zscaler™

3 Essential Requirements for Flawless Data Protection

Want a better CASB and stronger DLP? You have to start with the right foundation.

Anyone who works in IT or network security will tell you—data protection used to be much easier when all of your data was in the data center and your employees were all working in the office. But times have definitely changed.

Now, your data has left the data center and is everywhere, spread across hundreds of cloud apps. And your employees are embracing remote work—off the corporate network and away from your security controls. As if that wasn't problematic enough, most internet traffic is encrypted and difficult to inspect, which is why bad actors hide their threats there. And your employees are using unsecured networks or unmanaged devices, which opens your data up to even more opportunities for exposure.

In this brave new world, organizations need a data protection platform that was built from the ground up for cloud and mobility, and it should include these essential requirements.

Need to know

Protecting your data with a CASB and DLP is only as good as the architecture it sits on. It's essential to understand the recipe for success.

Essential Requirement #1

Insist on a purpose-built SASE architecture

With cloud and mobility, security appliances can't be everywhere. When users drop off-network, you go blind and your users and data get exposed. Moreover, to deliver airtight cloud access security broker (CASB) capabilities and data loss protection (DLP), you need full SSL inspection. Appliances just can't deliver this due to hardware restraints.

A purpose-built SASE cloud platform is the first requirement you need to deliver high-performance, always-on secure connections, no matter the user location. SASE unifies all CASB, DLP, and security services into an globally distributed cloud platform so you get less complexity, better data protection, and a fast user experience.
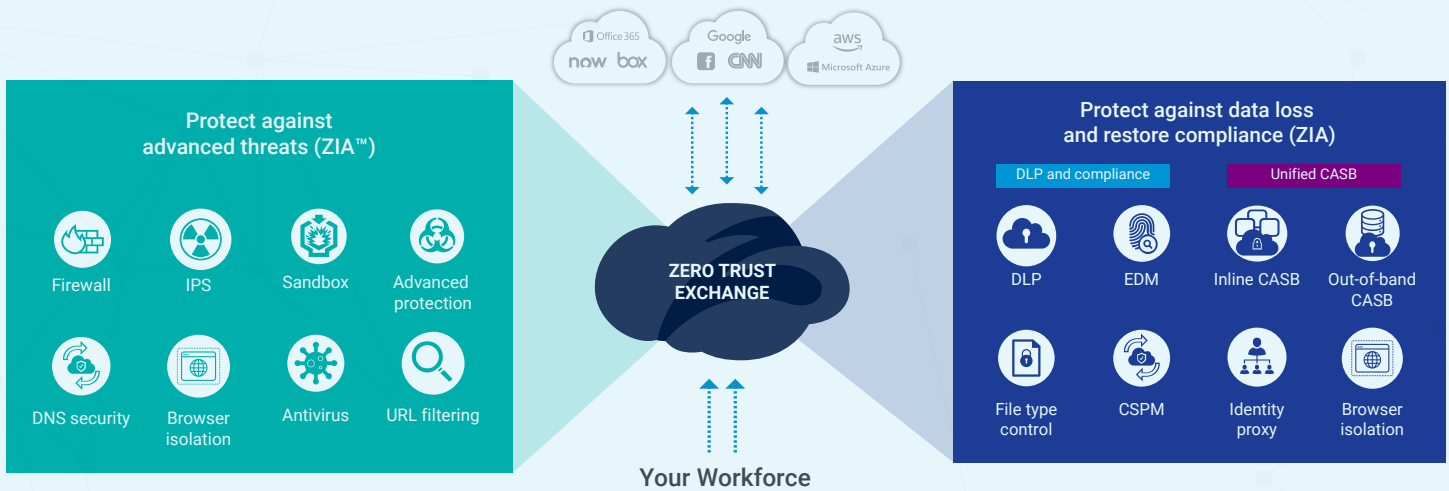
Need to know

Building an enterprise-grade, inline data protection architecture that scales across SSL is not easy. Only trust your traffic to a vendor with the most experience, a proven track record, and enterprise-grade SLAs.

The Zscaler™ Way

Protect against advanced threats (ZIA™)

Firewall · IPS · Sandbox · Advanced protection · DNS security · Browser isolation · Antivirus · URL filtering

ZERO TRUST EXCHANGE

Protect against data loss and restore compliance (ZIA)

DLP and compliance: DLP · EDM · File type control · CSPM

Unified CASB: Inline CASB · Out-of-band CASB · Identity proxy · Browser isolation

Your Workforce

Branch · HQ · Road Warrior

The Zscaler Zero Trust Exchange™ is a cloud-native proxy, built from the ground up for data protection and SSL inspection at scale across 150 data centers. Every user gets a fast, secure connection. And our unlimited SSL capacity means you can secure all your data across every user connection, on- or off-network.

As the market leader, Zscaler has been delivering inline inspection for more than a decade. Best of all, because DLP, CASB, and all other security services are integrated, you get simplified policy and a unified approach to data and threat protection.

Essential Requirement #2
Better data protection requires the best context

To properly classify the data you have, you need context, but it's the quality of context that helps you make the best, most informed decisions.

It was easy in the old days—users were accessing email from an Exchange server or you had just a few file servers. Everything you needed to make informed decisions was all there and easy to access.

Now, your data moves across hundreds of channels—from cloud apps to public clouds to file-sharing platforms. And all the context you need in those channels is hiding inside SSL encryption.

Need to know

Context is the lifeblood of your CASB and DLP. Look for a platform with the strongest classification engine that uncovers the most attributes in every single cloud transaction—on- or off-network, and inside SSL.

The Zscaler Way

When it comes to context, Zscaler is unmatched.

Our Zero Trust Exchange and our Client Connector app help you deliver always-on data protection across every connection on- or off-network. It also provides visibility into ALL of your SSL traffic, giving enterprises a treasure trove of context.

And, by leveraging Zscaler's industry and custom dictionaries and using advanced techniques, such as Exact Data Match (EDM) fingerprinting, you can quickly classify data across common industry formats (PCI, HIPAA) and custom definitions.

Context from a firewall or proxy	172.16.1.12 source IP	64.81.2.24 destination IP	TCP/443 destination port
	SSL protocol	HTTPS protocol	

Traditional inline approaches don't provide enough visibility into context.

Added context you get with full SSL decryption	JohnDoe user	prodmgmt group	HQ location
	upload app function	jumpshare application	PowerPoint file type
	file sharing URL category	"Confidential" content	

When you can decrypt all SSL without limits, you get the needed context to make better protection decisions.

Essential Requirement #3
Demand a unified platform that protects all channels

Protecting your data from leakage and exfiltration requires security to be everywhere your data is. If you can't control every channel, your data is vulnerable and exposed to potential threats.

Also, if you can't unify all CASB and DLP protections into one platform, you've made things way too complex. Without a single platform view, you end up with a disjointed policy, security gaps, and a greater propensity to make costly configuration mistakes.

Need to know

For all key data channels—in motion, at rest, endpoints, and cloud providers—a unified platform will dramatically improve your policy strength and simplify your workflows.

The Zscaler Way

Because all Zscaler cloud services are integrated into a purpose-built inline cloud architecture, all services work together in harmony to unify policy and streamline protection of your cloud data channels.

Data at rest
Control user and threat exposure in Microsoft 365 and SaaS

- DLP
- Threat prevention
- Historic data scans
- Sharing exposure

SaaS
Office 365
now box

Internet
Google
CNN

Public Cloud
aws
Microsoft Azure

Providers
Remediate misconfigurations in public cloud and SaaS (CSPM)

ZERO TRUST EXCHANGE

Identity

Pixels

Isolated browser

Edge compute in 150 DCs (SASE)
—Proven inline/SSL inspection—

Data in motion
Control unsanctioned and shadow apps, classify and control industry and custom data

- File type control
- Cloud app control
- Cloud DLP
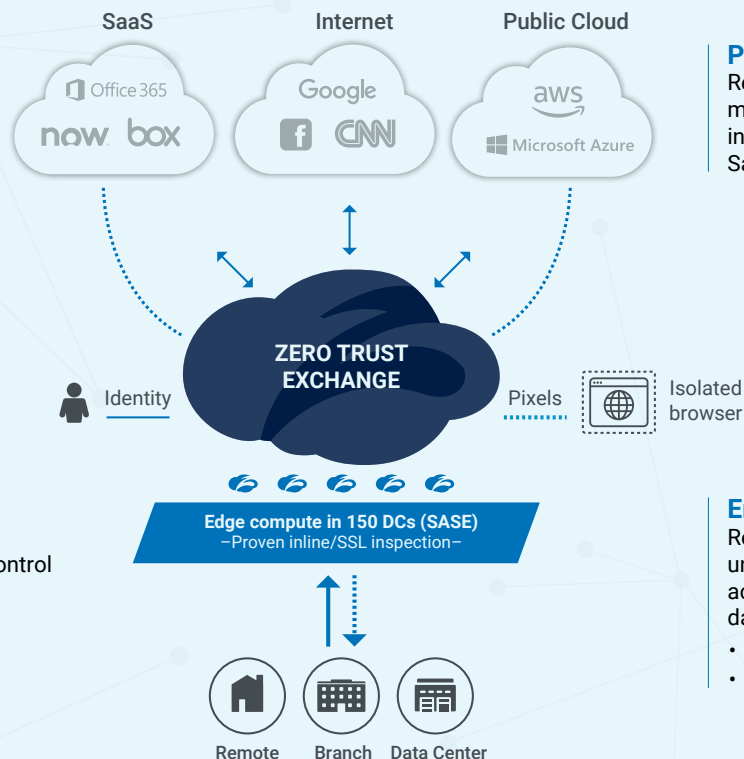- Exact data match
- Microsoft 365 inspection

Remote   Branch   Data Center

Endpoints
Restrict unmanaged/BYOD access and control data leakage

- Identity Proxy
- Browser isolation

Here's how it works:

Data in motion: Enterprise-grade inline inspection is essential for delivering real-time data protection. With Zscaler's purpose-built inline cloud, you can follow all users off-network, and inside SSL. Quickly classify and block critical data, no matter where it's headed, and lock down unsanctioned cloud apps.

Data at rest: As your users embrace their cloud apps, you must verify they are making the right decisions. With Zscaler out-of-band CASB, you can easily control improper sharing of files in Microsoft 365 apps, such as SharePoint and OneDrive, while also scanning files repositories for DLP and malware issues.

Endpoints: This channel is all about making sure the right people only have access to your data. With BYOD access control, you can do a quick SAML/SSO lookup and block unauthorized access to Microsoft 365 resources. Additionally, Zscaler Cloud Browser Isolation helps you prevent leakage onto unmanaged devices (BYOD) as it renders data on endpoints only as pixels. This means that a contractor can view and interact with data, but won't be able to save, download, or copy and paste the data. This ensures that nothing walks away on the device after the session.

Providers: The accidental misconfiguration of cloud applications is one of the most common causes of data exposure, costing companies time and money. Zscaler Cloud Security Posture Management (CSPM) automatically identifies and remediates application misconfigurations in SaaS, IaaS, and PaaS, so that your risk of data loss is reduced and you can maintain compliance.

Summary

The cloud and mobility have changed the way companies do business and the way employees work. Data is handled differently now, so it has to be protected differently. Security appliances no longer provide adequate protection for your data in today's world. You need a cloud-built security platform—with a SASE foundation—that protects your data wherever it is. You need Zscaler.

See our inline CASB/DLP in action
youtube.com/watch?v=R88TlNEMgGE

See our out-of-band CASB in action
youtube.com/watch?v=1KtoW-IXgMs

Contact us or book a personalized demo
zscaler.com/company/contact

About Zscaler

Zscaler accelerates digital transformation with its Zero Trust Exchange, a SASE-based platform that provides fast, secure connections between users, devices, and applications over any network.