The Easiest Way to Inspect, Protect and Gain Visibility Into Encrypted HTTPS Internet Traffic

The iboss cloud can easily inspect, protect and provide visibility into encrypted HTTPS Internet traffic.

Selective HTTPS Decryption Overview

The iboss cloud has deep SSL and TLS inspection capabilities built into the platform. Highly configurable selective decryption options are available to choose what encrypted traffic to inspect and which traffic to leave untouched. And since iboss cloud runs in the cloud, the ability to decrypt at massive scale is achieved. The iboss cloud can instantly deliver the following benefits:

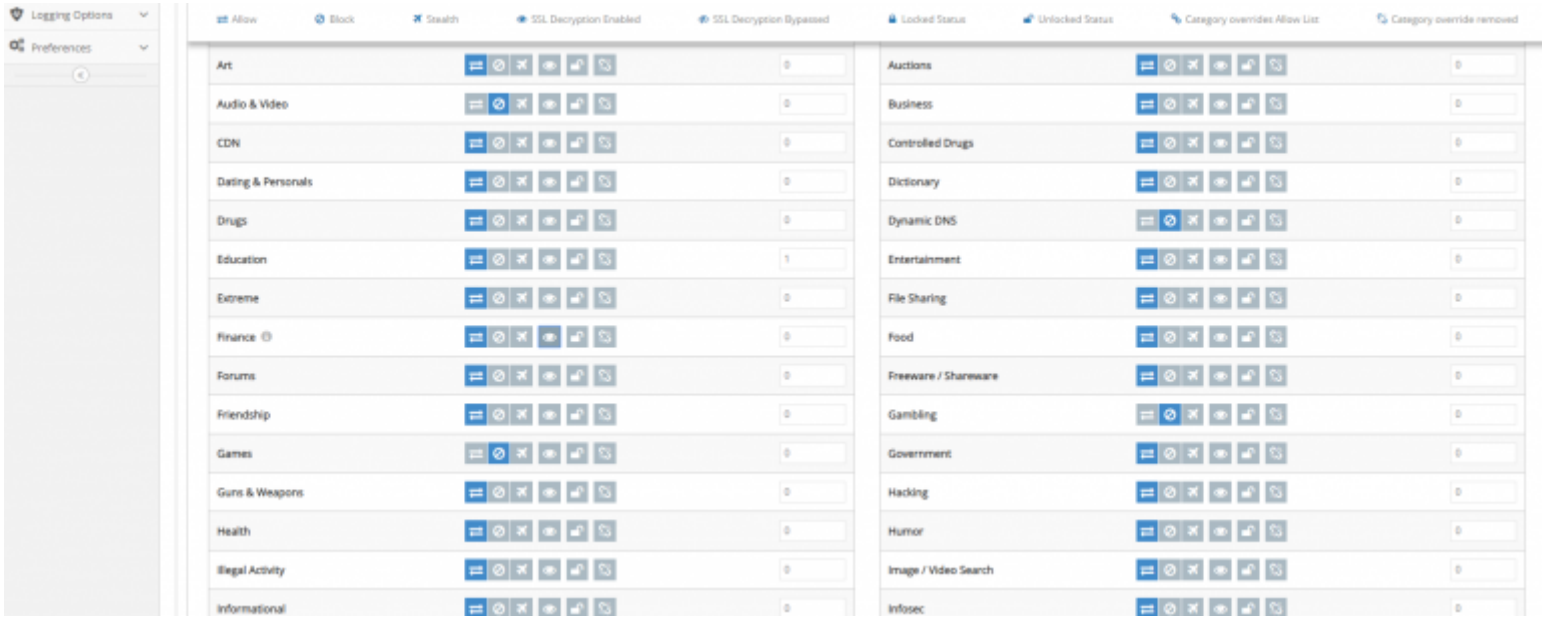
- Inspect encrypted HTTPS, SSL and TLS traffic to gain visibility into previously unseen traffic and activity
- Inspect content for malicious files and botnet Command and Control Center callbacks (CnC) to prevent malware and re-mediate infections quickly
- Gain visibility into activity including search engines to detect high risk and at risk users through detailed reports which include search terms and other full URL events
- Gain control over risky behavior on encrypted sites including preventing access to risky content and searches resulting in risky results
- Gain control and visibility over YouTube and other streaming video sites to prevent dangerous content and reduce bandwidth from unproductive activities
- Selectively choose what to decrypt from a vast number of criteria including decrypting based on domain, IP Address, category, and user group
- Prevent data loss by inspecting files and content buried deep inside encrypted HTTPS traffic which might be headed to storage sites such as DropBox and Box
- Easily deploy and implement SSL decryption within seconds as all of the complexities are handled by the iboss cloud platform automatically

Challenges Related to HTTPS and Encrypted Traffic

Encrypted traffic is predicted to reach and surpass over 75% of all web traffic in 2019. The movement to HTTPS is required for privacy and security. This presents various challenges as the encrypted traffic prevents proper inspection for malicious transfers and non-compliant activity. Regulations mandate and impose penalties for not properly inspecting and preventing access and transfers to content that violate regulations. This includes inspection of content related to insider trading in finance for SEC compliance, PII and health records in the medical field for HIPAA compliance, and adult content and violence in education for CIPA compliance. Inspecting encrypted traffic has many challenges that result in a high burden to IT staff that are responsible for ensuring the safety of the organization and its users:

- Designing a solution to perform decryption can be complex and involves expert knowledge of asymmetric encryption best practices which is the foundation of HTTPS
- Deploying decryption involves implementing a strategy to push the needed "root" certificates to devices which is complex due to the varying device types in use
- If decryption is available on the web gateway appliance solution, the load on web gateway appliances and proxies increase exponentially when decryption is enabled bringing the network to a halt
- The cost of purchasing and deploying more security appliances for the purpose of decryption becomes extremely costly and unmanageable blowing out IT budgets
- The need to decrypt traffic on organizationally owned devices while users are mobile make implementation even more challenging as users are outside of the network perimeter
- The need to selectively decrypt becomes very challenging as some traffic, such as trusted banking sites, do not need to be inspected
- Without inspecting encrypted HTTPS traffic, the organization becomes more blind by the day to Internet traffic containing malicious and non-compliant transfers which results in the inability to control the transfers and the increasing lack of visibility within reporting tools

The iboss cloud Solves the HTTPS Decryption Challenge



The iboss cloud was designed with the modern Internet in mind and includes all of the features necessary to inspect and control encrypted HTTPS traffic. The iboss cloud can solve these challenges easily as it abstracts all of the difficulties related to implementing HTTPS decryption so that IT administrators can focus on securing users.

Gain Visibility and Control Over HTTPS Encrypted Traffic

The iboss cloud will inspect the full contents of HTTPS transfers, including files, headers and full URLs to ensure proper visibility and control are applied. IT administrators gain the inspection capabilities needed into previously blind traffic to enforce the security rules in place to reduce risk. Detailed event logs are also produced providing the necessary visibility into user activity and transfers generated from encrypted transfers.

Inspect Encrypted Transfers for Malware and Infections

The amount of malware being transferred over encrypted HTTPS channels is increasing by the day. To make things worse, infected devices are using encrypted HTTPS to phone home to Command and Control centers at an alarming rate. The iboss cloud will decrypt HTTPS traffic and ensure that the files being transferred are free from malware. In addition, the communications being performed over HTTPS are inspected to determine if they are related to infected device communication so that the communication is blocked and IT staff is alerted.

Gain Visibility Into User Activity in Detailed Reports

Most search engines encrypt queries and search terms over HTTPS websites. This makes it difficult for administrators to get the visibility needed to identify risky and non-compliant behavior which is mandatory for compliance. The iboss cloud can easily inspect and extract the information necessary so that administrators get the details they need within reports, including detailed and granular URL logs that contain the full URL and search terms being accessed. The iboss cloud includes noise filters to quickly highlight the searches across popular search engines, such as Google, to get to the information needed quickly and easily.

Gain Control over Encrypted Cloud Applications Including Streaming Video Sites

The iboss cloud includes extensive CASB controls to inspect and apply policies to popular sites and cloud applications. This includes controls for YouTube and other streaming sites that perform transfers over encrypted HTTPs connections. With the ability to inspect and control encrypted HTTPS traffic, policies can be applied which reduce unnecessary bandwidth waste and increase productivity while reducing high risk behavior that can put an organization and its users at risk.

Selectively Decrypt HTTPS

The iboss cloud has advanced HTTPS decryption features including the flexibility needed to determine what gets decrypted and what remains untouched. Administrators can choose to decrypt based on a variety of criteria including website, IP Address, category and user group membership. The iboss cloud will automatically use it's extensive signatures and databases to determine what traffic should be passed along untouched based on the configured rules. This allows security to be applied, but highly trusted and sensitive applications to move untouched.

Prevent Data Loss Hidden in Encrypted Traffic

The iboss cloud can inspect full files, including Zip and compressed archives, for PII and other sensitive information. Combining this capability with the ability to decrypt and inspect HTTPS allows for a powerful combination that prevents unnecessary data loss and reduces organizational risk tremendously.

Easily Deploy HTTPS Inspection and Decryption

The iboss cloud makes implementing and deploying HTTPS decryption and inspection easy. The iboss cloud connectors automatically configure the endpoints with all of the necessary settings needed to perform decryption, including installing the needed HTTPS trusted CA root certificate which is traditionally manually installed. In addition, the massive cloud scale of iboss cloud allows any volume of decryption without impacting performance or having to deploy more security appliances. This solves issues for any organization that has tried to decrypt only to find the network is completely interrupted and the existing appliances are overloaded. The iboss cloud runs in the cloud and can process any amount of encrypted traffic necessary to gain the control and visibility desired by IT staff. Best of all, deploying SSL decryption with iboss cloud can be completed in seconds versus months, saving valuable IT time and overhead.

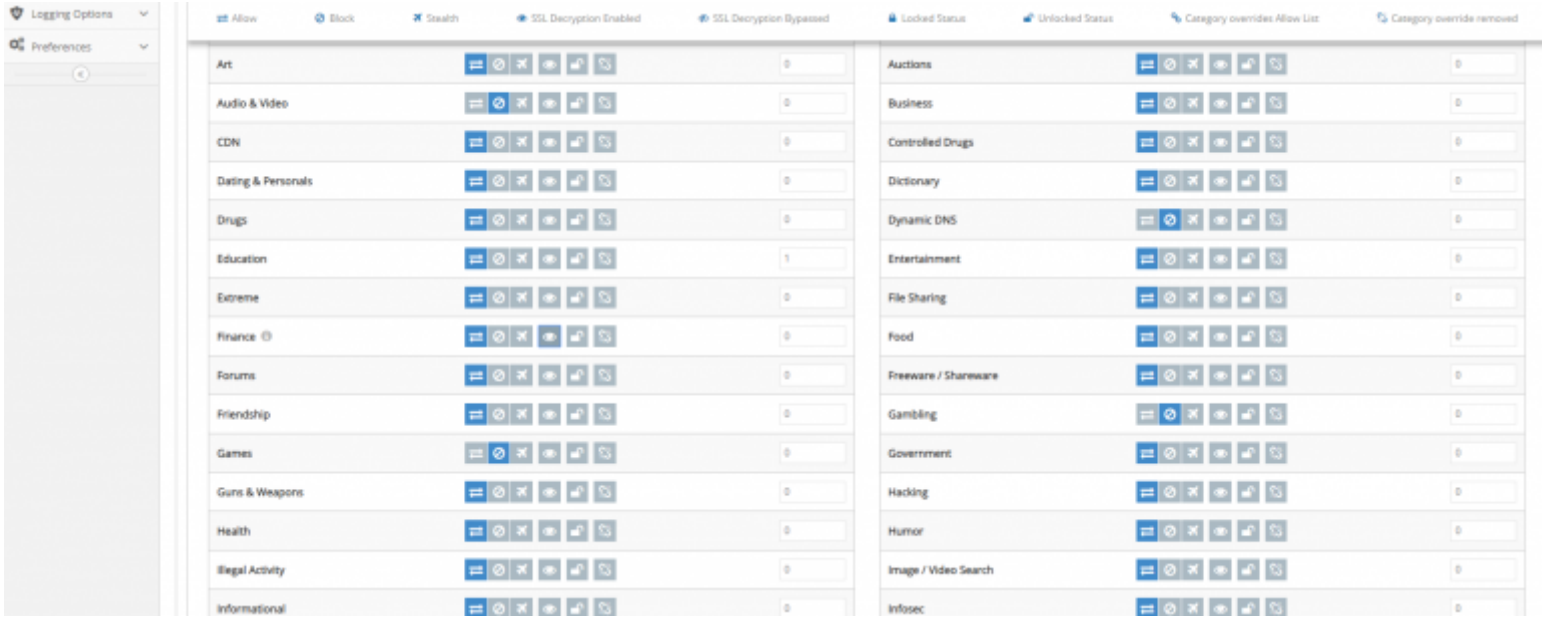
How It Works

Decrypting HTTPS with iboss cloud is fast and easy:

1. Get an active iboss cloud account
2. Connect users to iboss cloud using an iboss cloud connector. The connector handles everything necessary for configuring the endpoint to perform SSL decryption. Connectors are available for virtually all Operating Systems including Windows, Mac, iOS and Chromebooks
3. Enable HTTPS decryption within the iboss cloud admin console. Choose whether to decrypt all sites or selectively decrypt by categories, groups and other criteria
4. The iboss cloud platform handles the rest and administrators will see detailed logging traffic from HTTPS sites in the logs as well as be able to control HTTPS destinations on the Internet

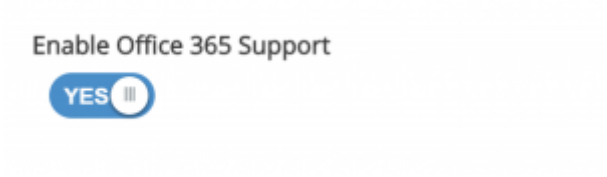
Feature Highlights

Selectively Decrypt by Category



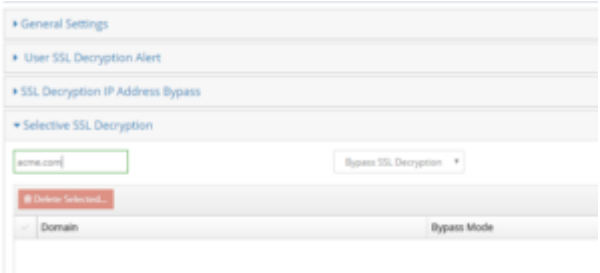
The iboss cloud can dynamically categorize Internet access to various destinations automatically. By combining this ability with HTTPS decryption, administrators can choose which categories they would like to decrypt or bypass and the iboss cloud will automatically apply those rules on a site by site basis depending on the site's category. Category based selective decryption can also be applied on a group by group basis to give even more granular control over decrypted content.

Ensure SSL Decryption Does Not Interrupt Office 365



By simply enabling Office 365 support within the iboss cloud, connections to Office 365 will never be interrupted as the iboss cloud is tied to Microsoft for changing signatures related to Office 365 traffic. This ensures users will have the best Office 365 experience and be as productive as they can be at all times.

Bypass SSL Decryption By Domain



Selectively bypass or decrypt by domain. This provides granular flexibility when needing to bypass or decrypt specific website destinations which are highly trusted and secure.

Pricing

SSL Decryption Capabilities	
SSL Decryption capabilities, including infinite scaling and selective decryption, are included at no cost with every iboss cloud subscription	Contact Us

For more information on SSL Decryption within iboss cloud, please visit https://www.iboss.com/platform/inspect-encrypted-ssl-traffic.

About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, iboss is designed to make transitioning from security appliances to cloud security a seamless process. iboss is trusted by more than 4000 organizations worldwide, spans over 100 points of presence globally and is backed by over 110 patents.

To learn more, visit https://www.iboss.com