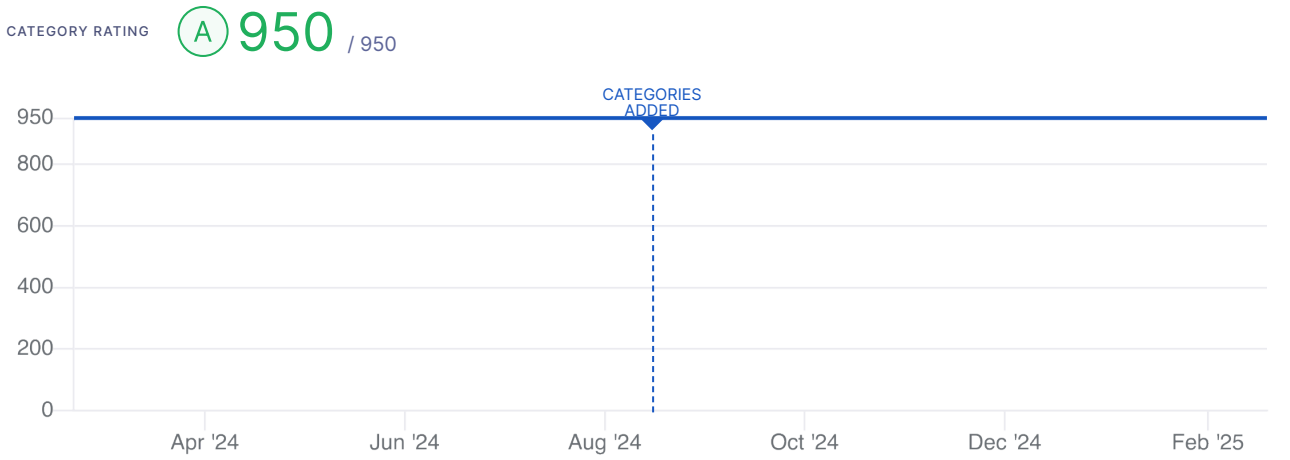
Risk category breakdown

Vulnerability Management

Vulnerability management requires identifying software vulnerabilities and upgrading to secure versions on a timeline appropriate to the severity of the vulnerability. Software with actively exploited vulnerability should be updated as quickly as possible. End of life software no longer receives security updates, and should be decommissioned or updated to an actively maintained version.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 0



Vulnerability Management Risk Breakdown

No risks detected in this category.

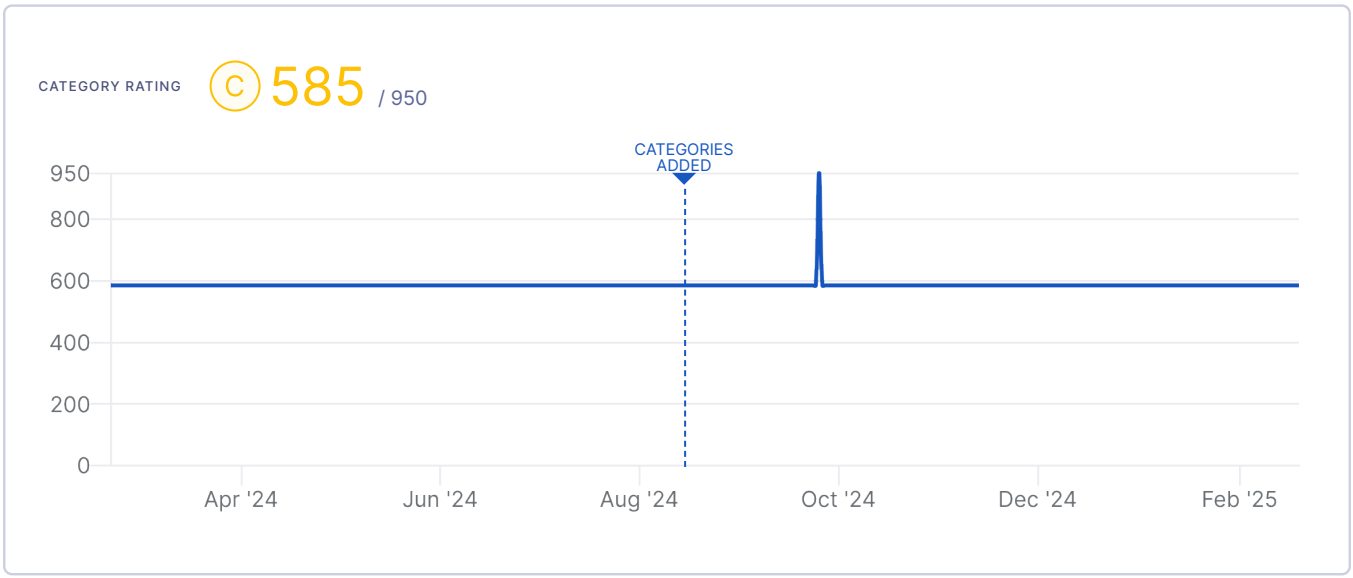
Risk category breakdown

Attack Surface

Attack surface risks present attackers with additional points on an organization's externally accessible boundaries for them to target. Attack surface reduction is the practice of increasing security by removing possible targets, either by decommissioning assets or moving them behind a network layer protection like a VPN.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 1	! 2



Attack Surface Risk Breakdown

Risk	Affected	Overview	Recommendation
!! Outdated WordPress installation detected	1 asset	Impacted web servers are running an outdated version of WordPress. Older versions have less features, more bugs, and worse performance and security.	WordPress needs to be updated to the latest stable version to avoid vulnerabilities present in previous versions. This also minimizes the risk of attackers inserting malicious code through plugins and other avenues.

Asset	Expected	Actual
hbpct.co.nz	`[latest stable version]`	`6.5.5`

Risk	Affected	Overview	Recommendation
! WordPress XML-RPC API enabled	1 asset	We've detected some websites have XML-RPC enabled. XML-RPC is a feature of WordPress that enables data to be transmitted, with HTTP acting as the transport mechanism and XML as the encoding mechanism. However, XML-RPC provides an additional surface for DDoS and brute force attacks.	Disable XML-RPC to reduce the risk of DDoS and brute force attacks by editing the .htaccess file.

Asset	Expected	Actual
hbpct.co.nz	`false`	`true`

Risk	Affected	Overview	Recommendation
! WordPress version exposed	1 asset	Impacted websites are exposing their WordPress version which makes it easier for attackers to find known vulnerabilities and exploits.	WordPress needs to be configured to stop exposing its version in the website's source code. This can be achieved by adding a function to remove the version in the WordPress theme's functions.php file or by various WordPress plugins.

Asset	Expected	Actual
hbpct.co.nz	`[not exposed]`	`6.5.5`

Risk category breakdown

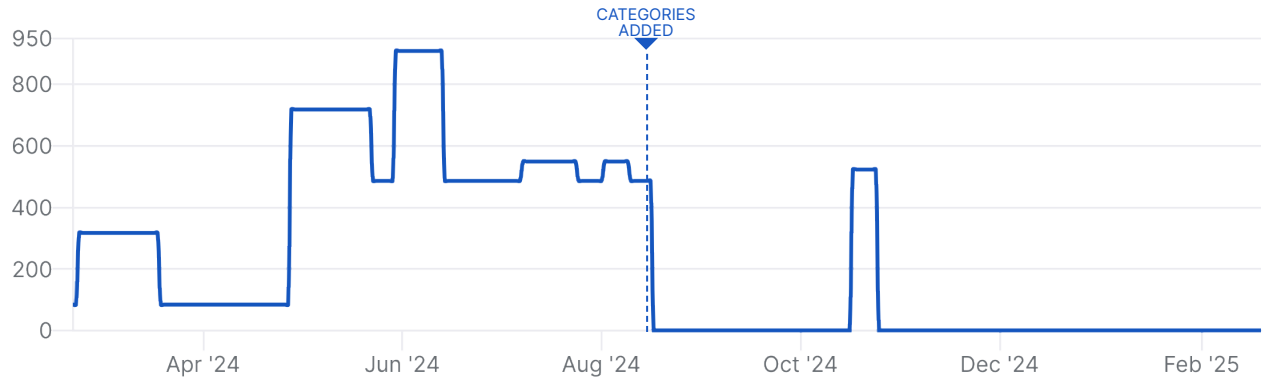
Network

Network layer security means restricting access to the services running on an IP address to only those expected to be internet-facing. Services identified as network risks are those intended to run inside a trusted network or where direct access allows attackers excessive opportunity for abuse.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 1	!!! 0	!! 3	! 0

CATEGORY RATING F 0 / 950



Network Risk Breakdown

Risk	Affected	Overview	Recommendation
!!!! 'FTP' port open	1 asset	File Transfer Protocol (FTP) is a common method for reliably sharing files between networked systems. By default FTP uses port 21. Data transferred in FTP is done so in plain text, including credentials. FTP can require user credentials, or use an anonymous mode that allows all connections. The FTP root is configured on the server to a specific directory, granting remote access to its contents, including subdirectories.	File transfers should be done on an intranet, VPN or other solution that prevents internet-wide exposure. FTP should be replaced with an encrypted solution such as SFTP or FTPS. This will protect data in transit from third party interception. If FTP must be open to the internet, it should be rigorously updated and maintained to ensure it is not vulnerable to any known exploits.

Asset	Expected	Actual
hbpct.co.nz	`[closed]`	`'FTP': [listening on port 21]`

Risk	Affected	Overview	Recommendation
!! 'IMAP' port open	1 asset	Internet Message Access Protocol (IMAP) is an email protocol used to retrieve email from a server. IMAP usually retains the messages on the server, allowing email to be checked from multiple devices, unlike Post Office Protocol (POP3) which downloads messages locally to one client. IMAP communicates in plain text and its default port is 143. IMAP is widely supported by both corporate and consumer email services.	IMAP should be replaced with a more secure protocol, such as IMAPS, which runs IMAP over SSL on port 993. Running IMAP in any capacity is insecure as it transmits passwords and data in plain text. Internet-facing email servers should be kept to a minimum to reduce the email attack surface. The types of protocols that are allowed should also be restricted to what is necessary. Many organizations only allow webmail over HTTPS for external email access.

Asset	Expected	Actual
hbpct.co.nz	`[closed]`	`'IMAP': [listening on ports 143, 993]`

Risk	Affected	Overview	Recommendation
!! 'POP3' port open	1 asset	Post Office Protocol, Version 3 (POP3) is an email protocol used to retrieve email from a server. By	POP3 should be replaced with a more secure protocol, such as POP3S, which runs POP3 over SSL

Network Risk Breakdown (continued)

		default POP3 downloads messages from the server onto the local client and deletes them from the server. POP3 can be configured to leave copies of the email on the server, the way IMAP does by default. POP3 communicates in plain text and its default port is 110. POP3 is widely supported by both corporate and consumer email services.	on port 995. Running POP3 in any capacity is insecure as it transmits passwords and data in plain text. Internet-facing email servers should be kept to a minimum to reduce the email attack surface. The types of protocols that are allowed should also be restricted to what is necessary. Many organizations only allow webmail over HTTPS for external email access.

Asset	Expected	Actual
hbpct.co.nz	[closed]	'POP3': [listening on ports 110, 995]

'SMTP' port open	1 asset	Simple Mail Transfer Protocol (SMTP) is an internet standard protocol used to send and receive email. Email servers use SMTP when talking to each other, and clients use SMTP to send email through their mail server. SMTP typically communicates over port 25.	Only a minimal number of hardened SMTP edge servers should exist. All other email servers should be restricted to internal networks and VPNs. SMTP is a particularly important service to properly configure, as failure to do so can blacklist your domain. SMTP should be configured to use authentication so that only specific users can send email. SMTP should use an encryption option, such as STARTTLS to attempt to make an encrypted connection.

Asset	Expected	Actual
hbpct.co.nz	[closed]	'SMTP': [listening on ports 465, 587]

'HTTP' port open	1 asset	HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet, specifically for delivering web pages and other web-based content. A HTTP port is a network communication port that allows Hypertext Transfer Protocol (HTTP) traffic to be transmitted between a client and a server. The most commonly used HTTP port is 80.	All web traffic should be conducted over an HTTPS connection, typically using port 443. By proactively redirecting or blocking the unencrypted HTTP port, the risk of data interception is greatly reduced.

Asset	Expected	Actual
hbpct.co.nz	[closed]	'HTTP': [listening on port 2086]

'HTTPS' port open	1 asset	HTTPS (HyperText Transfer Protocol Secure) is a secure protocol that is used to communicate over the internet. This protocol uses encryption to secure the data being transmitted between the server and client, preventing eavesdropping and tampering of the data. The most common port numbers used for HTTPS are 443, 80, and 8443.	Verify that the only servers with internet facing HTTPS ports are those intended to serve public webpages. Internal websites, web management tools and other sensitive web sites should be accessible to remote users via a VPN connection.

Asset	Expected	Actual
hbpct.co.nz	[closed]	'HTTPS': [listening on ports 2083, 2087]

Risk category breakdown

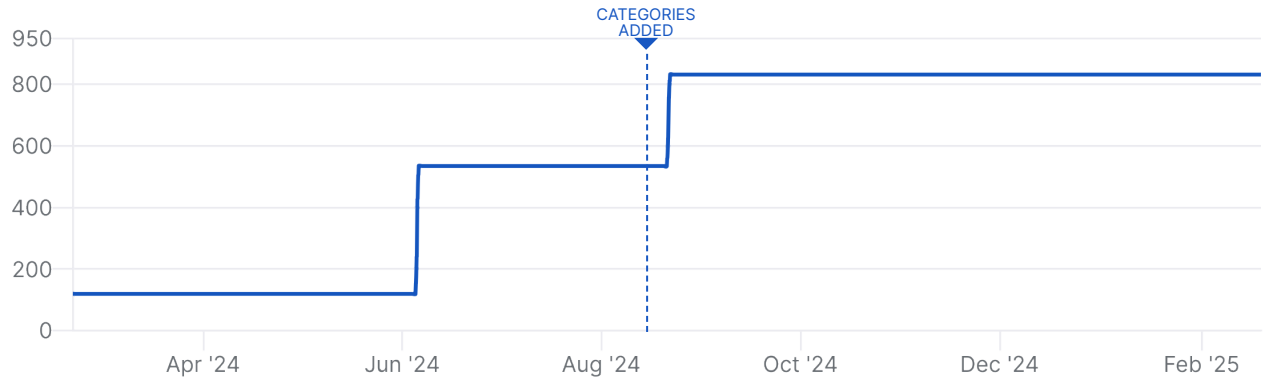
Email

Email security measures prevent malicious actors from impersonating the sender of an email message. These controls help prevent phishing campaigns against an organization, its vendors, and its customers. Email is a commonly abused method for attempting to gain access to a user's account, and effective email security can reduce this risk.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 1

CATEGORY RATING A 831 / 950



Email Risk Breakdown

Risk	Affected	Overview	Recommendation
! DMARC policy is p=quarantine	1 asset	Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email security feature that works in conjunction with Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) to ensure that messages actually originate from the organizations claimed in the From: address. It does this by “aligning” the From: address with either the SPF or DKIM policy in the sender domain. If a message’s From: address does not align with either of these policies, DMARC offers options on how to handle the message, including delivering it, quarantining it and blocking it altogether.	The p= value in DMARC provides instructions on what to do with an email that fails DMARC alignment. The p= value should ultimately be set to reject for best security; however, p=quarantine can be used temporarily to monitor DMARC behavior and ensure false positives are not being quarantined. Once this monitoring is complete, the p= value should be set to reject. This helps prevent fraudulent email from reaching end users.

Asset	Expected	Actual
hbpct.co.nz	`v=DMARC1; p=reject; ...`	`v=DMARC1;p=quarantine;sp=none;adkim=r;aspf=r;pct=100;fo=0;rf=afrf;ri=86400`

Risk category breakdown

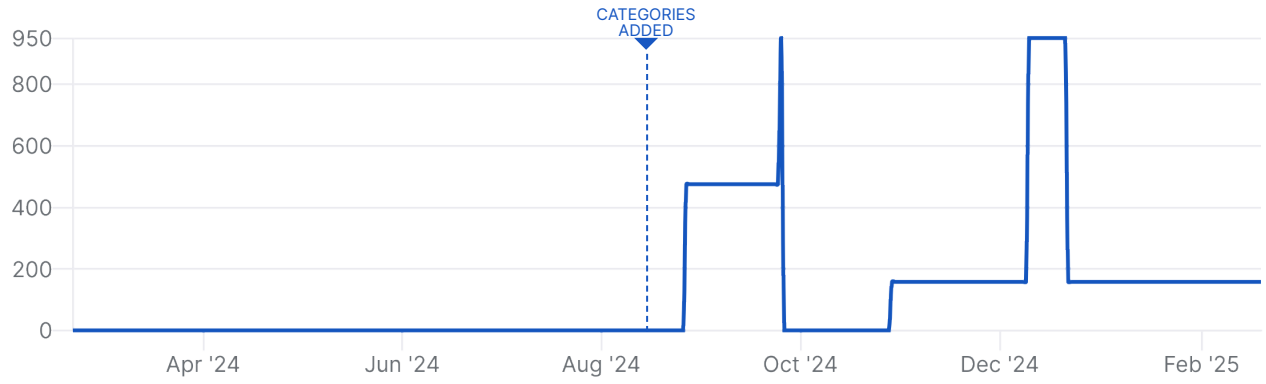
Data Leakage

Data leakage is the unintentional exposure of potentially sensitive information, including credentials, personal information, and business secrets. Data leakage risks can indicate lapses in best practice that could result in sensitive data being exposed in the future, as well as active exposures of sensitive data.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 1	! 0

CATEGORY RATING F 158 / 950



Data Leakage Risk Breakdown

Risk	Affected	Overview	Recommendation
!! Listable directories found	1 asset	This site uses WordPress, an open content management system configured by end users. WordPress uses a predictable directory structure for hosting files, typically assets used on the website. In this WordPress installation, one or more of those directories are directly listable, meaning all files in the directory can be viewed by anonymous users.	End users can configured WordPress directories to have any names, but the most common directories are the default names built into WordPress: wp-includes, wp-admin, and wp-content. More specifically, wp-content/uploads is where users are directed to upload content. As an administrator, you can disable directory listing by finding the .htaccess file in your site's code and adding "Options -Indexes" to the file contents.

Asset	Expected	Actual
hbpct.co.nz	`[none]`	`/wp-content/uploads, /wp-includes`

Risk category breakdown

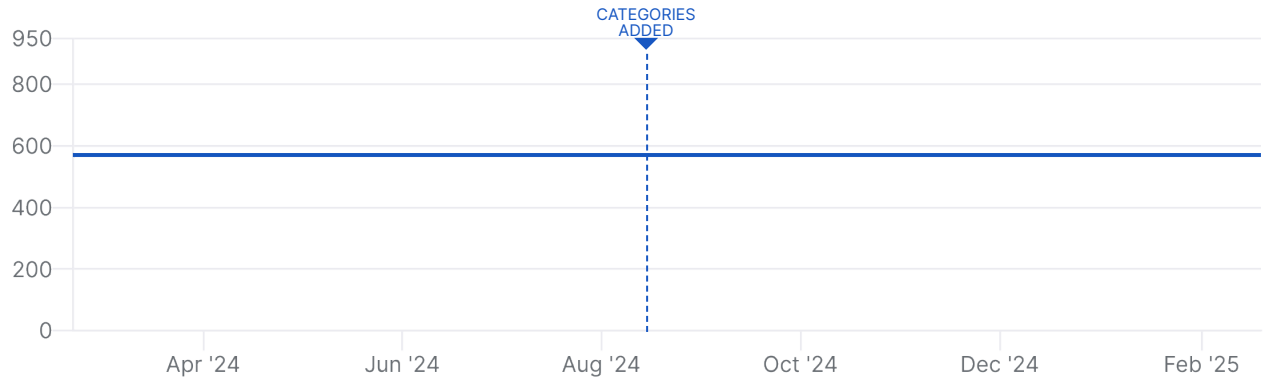
DNS

DNS security entails the management of settings in DNS records to ensure that organizations remain in control of their domains and the content served on their domains. Poor DNS security can allow attackers to gain control of domains and serve malicious content on sites that appear to belong to the victim organization.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 1

CATEGORY RATING C 570 / 950



DNS Risk Breakdown

Risk	Affected	Overview	Recommendation
DNSSEC not enabled	1 asset	Domain Name System (DNS) is the service that translates human-friendly names to IP addresses. When a URL is sent from the browser, it goes to a DNS server that references its database and returns an IP address for the browser to use. Domain Name System Security Extensions (DNSSEC) is an optional feature of DNS that authenticates (but does not encrypt) responses to DNS requests. DNSSEC uses certificates to ensure only authorized DNS translations are returned to a client.	Enable DNSSEC on the domain. This is a three step process that involves creating the necessary DNSSEC records in your domain, activating DNSSEC at your domain registrar and enabling DNSSEC signature validation on all DNS servers. The specifics of each step vary depending on the platforms and vendors in play.

Asset	Expected	Actual
hbpct.co.nz	`true`	`false`

Risk	Affected	Overview	Recommendation
CAA not enabled	1 asset	Certificate Authority Authorization (CAA) is a security mechanism that allows domain owners to specify which Certificate Authorities (CAs) are permitted to issue SSL/TLS certificates for their domain. The CAA policy is enforced through DNS (Domain Name System) records, providing an extra layer of security against unauthorized certificate issuance.	CAA is implemented as a DNS resource record (type CAA). Domain owners add CAA records to their DNS zone file, specifying which CAs are allowed to issue certificates for that domain. To allow Let's Encrypt to issue certificates, the record would look like: example.com. IN CAA 0 issue "letsencrypt.org".

Asset	Expected	Actual
hbpct.co.nz	`[set]`	`[not set]`

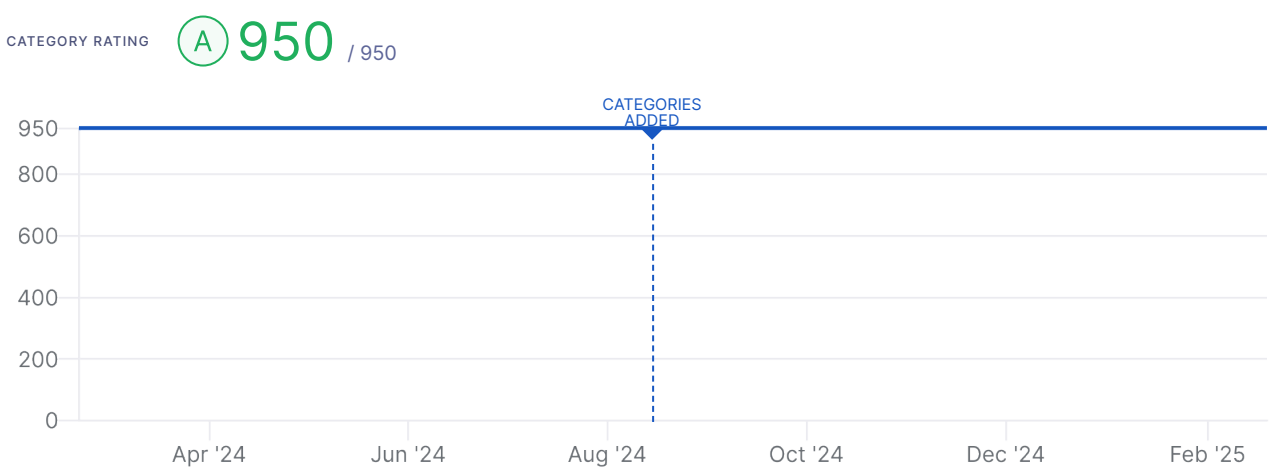
Risk category breakdown

Brand Reputation

Brand reputation highlights factors that indicate a company has suffered adverse media and may have risks associated with them as a business partner.

CURRENT RISKS BY SEVERITY

Critical Risk	High Risk	Medium Risk	Low Risk
!!!! 0	!!! 0	!! 0	! 0



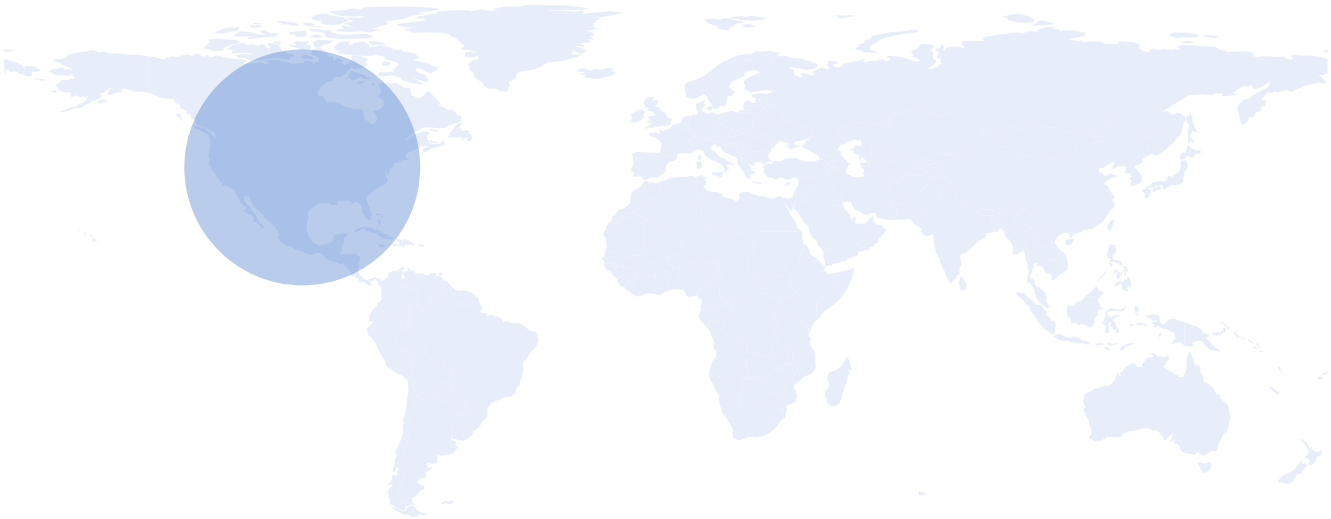
Brand Reputation Risk Breakdown

No risks detected in this category.

Geolocation

This geographical overview lets you discover the locations that an organization's infrastructure is operating in. Monitoring geolocation risk is a great way to understand whether your data is being hosted in different countries that may have different data and privacy laws protecting it.

HOSTING COUNTRIES	IP ADDRESSES
1	1



Country	No. IP addresses	Percentage	Services
United States	1	100%	

Evidence used to generate this report

Automated scanning

This report includes analysis performed on the following domains and IPs as of Feb 19, 2025.

ACTIVE DOMAINS & IPS	INACTIVE DOMAINS & IPS	TOTAL DOMAINS & IPS SCANNED
1	6	7