The Platform

Easily and Selectively Inspect Encrypted HTTPS Traffic

Make the change from using cumbersome appliances to perform SSL decryption to inspecting encrypted content in the cloud with iboss

As websites and cloud apps move to encrypted HTTPS connections, the need to inspect encrypted content is a critical capability to meet compliance, prevent malware and protect against data loss. Performing decryption with network appliances is expensive and does not scale. The iboss cloud performs this function in the cloud to inspect encrypted traffic at scale and with ease.

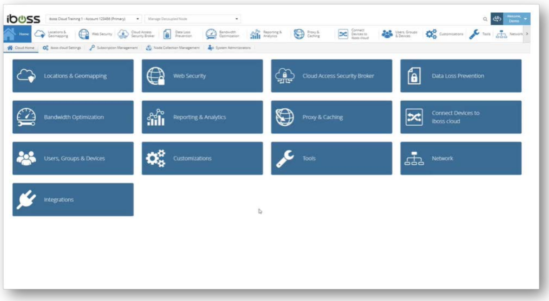
Selectively decrypt HTTPS traffic to inspect content for compliance, malware and data loss

Decrypt traffic based on a variety of criteria including user, group, category and source

Leverage the elasticity of the cloud to decrypt traffic at scale

Selectively decrypt HTTPS traffic to inspect content for compliance, malware and data loss

Although decrypting SSL/TLS HTTPS traffic is a necessity, the need to do so may need to be selectively controlled. For example, it may be desirable to avoid breaking HTTPS on highly trusted financial sites while decrypting traffic to destinations that host generic files, like Box or Dropbox. The iboss cloud provides a broad array of selective decryption options that allow certain traffic to be decrypted while leaving other traffic untouched.

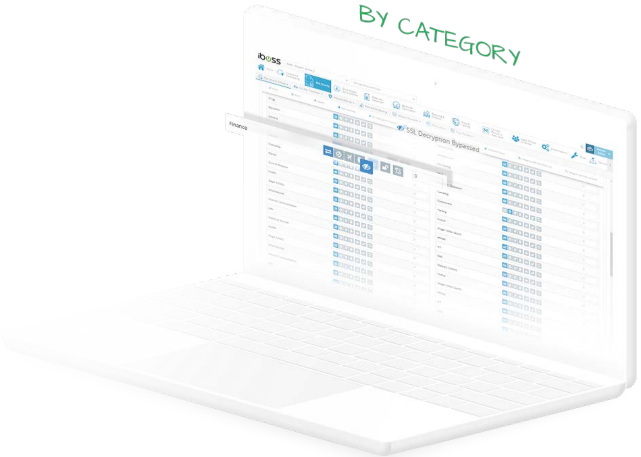


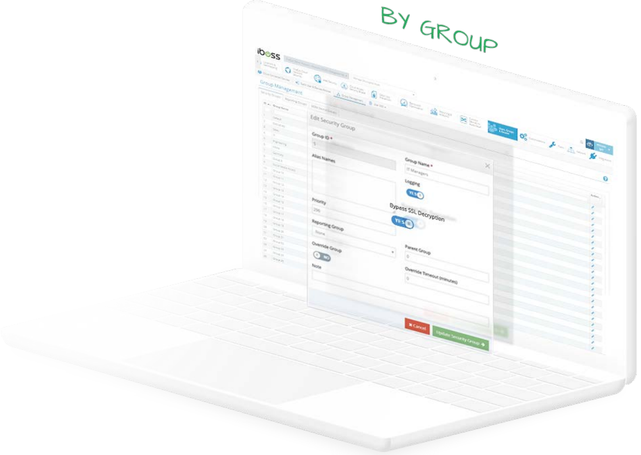
These granular and selective controls on HTTPS decryption and bypass are critical in ensuring administrators have the tools they need to adequately apply web filtering, compliance, malware defense, botnet detection and data loss protection to users in the organization.

Decrypt traffic based on a variety of criteria including user, group, category and source

HTTPS decryption can be applied to specific users or groups of users on the network based on a user's Active Directory Group, LDAP Security Group or Organization Unit (OU).

Specific destinations can be decrypted by specifying specific domains. Complete categories of websites can be decrypted or bypassed from decryption. Or, decrypti on can be applied to a network subnet or bypassed for the subnet altogether.


By CATEGORY


By GROUP

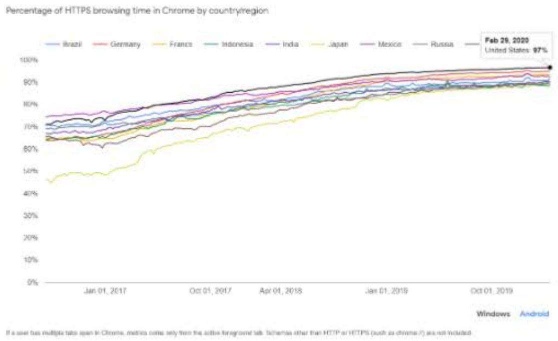
By DOMAIN OR APP

Decrypt or Bypass easily by domain
Easily Decrypt Specific apps

By NETWORK SUBNET

Leverage the elasticity of the cloud to decrypt traffic at scale

Encrypted SSL/TLS traffic continues to be on the rise. According to Google's Transparency Report on HTTPS traffic, as of the end of the end of February 2020, 97% of all browsing time through the Chrome browser was over HTTPS encrypted connections. Virtually all data traveled to the cloud over encrypted data channels making it impossible to inspect and protect network data which is masked by the protected connection.



Google HTTPS Transparency Report – Percentage of Browsing Time Over HTTPS

View the Google HTTPS Transparency Report.

With this amount of encrypted HTTPS traffic, there are no amount of network security appliances that can handle the load of performing HTTPS decrypt so that compliance, malware defense, and data loss can be applied to cloud connections. To make things worse, without decryption, reporting visibility vanishes as the content of the connections is not visible for the purposes of reporting.

The iboss cloud delivers network security as a service, in the cloud. This allows organizations to decrypt any volume of HTTPS traffic for network security without worrying about increasing costs or slowing cloud connections due to HTTPS decryption. The iboss platform delivers the service through the use of containerization, which allows infinite horizontal scaling. Horizontal scaling allows the iboss cloud to add more "checkout lanes" as bandwidth and encrypted traffic increase to ensure fast connections from anywhere in the world.

Buy Now

The iboss cloud can secure user Internet access on any device, from any location, in the cloud. Best of all, you can start using it immediately to protect your users instantly.

What you get

- In the cloud Internet security
- Advanced Internet malware protection that follows users
- Advanced cloud and SaaS controls
- Web filtering and compliance controls
- Internet security for in-office users without appliances
- Branch office Internet security without data backhaul
- And a lot more...

Buy now

Contact Us

Get in touch with a technical specialist for a live demo.

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEIA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

Contact Us