Datasheet

Blue Hexagon Threat Protection Platform

Blue Hexagon engaged independent data privacy risk management provider TrustArc® to review and document the privacy and data protection practices described in this datasheet. The purpose of this document is to provide customers of Blue Hexagon with information needed to assess the impact of this service on their overall privacy posture by detailing how personal information may be captured, processed and stored by and within the service.

Network Threat Protection Harnessing the Power of Deep Learning

Product Summary

Blue Hexagon has built the industry's first real-time deep learning platform for network threat protection. Built by a team with decades of machine learning and deep learning expertise, the Blue Hexagon proprietary neural network architecture is designed for speed and efficacy. Blue Hexagon detects known and unknown threats in less than a second at nearly 100% efficacy and up to 20G hardware and higher cloud/virtual appliance wire speed performance. The platform works out-of-the-box and requires no baselining. Prevention can be enabled via inline blocking or orchestrated enforcement to endpoints, firewalls and web proxies, to block malicious traffic at the network or application. The platform can detect and stop--in real-time--both known and unknown threats hidden within encrypted SSL traffic, giving security teams new visibility into threats without compromising privacy, confidentiality, or network performance. The Blue Hexagon Threat detection solution can be deployed on premises or in AWS and Azure cloud environments for network defense.

Information Processed by Blue Hexagon Threat Assessment Platform

Blue Hexagon is deployed on a SPAN/TAP port of a firewall and inspects a copy of all the traffic passing through. As part of this inspection the platform generates metadata which is displayed in an administration console hosted in the cloud. Blue Hexagon customers may decline the transmission of any data element, including those which may contain personally identifiable information. For specifics on the types of data and various data elements the platform my process, please see the following table:

Data Type / Description	May Be Anonymized	May Contain PII
Actions taken in response to threat detection (e.g. Send to EDR)	No	No
Appliance identifier e.g. "hq". Each Blue Hexagon appliance in your network is assigned a unique ID	No	No
Unique identifier for a single file instance	No	No
Threat Category (e.g. information stealer, ransomware)	No	No
Comma-separated list of file hashes indicating the files contained in an archive	No	No
Originating endpoint's IP address (client endpoint)	Yes	Yes
Threat Family (to be read in conjunction with Threat Category)	No	No
Name of file, if available	Yes	No
Size of the file in bytes	No	No
File type (e.g. EXE, PDF, MS-DOC)	No	No

Data Type / Description	May Be Anonymized	May Contain PII
SHA256 hash of the file	No	No
HTTP Host header	Yes	Yes
HTTP Request verb: GET, POST, etc.	Yes	No
HTTP Response mime_type (e.g. application/pdf)	Yes	No
Status code returned by the server	Yes	No
URI used in the HTTP request	Yes	No
Value of the User-Agent header	Yes	No
mime_type of file payload (e.g. application/pdf)	No	No
For each threat, score associated with various threat categories	No	No
Originating endpoint's TCP/UDP port (or ICMP code)	No	No
Threat verdict - benign or malicious	No	No
Responding endpoint's TCP/UDP port (or ICMP code)	Yes	No
Time taken by Blue Hexagon appliance to deliver verdict (in milliseconds)	No	No
Severity level of the threat (1-7)	No	No
Contents of the SMTP CC header	Yes (default)	Yes
Contents of the SMTP first Received header	Yes	Yes
Contents of the SMTP FROM header	Yes (default)	Yes
Contents of the SMTP In-Reply-To header	Yes (default)	Yes
Contents of the SMTP MAIL FROM header	Yes (default)	Yes
Message transmission path, from headers	Yes	Yes
Contents of the SMTP ReplyTo header	Yes (default)	Yes
Contents of the SMTP TO header	Yes (default)	Yes
Contents of the SMTP X-Originating-IP header	Yes	Yes
Source protocol of the file data (HTTP/SMTP/FTP_DATA)	No	No
Country corresponding to Source IP	Yes	No
Responding endpoint's IP address (typically HTTP or SMTP server)	Yes	No
Type of threat: payload malware, C&C, etc.	No	No
Threat Kill Chain stage (1-7)	No	No
UTC timestamp (seconds since epoch with microsecond precision)	No	No

Purpose of Information Processed by Blue Hexagon

The primary purpose of processing information through Blue Hexagon is to assess threats by:

- Inspecting malware and zero days.
- Blocking known threats.
- Blocking unknown threats.
- Orchestrating response and remediation controls post-detection.

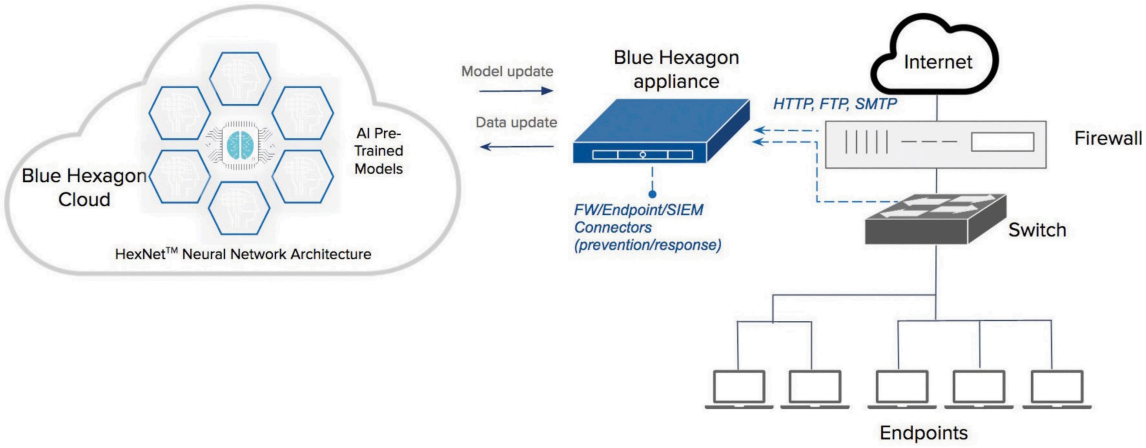
How Blue Hexagon Addresses Data Protection

Processing personal data to ensure network and information security via the Blue Hexagon Threat Assessment Platform is broadly recognized as a legitimate interest and specifically identified in the EU General Data Protection Regulation (GDPR):

> *(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.*
>
> *This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.*[1]

Where a service provider, such as Blue Hexagon, processes personal data to ensure network and information security, this is a *legitimate interest* of the service provider and its customers, providing a legal basis for the processing of personal data by Blue Hexagon under EU data protection laws.

Data Flow



This legitimate interest also provides a basis for customers storing personal data in the cloud or monitoring network traffic for security events, in accordance with privacy or regulatory requirements. In such an event, customers can use their privacy options, described herein, when configuring firewall or administration accounts, to limit data processing or access.

Also, in the event of a need to share logs or information with Blue Hexagon offices in other regions, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission2 or other legal instruments, provided for in EU data protection law.

What Blue Hexagon Does to Comply with Data Protection Rules (The General Data Protection Regulation & The California Consumer Protection Act)

Blue Hexagon is committed to protecting personal data processed by Blue Hexagon Threat Assessment Platform. We will not access the content of the information in a way that would allow the service to acquire meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats or investigating suspicious behavior indicative of attack.

---

[1] *GDPR, recital 49; also see Article 29 Working Party Opinion 06/2014 on the notion of legitimate interest of the data controller, WP217, adopted 9 April 2014, p. 24-25.*

[2] *http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm*

File/header extraction & analysis is fully automated using deep learning, and files determined to be benign are deleted shortly after analysis. Only malicious files are stored for further analysis (this can be disabled per the customer's requirement) as well as development and testing of new security products. We do not share such files with anyone else.

Files stored on or processed by Blue Hexagon systems are secured with state-of-the-art technologies, and Blue Hexagon operates rigorous technical and organizational security controls.

Customers Privacy Options

Customers can choose which elements of session data and what types of files to share with Blue Hexagon for analysis. Customers have the option to restrict all sharing while still receiving malware and threat detection models. However, we strongly encourage customers to share data with the network, because this enables the detection of emerging threats and the distribution of protective measures to all Blue Hexagon customers as soon as possible.

Retention

Customers have complete control over the duration of storage for logs on the platform. Files sent to Blue Hexagon for processing and analysis are retained until processing takes place. Once analyzed, files categorized as benign are retained for 30 days in case the analysis decision is reversed. Files determined to be malicious are retained for 7 years. Signatures and sample reports for corresponding files, which do not include personal information, are stored indefinitely.

Access and Disclosure

Access by the Customer

Customers access information related to the Blue Hexagon service through the platform interface. The customer's system administrator controls access to the interface by granting appropriate privileges to authorized users.

Access by Blue Hexagon

Data is processed by Blue Hexagon in an automated fashion, and access by Blue Hexagon occurs when required to troubleshoot a customer support inquiry or address issues related to the service. All access privileges are managed by Blue Hexagon leadership and are audited for privilege access violations.

Security

Session data sent from firewalls to Blue Hexagon is encrypted in transit. All data in the cloud is encrypted while at rest. Blue Hexagon also has a robust information security program to demonstrate its strong security policies and internal controls environment. Blue Hexagon is SOC 2 compliant. SOC 2 defines criteria for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality and privacy.

About this Datasheet

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. Both the General Data protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) were considered during the discovery process. The creation of this datasheet was supported by a comprehensive Data Protection Impact Assessment as well as a CCPA Assessment. The discovery process relied upon the good faith accuracy of the information provided; TrustArc has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

Blue Hexagon is a deep learning innovator of AI You Can Trust(™) to stop cyber adversaries at sub-second speed, before the infiltration. The company's real-time, deep learning platform delivers world's highest detection efficacy for zero-day and known threats, and real-time orchestration and blocking controls, to protect enterprise network, cloud and email. Blue Hexagon Deep Learning models do not require baselining and eliminate learning delays, sandbox and rules or signatures. Blue Hexagon is headquartered in Sunnyvale, CA, and backed by Benchmark and Altimeter Capital. For more information, visit www.bluehexagon.ai or follow @bluehexagonai.

Headquarters
298 S. Sunnyvale Avenue, Suite 205
Sunnyvale, CA 94086
www.bluehexagon.ai
inquiries@bluehexagon.ai

BH-GDPR-CCPA-051120

BLUEHEXAGON