Cyberstash Managed Threat Intelligence Gateway

Summary

An automated, predictive, actionable cybersecurity service that protects your organisation by blocking millions of cyber threats in real time.

Predictive intelligence must also be automated, real-time, and actionable. It should be integrated with an organisation's existing IT infrastructure and, most importantly, be used effectively and efficiently knowing about the sources of threats but doing nothing until they target your organisation is neither effective nor efficient. To optimise risk and resources, it's better to:

Protect exposed services:

Proactively block inbound communication from IP addresses used by attackers.

Minimize exposure:

Proactively block traffic to and from countries or autonomous systems known to be associated with high levels of cyber-criminal activity.

Protect users:

Proactively block outbound communication to IP addresses and domains used by attackers

Benefits

Increases your cybersecurity program ROI by taking proactive blocking action against emerging threats and thereby reducing the workload on your security staff

Strengthens network security defences and evidently reduce risk by proactively blocking threats using re-al-time defensive controls powered by a vast arsenal of globally collected threat intelligence indicators.

How does it work?

The solution uses sophisticated threat intelligence to defend organisations against cyber threats. At any given time, the Internet hosts millions of IP addresses and domains with links to malicious cyber activity. All of us are connected to a global network; none of us works in isolation, and we all face similar threats from adversarial sources that do not discriminate when deciding who to target. CyberStash leverages the collective threat intelligence gathered globally to detect and block known and emerging threats in real time and reduce an organisation's exposure to the staggering number of potential attackers.

What are we up against and how do we respond?

An unbelievable 850,000 new malicious IP addresses are launched each day; 8 million spam and phishing attacks occur every day, and 30-to-50 million malicious domains exist at any one time.

For most organizations, the big challenge is getting hold of the right-fit technology, skills, and resources to implement a truly effective security program - one that can draw on the immense protective and detective value of collective threat intelligence as part of a defense-in-depth approach to implementing a cybersecurity program that demonstratively reduces business risk.

What you get

Cloud-native management of your policies, intelligence, investigation, & reporting that's self-managed, co-managed or completely managed by CyberStash Security Analysts.

Protection against 150 million known threat indicators using continuously updating, risk-based, policy-driven, actionable threat intelligence that blocks and detects known sources of threats.

A Threat Intelligence Gateway that provides up-to-the-minute, line-speed protection against known sources of threats, both inbound and outbound, at scales of up to 10 Gbps.

Leverage of a vendor-agnostic open platform with centralised management to enforce risk-driven policies, to inform threat hunting, and to investigate and respond to incidents.

Cyber Threat Inetligence Framework

The CyberStash Managed Threat Intelligence Gateway solution aligns with the following framework for operationalising Cyber Threat Intelligence:

Collect

- Collection of millions of accurate threat indicators from multiple sources including commercial and open-source feeds and government advisories.
- Multiple types of threat intelligence including IP reputation blocklists, malicious domains and high-risk Autonomous Systems Numbers (ASNs).

Aggregate

- Multiple threat aggregation and consolidation into a single feed.
- An open platform that easily integrates threat intelligence with standards like STIX/TAXII
- Analytics to drive advanced intelligence and threat detection.

Automate

- Threat feeds dynamically updated in real-time.
- Automated emerging threat protection.
- Automated risk-based policy application at line-speed.

Detect

- Pivot, hunt for and investigate suspicious traffic.
- Block previously unknown threats and unwanted traffic.
- Advanced network-centric threat detection.

OUT-OF-BOX THREAT INTELLIGENCE

The CyberStash Threat Intelligence Gateway solution is integrated with the following commercial and threat intelligence providers. It comes out-of-the-box with millions of indicators and allows organisations to add their own intelligence feeds:

WELL-FED THREAT INTELLIGENCE
Well-Fed threat intelligence is generated by charting attackers to see where they actually live so you have the latest information to protect yourself. Approximately one million malicious domains are monitored every hour and are curated and whitelisted to ensure that you have reliable information you need to protect yourself from cybercriminals. This includes Sinkhole IP Feed, DGA Feeds, and MaldomainML which is a feed based on proprietary machine learning and analytical methods of DNS telemetry developed in Bambenek Labs.

MALWARE PATROL THREAT INTELLIGENCE
Malware Patrol specializes in real-time threat intelligence that protects users and enterprises in over 175 countries against cyber attacks. The highly refined and continuously updated indicators identify compromised machines, botnets, command and control (C2) servers, malware, ransomware, cryptominers, DGA infrastructure, phishing, DNS over HTTPs (DoH) resolvers, and Tor exit nodes.

PROOFPOINT ET INTELLIGENCE™
Proofpoint ET Intelligence provides actionable, up-to-the-minute IP and Domain reputation feeds.

WEBROOT BRIGHTCLOUD® IP

Bright Cloud Dynamic domain threat intelligence feed provides us with 5,000 domains per minute, resulting in intelligence on over 230 million domains per month.

INTEL 471 THREAT INTELLIGENCE
Threat Intelligence is derived from across 14 countries to provide near real-time coverage of threat actors and malware activity. Intel 471's Malware Feed consists of Malware IP Indicators possessing high confidence, timely and rich context curated from Intel 471's industry leading access in the cybercriminal underground. Types of malware covered are banking trojans, infostealers, loaders, spambots, and ransomware.

CYJAX THREAT INTELLIGENCE FEED
The Cyjax Threat Intelligence feed consists of a validated feed of contextualised IP and domain indicators of compromise (IOCs) discovered from Cyjax research and across the threat landscape to allow for additional enrichment and cross-correlation with other threat information and intelligence.

DOMAINTOOLS MALICIOUS DOMAIN BLOCK LISTS
Domain and DNS data covering over 95% of all registered domains, used predictively before any malware has caused damage.

BITDEFENDER THREAT INTELLIGENCE FEED

Bitdefender Labs correlates hundreds of thousands of Indicators of Compromise (IoCs) collected through the Global Protective Network (GPN) protecting hundreds of millions of systems globally and turn data into actionable, real-time insights into the latest threats.
The Bitdefender Advanced Threat Intelligence solution consists of unique feeds including:

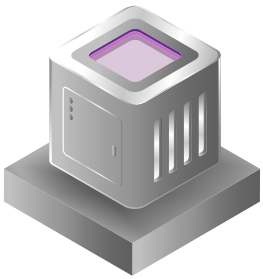
- *Advanced Persistent Threats (APT) Domains - A collection of domains hosting Advanced Persistent Threats Malicious Domains - A collection of domain addresses associated with general malware activities*
- *Phishing Domains - A collection of domain addresses associated with phishing attacks*

CYBERSTASH EMERGING DOMAINS AND IP BLOCK LISTS
Indicators released by Government advisories and emerging Advanced Persistent Threats (APTs) are added to the CyberStash block list.

OPEN-SOURCE THREAT FEEDS

The CyberStash Threat Intelligence Gateway solution is integrated with the following open-source threat intelligence providers:

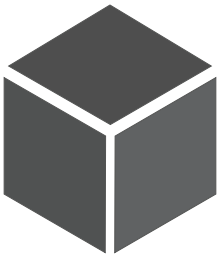
- **Cisco Talos**
- **Blocklist.de**
- **CINS Army List**
- **Abuse.ch**
- **Check Point Tor List**
- **DHS CISCP**
- **Emerging Threats Block Rules**
- **Ransomware Tracker**
- **State of Missouri SOC**
- **ZeuSTracker**



BYO INTEL FEEDS & INTEGRATIONS

The Threat Intelligence Gateway also integrates with most other commercial and open-source intelligence providers. This effectively gives our clients the unlimited potential to expand their threat intelligence capability. In fact, we have over 50 point-and-click integrations with Threat Intelligence Platforms, SIEMs, SOARs, and other applications.

Service Packages



CyberStash combines best-in-class technology, people, and processes to deliver its Managed Threat Intelligence Gateway Service.

	Standard	Enterprise	Managed
Throughout	**Up to 10 Gbps per Gateway**		
Service Establishment	✓	✓	✓
Out-of-Box Threat Intelligence	✓	✓	✓
Emerging Threat Protection	✓	✓	✓
Baseline Policy Development	✓	✓	✓
Device Life Cycle Management	✓	✓	✓
Block List & Allow List Management	✓	✓	✓
Event Logging to Client SIEM	✓	✓	✓
Service Management	✓	✓	✓
Risk-Based Policy Development	—	✓	✓
Policy Enhancement and Tuning	—	✓	✓
CyberStash Emerging Threat Management	—	✓	✓
Incident Response Management	—	✓	✓
CyberStash Cloud SIEM	—	—	✓
DNS Logging and Correlation	—	—	✓
Threat Detection and Response	—	—	✓
Real-Time Threat Dashboards	—	—	✓

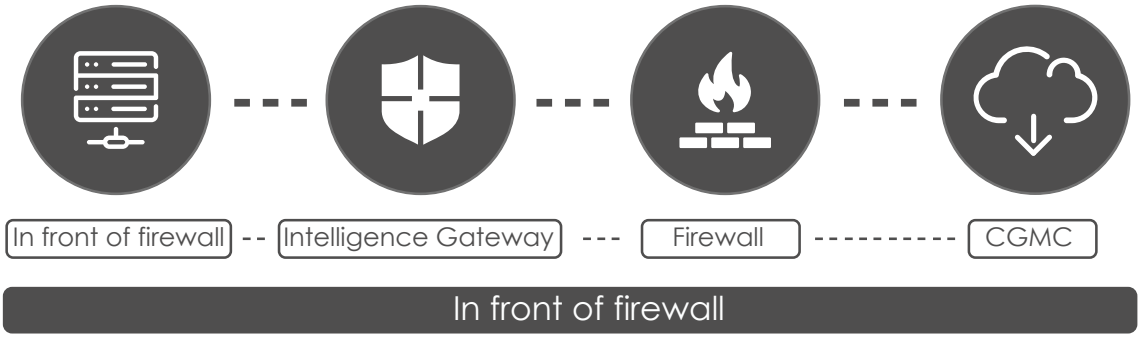
Deployment Options

The Threat Intelligence Gateway is either deployed in front of your perimeter firewall or behind it. CyberStash works with your team to select the preferred deployment model as part of the solution design. We provide on-premises and Public Clouds deployment options such as AWS, Microsoft Azure (coming soon) and Google Cloud (coming soon).

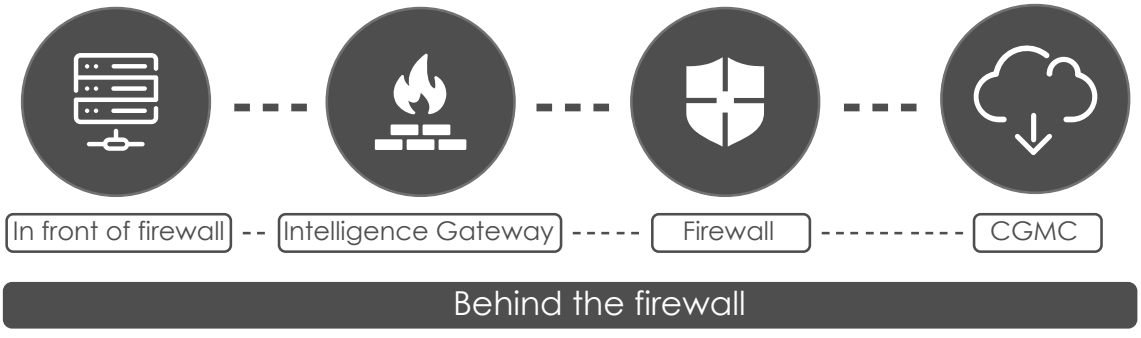
The Gateway connects to your network at layer-2 with 2 of its ports paired in bridge mode, so there is no need to change the IP addressing of your existing infrastructure.

The Gateway includes a management interface that connects to your DMZ or corporate network. The management interface is used to communicate with the CyberStash Global Management Centre (CGMC) in the cloud where policies are configured and enforced. It is also used to continuously fetch new threat indicators from CGMC.

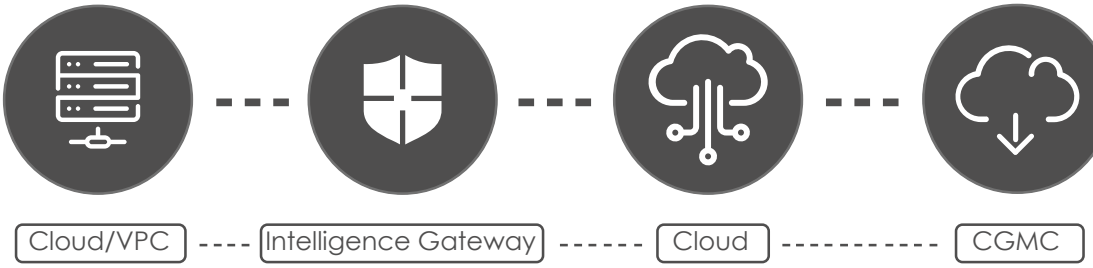
The hardware supports either Ethernet or fibre ports and can be configured to fail-close or fail-safe. When operating in fail-safe mode, traffic passes through the Threat Intelligence Gateway if the hardware fails.



In front of firewall



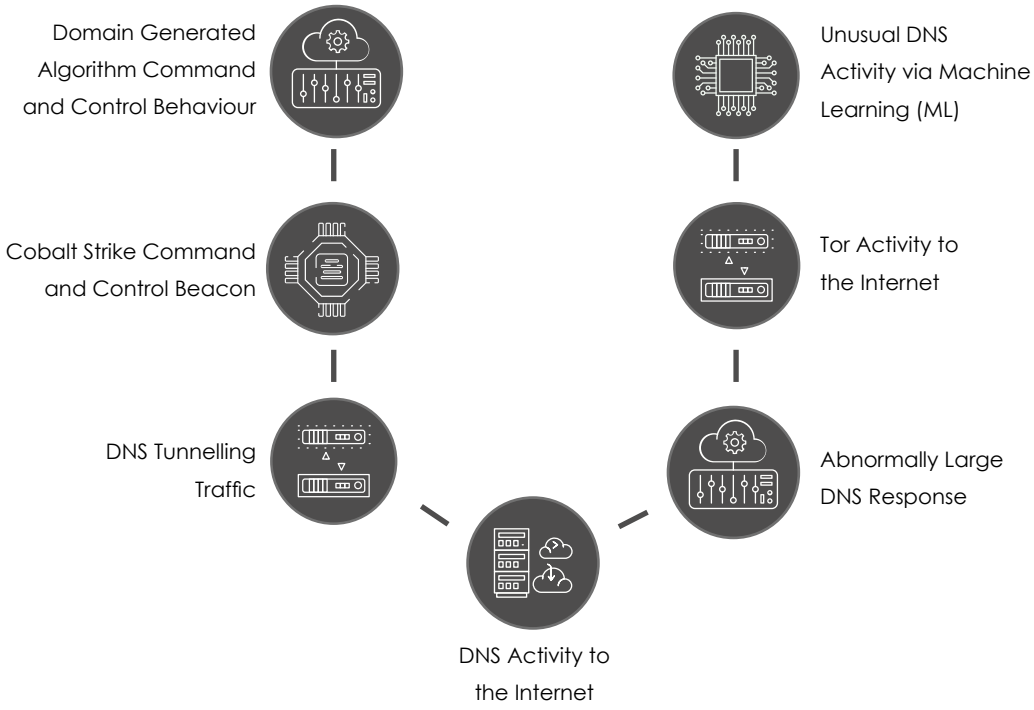
Behind the firewall



Behind of cloud

Threat Management Architecture

As part of our Premium Service Package architecture, CyberStash collects DNS events from the client's environment and network traffic events from the Threat Intelligence Gateway, which is also deployed on client premises. We then securely transport these events to the CyberStash Cloud SIEM, which allows us to provide threat correlation, hunting, investigation and advanced threat detection.



Risk-Based Threat Classification Policies

CyberStash classifies and responds to threats by Threat List Policies, Block List Policies, Country List Policies and ASN List Policies.

Maximise configuration flexibility, risk-Based Policies are applied separately to inbound and outbound traffic, to specific asset groups, and to the following threat categories:

- **Command and Control**
- **Endpoint Exploits**
- **Botnet**
- **Drop Site**
- **Web Exploits**
- **Spam**
- **Scanner**
- **Advanced Persistent Threat**
- **Brute Force Password**
- **TOR / Anonymizer**
- **Proxy / VPN**
- **DDOS**
- **Compromised**
- **Fraudulent Activity**
- **Illegal Activity**
- **Undesirable Activity**
- **P2P Node**
- **Online Gaming**
- **Remote Access Server**

Incident Response management

Our Advanced and Premium Service Packages include Incident Response Management. This enables our clients to call on the CyberStash security team to respond on their behalf and block an attack by:

- IP Address or CIDRs
- Domain
- IP Address or CIDRs
- Autonomous Systems 3 Numbers(ASNs)

CyberStash combines threat intelligence with technology, processes, and skills to massively reduce an ganisation's exposure to most known sources of threats on the Internet. We provide real-time, automated, and predictive threat protection, detection, and incident response, by leveraging threat intelligence to minimise an organisation's risk to cyber threats.

Inquiries
info@cyberstash.com
www.cyberstash.com/contact/sales-inquiries

Become a Reseller
info@cyberstash.com
1300 893 802