

Gartner

Here's what the analysts say:

DRPS stretch detection and monitoring activities outside of the enterprise perimeter by searching for threats to enterprise digital resources, such as IP addresses, domains and brand-related assets. DRPS solutions provide visibility into the open (surface) web, dark web and deep web environments by providing contextual information on threat actors and the tactics and processes that they exploit to conduct malicious activities.

By [Dan Ayoub](#) – [Source](#)

Data443's position on IP Reputation capabilities

Data443's GlobalView™ Threat Intelligence and the IP Reputation Engine power our solution to redefine digital risk management. By analyzing billions of internet transactions daily, our IP Reputation Intelligence proactively identifies and mitigates threats, aligning with the advanced standards of DRPS solutions. Our strategy covers the entire spectrum of the web, including the open, dark, and deep web, to provide comprehensive visibility into cyber threats that exist beyond conventional security perimeters.

This initiative reflects our dedication to enhancing digital security measures, protecting against threats to enterprise digital resources such as IP addresses, domains, and brand-related assets. Utilizing the latest technologies and algorithms, we offer real-time insights into malicious URLs, phishing, and malware, coupled with contextual information about threat actors, their strategies, and methodologies.

IP Reputation Engine

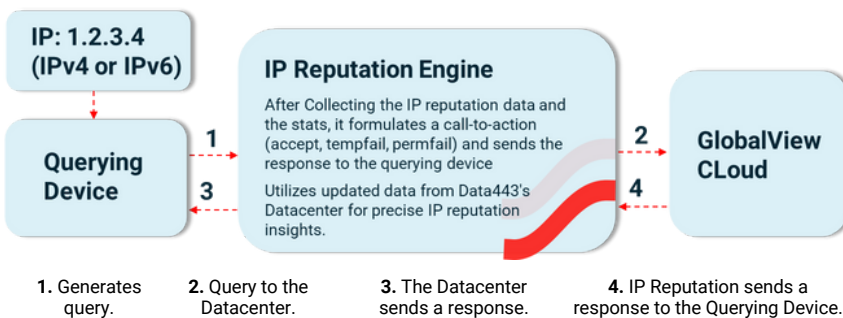
Central component for IP reputation analysis.

Data443's Datacenter

Provides real-time global email traffic analysis and IP reputation data.

Querying Devices

Interfaces with IP Reputation for IP reputation assessments.



Features and Modules

The features of Data443's Cyren Threat InDepth are:

- › **Real-Time Information:** Provides real-time information on ongoing and emerging cyber threats.
- › **Malware File Detection:** Offers robust malware file detection capabilities, analyzing millions of suspicious files to detect new malicious files.
- › **Phishing and Fraud Detection:** Detects phishing and fraudulent activities, analyzing URLs and web content to identify zero-day phishing attacks.
- › **IP Threat Detection:** The platform analyzes billions of web and email transactions in real time to identify high-risk IP addresses associated with spam, phishing, and malware.
- › **Early Detection:** Provides early detection of cyber threats, leveraging unique intelligence powered by the GlobalView network and listing only infected hosts active within the last 24 hours.
- › **Customizable Categories:** Intelligence feeds can be tailored to specific needs with customizable categories to focus on the threats most relevant to the operations.
- › **Integration Flexibility:** The platform offers integration flexibility, allowing seamless integration with partner applications via SDK or text data feed.
- › **Comprehensive Coverage:** Provides comprehensive coverage of cyber threats by analyzing billions of transactions across email content, suspicious files, and web traffic.
- › **Global Data:** Enables organizations to gain insights into current and emerging security threats worldwide, enhancing their cybersecurity posture.
- › **Incident Response:** Accelerates incident response by providing actionable insights to prioritize and respond to threats effectively to make informed decisions and mitigate risks promptly.
- › **Cloud Enabled:** The platform is cloud-enabled, offering scalability and flexibility to meet evolving needs and can be accessed anytime, anywhere, ensuring continuous protection against cyber threats.
- › **Up-to-date Data:** Security measures remain up-to-date and effective against evolving threats.

GAP Analysis

	Data443 Risk Mitigation Inc.	DNSBLs
Support & Pricing		
Free Trial	Yes	Yes
Demo	Yes	Yes
Quotation-based	Yes	Yes
Subscription-based	Yes	Yes
Troubleshooting Assistance	Yes	Yes
Core Features		
Real-Time Information	Yes	Yes
Malware File Detection	Yes	No
Phishing and Fraud Detection	Yes	Yes
IP Threat Detection	Yes	Yes
Early Detection	Yes	No
Predictive Phishing Detection	Yes	No
Customization & Integration		
Customizable Categories	Yes	Yes
Integration Flexibility	Yes	No
Cloud Enabled	Yes	No
Data & Intelligence		
Comprehensive Coverage	Yes	Yes
Global Data	Yes	No
Up-to-date Data	Yes	Yes
Contextual Data	Yes	No
Dynamic Threat Intelligence	Yes	No
Machine Learning	Yes	No
Analysis & Response		
Incident Response	Yes	No
Threat Prioritization	Yes	No
Risk Score	Yes	No

Company Overview

DNSBL.info offers DNS-based blocklist (DNSBL) services to improve email security by mitigating spam threats. It provides real-time blocklist data to help organizations block spam, phishing, and other malicious emails. Designed for businesses, email service providers, and network administrators, it ensures reliable and accurate blocklist data to protect email communication.

Supported Systems

DNSBL.info DNS Blacklists supports some of the systems such as:

- › Web Browsers
- › Email security gateways
- › Spam filters
- › Network applications

GAP Analysis

	Data443 Risk Mitigation Inc.	Zvelo
Support & Pricing		
Free Trial	Yes	No
Demo	Yes	No
Quotation-based	Yes	Yes
Subscription-based	Yes	No
Troubleshooting Assistance	Yes	No
Core Features		
Real-Time Information	Yes	Yes
Malware File Detection	Yes	Yes
Phishing and Fraud Detection	Yes	Yes
IP Threat Detection	Yes	Yes
Early Detection	Yes	Yes
Predictive Phishing Detection	Yes	Yes
Customization & Integration		
Customizable Categories	Yes	No
Integration Flexibility	Yes	Yes
Cloud Enabled	Yes	No
Data & Intelligence		
Comprehensive Coverage	Yes	Yes
Global Data	Yes	Yes
Up-to-date Data	Yes	Yes
Contextual Data	Yes	No
Dynamic Threat Intelligence	Yes	No
Machine Learning	Yes	No
Analysis & Response		
Incident Response	Yes	Yes
Threat Prioritization	Yes	Yes
Risk Score	Yes	No

Company Overview

Zvelo, Inc. offers solutions for website content categorization, contextual categorization, and the detection of malicious activities and botnets. It supports web filtering, brand safety, semantic targeting, traffic quality analysis, contextual targeting, and ad fraud prevention. Zvelo serves network security providers, mobile service providers, and organizations requiring subscriber analytics solutions.

Integrations

The integrations of zveloCTI™ include:

- › CrowdStrike
- › Carbon Black
- › SentinelOne
- › Tanium
- › Splunk
- › IBM QRadar
- › Zscaler
- › Netskope
- › RiskIQ
- › Tenable.io
- › Cobalt
- › AttackIQ
- › Cisco Umbrella
- › OpenDNS
- › Mimecast
- › Barracuda
- › Others

Supported Systems

zveloCTI™ supports some of the systems such as:

- › Browsers
- › Platforms
- › Applications
- › Cloud Services



Main Campus

4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Data443

Website: www.data443.com
Email: info@data443.com

Call

US: +1 919 526 1070
UK: +44 203 7693 700

GAP Analysis

	Data443 Risk Mitigation Inc.	Spamhaus
Support & Pricing		
Free Trial	Yes	Yes
Demo	Yes	No
Quotation-based	Yes	Yes
Subscription-based	Yes	Yes
Troubleshooting Assistance	Yes	No
Core Features		
Real-Time Information	Yes	Yes
Malware File Detection	Yes	No
Phishing and Fraud Detection	Yes	Yes
IP Threat Detection	Yes	Yes
Early Detection	Yes	No
Predictive Phishing Detection	Yes	No
Customization & Integration		
Customizable Categories	Yes	No
Integration Flexibility	Yes	Yes
Cloud Enabled	Yes	Yes
Data & Intelligence		
Comprehensive Coverage	Yes	Yes
Global Data	Yes	Yes
Up-to-date Data	Yes	Yes
Contextual Data	Yes	Yes
Dynamic Threat Intelligence	Yes	Yes
Machine Learning	Yes	No
Analysis & Response		
Incident Response	Yes	Yes
Threat Prioritization	Yes	No
Risk Score	Yes	No

Company Overview

Spamhaus provides IP and domain reputation data, offering real-time threat intelligence that integrates into existing infrastructures. It aids in detecting and preventing spam, malware, ransomware, botnets, and phishing. Spamhaus serves technology companies, internet service providers, and hosting firms globally.

Integrations

The integrations of Spamhaus DQS and

- › Intelligence API include:
- › Microsoft Exchange
- › Comcast
- › AT&T
- › atmail
- › Talos
- › Office 365
- › G Suite
- › Halon
- › MDaemon
- › Cisco Email Security
- › McAfee
- › Others

Supported Systems

Spamhaus DQS and Intelligence API supports some of the systems such as:

- › Applications
- › Email Security Gateways
- › Web Security Gateways
- › Web Browsers
- › Platforms

GAP Analysis

	Data443 Risk Mitigation Inc.	Cisco Umbrella
Support & Pricing		
Free Trial	Yes	Yes
Demo	Yes	No
Quotation-based	Yes	Yes
Subscription-based	Yes	No
Troubleshooting Assistance	Yes	Yes
Core Features		
Real-Time Information	Yes	Yes
Malware File Detection	Yes	No
Phishing and Fraud Detection	Yes	Yes
IP Threat Detection	Yes	Yes
Early Detection	Yes	No
Predictive Phishing Detection	Yes	No
Customization & Integration		
Customizable Categories	Yes	No
Integration Flexibility	Yes	Yes
Cloud Enabled	Yes	Yes
Data & Intelligence		
Comprehensive Coverage	Yes	Yes
Global Data	Yes	No
Up-to-date Data	Yes	Yes
Contextual Data	Yes	Yes
Dynamic Threat Intelligence	Yes	No
Machine Learning	Yes	Yes
Analysis & Response		
Incident Response	Yes	Yes
Threat Prioritization	Yes	Yes
Risk Score	Yes	Yes

Company Overview

Cisco Umbrella is a cloud-based security provider that offers secure web gateway, firewall, and cloud access security broker (CASB) services through a unified cloud security platform. Its solutions, scalable and flexible, protect devices, remote users, and distributed locations globally. Using machine learning, it identifies and predicts malicious domains, protecting organizations from emerging cyber threats.

Integrations

The integrations of Cisco Umbrella Recursive DNS Services and Investigate include:

- › Splunk
- › Zerofox
- › Meraki
- › FireEye
- › CheckPoint
- › Phishme
- › ThreatConnect
- › ThreatQuotient
- › Phantom
- › swimlane
- › Anomali
- › IBM
- › AMP Threat Grid
- › Siemplyfy
- › Others

Supported Systems

Cisco Umbrella Recursive DNS Services and Investigate supports some of the systems such as:

- › Cloud Platform
- › Applications
- › Windows 10
- › Windows 11
- › macOS 11 or later
- › Web Browsers

GAP Analysis

	Data443 Risk Mitigation Inc.	Cisco Talos
Support & Pricing		
Free Trial	Yes	No
Demo	Yes	No
Quotation-based	Yes	Yes
Subscription-based	Yes	No
Troubleshooting Assistance	Yes	Yes
Core Features		
Real-Time Information	Yes	Yes
Malware File Detection	Yes	No
Phishing and Fraud Detection	Yes	Yes
IP Threat Detection	Yes	Yes
Early Detection	Yes	No
Predictive Phishing Detection	Yes	No
Customization & Integration		
Customizable Categories	Yes	Yes
Integration Flexibility	Yes	Yes
Cloud Enabled	Yes	Yes
Data & Intelligence		
Comprehensive Coverage	Yes	Yes
Global Data	Yes	Yes
Up-to-date Data	Yes	Yes
Contextual Data	Yes	Yes
Dynamic Threat Intelligence	Yes	No
Machine Learning	Yes	No
Analysis & Response		
Incident Response	Yes	Yes
Threat Prioritization	Yes	No
Risk Score	Yes	No

Company Overview

Cisco Talos is a cybersecurity intelligence and research group focused on defending organizations against evolving cyber threats. It combines expert security teams with advanced technology to offer comprehensive threat intelligence. This intelligence supports organizations in detecting, analyzing, and mitigating cybersecurity risks. Talos uses real-time data and research to provide actionable insights against malware, ransomware, phishing, and other cyber threats.

Integrations

The integrations of Cisco Talos Incident Response include:

- › Splunk
- › IBM QRadar
- › LogRhythm
- › Palo Alto
- › McAfee
- › Symantec Security Analytics
- › FireEye Helix
- › CrowdStrike Falcon
- › Fortinet FortiGate
- › Check Point
- › Rapid7 InsightIDR
- › Cisco SecureX
- › ThreatConnect
- › Forescout eyeExtend
- › Others

Supported Systems

Cisco Talos Incident Response supports some of the systems such as:

- › Cloud Applications
- › Windows
- › macOS
- › Web Browsers

GAP Analysis

	Data443 Risk Mitigation Inc.	IPXO
Support & Pricing		
Free Trial	Yes	No
Demo	Yes	Yes
Quotation-based	Yes	Yes
Subscription-based	Yes	No
Troubleshooting Assistance	Yes	Yes
Core Features		
Real-Time Information	Yes	Yes
Malware File Detection	Yes	No
Phishing and Fraud Detection	Yes	No
IP Threat Detection	Yes	Yes
Early Detection	Yes	Yes
Predictive Phishing Detection	Yes	No
Customization & Integration		
Customizable Categories	Yes	Yes
Integration Flexibility	Yes	Yes
Cloud Enabled	Yes	Yes
Data & Intelligence		
Comprehensive Coverage	Yes	Yes
Global Data	Yes	Yes
Up-to-date Data	Yes	Yes
Contextual Data	Yes	Yes
Dynamic Threat Intelligence	Yes	No
Machine Learning	Yes	No
Analysis & Response		
Incident Response	Yes	Yes
Threat Prioritization	Yes	No
Risk Score	Yes	No

Company Overview

IPXO is a comprehensive Internet Protocol platform that streamlines IP address management for businesses. It offers solutions for IP acquisition, management, security, and data intelligence, facilitating efficient leasing and monetization of IPv4 and IPv6 resources across more than 75 industries. IPXO's services include DNS management, abuse management, IP reputation, and delegated RPKI, among others.

Integrations

The integrations of IPXO IP Reputation include:

- › Equinix
- › Zyte
- › HostPapa
- › Avast
- › Namecheap
- › Deft
- › Splunk
- › Salesforce
- › Mailchimp
- › Microsoft 365
- › AWS
- › G Suite
- › Symantec
- › Others

Supported Systems

IPXO IP Reputation supports some of the systems such as:

- › Applications
- › Email Security Gateways
- › Platforms
- › Web Browsers



Main Campus

4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Data443

Website: www.data443.com
Email: info@data443.com

Call

US: +1 919 526 1070
UK: +44 203 7693 700

Support & Pricing

Free Trial	Yes	Yes	No	Yes	Yes	No	No
Demo	Yes	No	No	No	No	No	Yes
Quotation-based	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Subscription-based	Yes	No	No	Yes	No	No	No
Troubleshooting Assistance	Yes	Yes	No	No	Yes	Yes	Yes

Core Features

Real-Time Information	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Malware File Detection	Yes	No	Yes	No	No	No	No
Phishing and Fraud Detection	Yes	Yes	Yes	Yes	Yes	Yes	No
IP Threat Detection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Early Detection	Yes	No	Yes	No	No	No	Yes
Predictive Phishing Detection		No	Yes	No	No	No	No

Customization & Integration

Customizable Categories	Yes	Yes	No	No	No	Yes	Yes
Integration Flexibility	Yes	No	Yes	Yes	Yes	Yes	Yes
Cloud Enabled	Yes	No	No	Yes	Yes	Yes	Yes

Data & Intelligence

Comprehensive Coverage	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Global Data	Yes	No	Yes	Yes	No	Yes	Yes
Up-to-date Data	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Contextual Data	Yes	No	No	Yes	Yes	Yes	Yes
Dynamic Threat Intelligence	Yes	No	No	Yes	No	No	No
Machine Learning	Yes	No	No	No	Yes	No	No

Analysis & Response

Incident Response	Yes	No	Yes	Yes	Yes	Yes	Yes
Threat Prioritization	Yes	No	Yes	No	Yes	No	No
Risk Score	Yes	No	No	No	Yes	No	No