



# Web Security Services

The rapid expansion of public cloud services, remote workers and BYDO has revolutionized how and where data is stored and accessed.

Protect your business in the cloud and as your users become more mobile and personal and business data comingles on removable media and devices.

ZebraCloud Services protects networks from the most advanced threats while saving valuable time and resources. Email Security are built on a common architecture, allowing for hassle-free maintenance and software updates to ensure the highest level of protection.

ZebraCloud Services was established to provide small and medium sized organizations with access to edge technologies that are generally designed and deployed across large organizations. These small and medium sized organizations present information security needs that require harsh standards and high compatibility demands, based on pay-as-you-go models.

## Top 3 Problems We Solve

1

Outsmart advanced threats with real-time security ratings to both web and email traffic that rapidly identify and classify information.

---

2

Stop more advanced, non-signature threats to your data than any other solution, protecting users everywhere, even on third-party networks.

---

3

Prevent email-based threats like ransomware, from reaching your network. Phishing education reminds users, wherever they are, not to click on suspicious links.

---

# Web Security Services

ZebraCloud Web Security Services is a flexible web protection solution that provides fine-tuned control over your users' web access, while providing comprehensive protection against web threats such as viruses, malware, data loss, and phishing attacks.

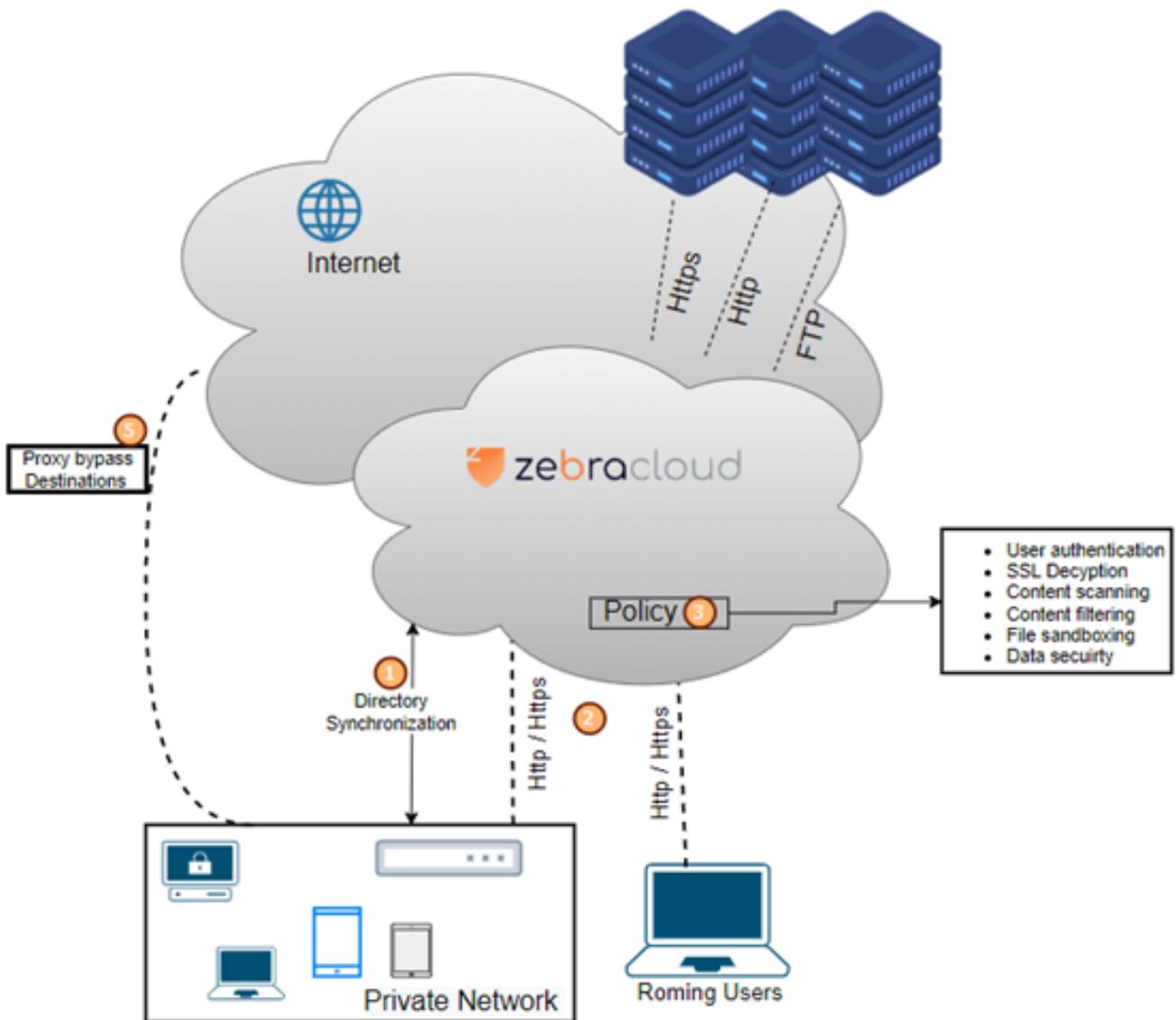
## How ZebraCloud Web Security Services works

ZebraCloud Web Security Services operates as a proxy server for HTTP and HTTPS traffic, as well as FTP over HTTP. When users request a web resource, their browsers do not connect directly to Internet web servers, but instead connect to the cloud proxy, which in turn relays requests to the origin server. This allows the cloud service to apply filtering rules and perform content scanning, providing protection against security threats, data loss, and inappropriate content.

The service can use various methods to identify and authenticate users: The ZebraCloud Web Security Services Endpoint, a third-party single sign-on identity provider, NTLM transparent identification, or manual authentication with a user name and password. Roaming users (those connecting from an unknown IP address) can be identified via the ZebraCloud Web Security Services Endpoint, via a single sign-on provider, or they are required to authenticate.

Optional SSL decryption allows the content of HTTPS sessions to be scanned, and allows the service to show the correct notification page to users (for example, a block page if the SSL site is in a category that is blocked). Content is re-encrypted after inspection.

# ZebraCloud Web Security Services



## The diagram shows the following elements of the service



Directory synchronization allows user details from an LDAP directory to be synchronized with the cloud, enabling users to be identified and authenticated. This allows user- and group-level policy settings to be applied, as well as providing detailed user-level reporting.



Web traffic is directed to the cloud service from a private network, and from roaming users connecting from outside their LAN. There are various methods to redirect traffic.



Authentication, filtering and enforcement settings are applied by a policy, which determines which requests to allow or block, performs real-time content scanning, and applies data security filtering, helping to prevent inadvertent or malicious data loss.



When policy decisions have been applied, web requests are then forwarded to the origin server, and content is served to the user's browser. If content is blocked, or security threats are detected, configurable notification pages are shown, informing the user of the reason why access to the resource is not allowed.



Some web requests can go directly to the origin server, if the address is defined as a proxy bypass destination.

# Sandbox

provides real-time, inline, contextual defenses for email security by using composite risk scoring and predictive analytics to deliver the most effective security available. It provides containment by analyzing inbound and outbound traffic with data-aware defenses for data theft protection. Over 10,000 analytics across eight defense areas include real-time classifiers, behavioral sandboxing and other advanced capabilities, enabling sandbox to detect and stop more threats. collects data from more than 900 million endpoints and analyzes 3–5 billion web requests every day.



## Real-Time Security Classification

Inspects all traffic content for malicious or suspicious code such as obfuscated scripts and iframe tags that often hide malware behind dynamic content.



## Real-Time Content Classification

Employs advanced machine learning to quickly and accurately classify web pages into highly granular content categories for effective access filtering.



## URL Classification

Applies current classification information for known web pages, and assesses new pages and links based on associated sites and redirections.



## Behavioral Sandboxing

Allows suspicious files to be executed and evaluated for malicious activities in a secure sandbox which emulates a real machine down to the processor and memory layers.



## Reputation Analysis

Reputation databases are applied to URLs to block web traffic from untrustworthy sources.



## Real-Time Data Classification

Classifies structured and unstructured data with parsing and decoding support to address outbound data theft.

# Customer needs

## Your Needs

## ZebraCloud Solutions

ZebraCloud Solutions

Leverages Sandboxing, going beyond antivirus defenses to provide contextual awareness, composite risk scoring, and multi-layered, real-time analysis of web content.

Prevent malware from entering your network and stealing your data

Scans and analyzes social media sites and content in real time to prevent malware and advanced attacks from entering your network and stealing data or damaging your brand. Secure your remote users with or without endpoint software. Includes an optional lightweight, tamper-resistant client that combines strong web security service enforcement with transparent authentication of users connecting to Zebra Cloud infrastructure.

Empower the social web, but control inappropriate content automatically

ZebraCloud social web controls provide the flexibility to allow Facebook access but prohibit posting content or playing games, or allow access to LinkedIn, but prevent job searches.

Easily add new capabilities, like Email Security, when the time is right

ZebraCloud Web Security and ZebraCloud Email Security are integrated at every level. A single user interface configures both, and both leverage shared management services including user directory synchronization, delegated administration, reporting, account management, and more.

# Customer needs

## Your Needs

## ZebraCloud Solutions

Simplify user authentication/  
identification

ZebraCloud Web Security simplifies user authentication and identification with multiple mechanisms including Endpoint client, identity provider integrations, NTLM identification and Secure Forms with customisable timeouts.

Spend less time on web security

ZebraCloud Web Security reduces business costs and complexity because it is delivered as a service. Everything from processing to hardware to maintenance is managed by Blocking threats at the gateway gives time back to IT to focus on other projects.

Manage and monitor activity and  
performance at any time

ZebraCloud Security includes an intuitive, web-based console that integrates all management and reporting capabilities.

Customizable, easy-to-read  
reporting

Advanced Cloud-based reporting functionality provides fast, efficient, easy customizable reporting with more than 80 pre-defined reports, providing added-value and actionable insight into Security risks, traffic and more.



# Web Security Services