Zscaler™ Cloud DLP
Close the gaps in your data protection strategy

Zscaler Cloud DLP protects against the loss of sensitive data across all users and branches, regardless of location, through full inline SSL inspection

The challenge of data protection in a cloud-first world

Around the globe, reports of data breaches continue to make headlines, while GDPR imposes new rules to strengthen and unify data protection. Traditionally, organizations would respond to such challenges by adding yet another appliance to an already complex security stack, but the transformation to a cloud-first world has changed the rules of the game.

While the new norm consists of applications in the cloud and users connecting directly to them from anywhere, you are inevitably left with blind spots. As your users bypass your security controls while off network, your visibility and control of critical data and personal information is lost.

These blind spots increase your risk of data loss—whether that data is exposed unintentionally due to a lack of user awareness, or it is being extracted maliciously. And, because 70 percent of all web traffic is encrypted¹, sensitive data is often concealed in SSL traffic, which is hard to inspect due to capacity and cost constraints.

Protect your data with Zscaler Cloud DLP

With mobile users and the majority of your applications in the cloud, it makes sense to move your data protection and security controls to the cloud, too. Zscaler Cloud DLP is part of the Zscaler Security Cloud, a platform that sits between users and the internet, inspecting all traffic and providing the same comprehensive protection to all your users, no matter where they go.

Your users might have left the network, but that doesn’t have to mean your sensitive data will leave with them. Zscaler Cloud DLP empowers you to illuminate blind spots by providing protection and visibility where you don’t have it today—and with full content and SSL inspection. Zscaler Cloud DLP enables you to protect sensitive data with advanced controls and granular policy, which can easily be deployed as part of the Zscaler security platform, all while remaining in compliance with regulatory mandates.

Zscaler Cloud DLP benefits

With Zscaler Cloud DLP, you can extend your protection to follow users wherever they go, without bypassing your security controls when connecting direct-to-cloud. Because it’s part of the Zscaler platform, it provides a range of benefits that can only be delivered through a global, purpose-built security cloud:

**Consistent data protection and full SSL inspection**
- Provide identical protection to all users and branch offices
- Scan and monitor every byte inline, without capacity limits, with full SSL inspection
- Leverage advanced controls like Exact Data Match (EDM) to eliminate false positives

**Full integration for better protection**
- Leverage integrated web security, threat prevention, and CASB capabilities
- Simplify administration and reporting with a unified management console
- Easily integrate with your SIEM and third-party DLP or CASB solutions

**Complete visibility and control**
- Extend your visibility to users off network and discover cloud applications
- Control data flowing to shadow IT and unsanctioned applications with granular policies
- Forward logs in real time for faster incident analysis and remediation

**Compliance and data privacy**
- Meet compliance mandates such as PCI, HIPAA, and GDPR with policy that follows the user
- Report on security and risk assessment from anywhere within seconds
- Integrate with existing governance, risk, and compliance (GRC) workflows

**Simplified deployment and architecture**
- Deploy data loss prevention in minutes without changing your network architecture
- Simplify policy creation and administration with integrated workflows
- Reduce network complexity by enabling direct-to-cloud connections

**Reduced cost and complexity**
- Put an end to purchasing, standing up, and maintaining point products
- Eliminate the guesswork of inspection capacity planning with user-based subscription
- Optimize MPLS backhauling and lower total cost of ownership
Zscaler Cloud DLP capabilities

Increase precision with Exact Data Match (EDM)
Maximize your data protection by fingerprinting sensitive information from your databases, without transferring it to the cloud. With EDM and highly customizable policies, Zscaler Cloud DLP can detect and stop the transfer of exact tokens belonging to a particular record to unauthorized parties or services. This technique eliminates false positives and thus improves both your security posture as well as productivity of your administrators.

FEATURES

• Dictionaries and engines
  Leverage predefined dictionaries and preconfigured engines or customize them for your specific needs

• Content matching
  Match specific keywords, patterns, regular expressions, and other identifiers

• Exact Data Match (EDM)
  Identify exact records without moving any data to the cloud

• Machine learning-based matching
  Detect records such as financial and healthcare statements without prior identification or fingerprinting

• File type control
  Detect hundreds of file types and block those specified in DLP policy

• Granular policy
  Target specific users, groups, locations, destinations, and content types with multi-criteria policies

• ICAP forwarding
  Send identified and blocked data over secure ICAP to existing DLP solutions for remediation

• Contextual reporting and auditor workflow
  Provide customized reports and notifications for visibility into DLP violations

• Logging in preferred geolocation
  Specify geolocations where logs are written to disk

• Real-time log feeds
  Stream real-time log events to an external SIEM for further insights

Investigate data loss incidents in real time
With visibility into each DLP violation, you can customize your notification workflow and reporting and instantly analyze and report on any compliance concern. Zscaler Nanolog™ Streaming Service (NSS) can also forward logs in real time to your third-party DLP solution via secure ICAP, or feed into your SIEM to integrate with your GRC workflows—buying you crucial time for analysis and remediation of data loss incidents.
Why Zscaler Cloud DLP

**Better data protection**
Get identical protection for all users and branches regardless of location.

**Complete visibility**
Illuminate blind spots by inspecting all your SSL traffic, without capacity limits or costly appliances.

**Elastic scale**
Always enforce your policies inline with consistent performance.

**Fully integrated platform**
Eliminate the need for architectural changes and maintenance of point products.

Zscaler purpose-built, multitenant cloud security platform

Secure internet and web gateway as a service
Zscaler delivers a completely integrated gateway that inspects all ports and protocols, even across SSL.

- Global Policy Engine
- Real-time Analytics
- ID Provider
- SIEM Logging
- Client Connector or PAC File
- GRE/IPsec
- Default route to internet
- Block the bad, protect the good

Just point your traffic to the Zscaler cloud. For offices, you can set up a tunnel from your edge router. For mobile, you can use Zscaler Client Connector (formerly Zscaler App) or a PAC file.

Close the gaps in your data protection strategy
As part of the integrated Zscaler Cloud Security Platform, you can easily activate Cloud DLP to expand data protection to all your users.

**Request a Demo**

About Zscaler
Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.