THE PRIVACY-FIRST DIGITAL WORKPLACE FOR PUBLIC ADMINISTRATIONS

SECURITY & PRIVACY

FEATURES IN ZEXTRAS CARBONIO

ZEXTRAS®

Introduction

The importance of email privacy and security cannot be overstated, especially for institutions such as the government, financial and healthcare organizations, businesses, and individual users. With the ever-increasing threat of **viruses, spam, malware**, and **hackers**, it's crucial to maintain constant vigilance to safeguard data.

To address these issues effectively, Zextras Carbonio offers a comprehensive set of Privacy and Security features that **protect your valuable information** providing peace of mind for your organization.

Additionally, Zextras Carbonio's privacy and security features offer other benefits, including **compliance with legal and regulatory requirements, as well as directives issued by governmental agencies.**

TABLE OF CONTENTS

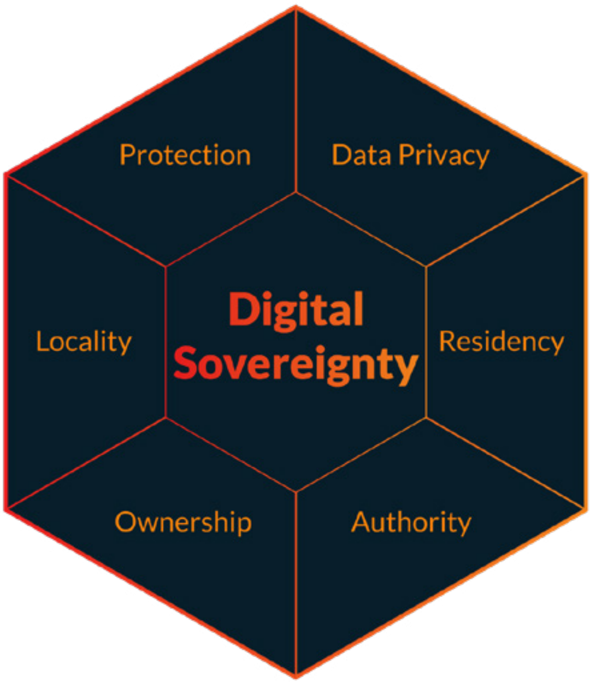
A Trusted Choice for Public Administrations Seeking Top-Level Security

It’s no surprise that so many people and public administrations trust Zextras Carbonio as their go-to choice for a secure digital workplace. With **over 500 public administrations** currently utilizing their services and **over 120 million users** around the globe, Zextras has proven its ability to provide a reliable and secure platform for the **Public sector and Telcos**.

Their commitment to data privacy and protection has made them a trusted partner for industries that require strict regulation, ensuring their confidential information stays safe and secure. As the **demand for secure digital workplaces continues to grow**, Zextras Carbonio remains at the forefront, providing innovative solutions to meet the evolving needs of organizations around the world. Let’s take a closer look at how Zextras achieved this esteemed reputation.

With over 500 public administrations currently utilizing their services and over 120 million users around the globe, Zextras has proven its ability to provide a reliable and secure platform for the Public sector.

The Digital Workplace designed for Digital Sovereignty



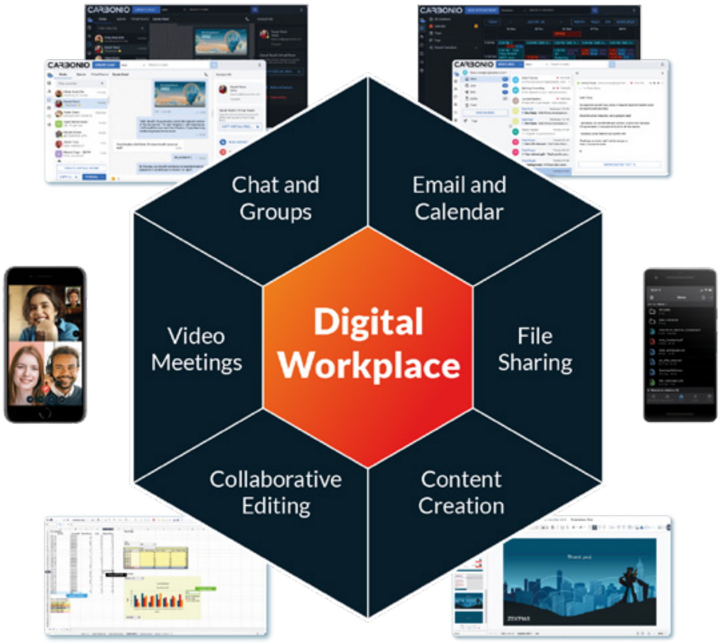
Digital sovereignty is the right of an organization to maintain control over its **digital data and infrastructure**, ensuring that it remains secure and private. It is considered to be far **vaster than data sovereignty,** encompassing not only data, but also the **infrastructure and its associated processes, services, and technologies**.

The concept of digital sovereignty has become increasingly critical in the age of digital transformation, as organizations strive for autonomy and control over their data in a highly interconnected world.

All of Zextras products and services were designed around **Security** (safeguarding the data). and **Privacy** (protecting the people data refers to).

Zextras Carbonio is an all-in-one **digital workplace** that unlocks **digital sovereignty** for organizations. All communication needs can be performed without ever switching context, in a private environment:

- **Email, contacts, calendar**
- **Chats, videomeetings**
- **Documents creation and co-editing**
- **File management and sharing**



Zextras Carbonio's Privacy and Security Features

We can categorize Carbonio's privacy and security features into five distinct groups:

a. Secure Deployment Options

- On-premises Deployment
- Private Cloud Deployment

b. Mobile Device Governance

- Data Encryption
- Dedicated Passwords
- Support for QR Codes
- ActiveSync ABQ Device Control
- ActiveSync DoS Filter

c. Government Mandates for Privacy and Security Solutions

d. Integrated Security Features

- Integrated Anti-virus and Antispam
- Two-factor Authentication (2FA)
- Carbonio Service Mesh
- Securing LDAP Password
- SPF, DKIM, and DMARC
- Protected Communication (TLS, HTTPS, WebRTC, etc)
- Integrated Real-time Blacklists (RBL) Checks

e. Integration with Third-Party Solutions

- SAML Integration
- Integration of Let's Encrypt Certificate Authority (CA)
- External LDAP/AD Integration
- External Anti-virus/ Antispam Engines

In short

a. Secure Deployment Options

Carbonio offers two deployment options, giving users the freedom to choose where their data resides for maximum privacy and security:

- **On-premises Deployment**
- **Private Cloud Deployment**

With an on-premises deployment, data remains within the organization’s data center, allowing users to retain full control and sovereignty over their information. Alternatively, Carbonio provides private cloud-based services, prioritizing privacy and implementing stringent security measures to protect data and prevent unauthorized access.

With this flexibility on where to store your data, Carbonio enhances the security of your data, granting you the freedom to select the storage option that best suits your organization’s unique security needs and safeguards your information effectively.

Additionally, Carbonio allows you to store computing resources, storage resources, and backup resources in separate locations, providing not only flexibility but also security.

b. Mobile Device Governance

In today's mobile-driven environment, safeguarding sensitive information and maintaining stringent data governance practices are of paramount importance.

Carbonio's robust mobile data policies grant you complete control over the data downloaded onto mobile devices. By ensuring that data remains inaccessible on unauthorized devices, the risk of potential data breaches stemming from lost or misused phones is effectively mitigated, guaranteeing the utmost protection for your organization through features including:

- **Data Encryption** on mobile devices
- **Dedicated Passwords** to set a unique password for authentication on mobile devices
- **Support for QR Codes** to eliminate the need for users to manually enter their credentials
- **ActiveSync ABQ Device Control** allows for granular access control - Allow/ Block/ Quarantine - of mobile devices connecting to the server
- **ActiveSync DoS Filter** for devices surpassing the predetermined connection rate

c. Obligatory Measures by Government Decree

Enhancing security and safeguarding privacy have emerged as imperative mandates for numerous government entities. Carbonio, a distinguished solution, exemplifies unwavering dedication to fortifying data protection measures. Irrespective of whether it is deployed in the private cloud or on-premises, Carbonio ensures that sensitive information remains securely within the confines of the respective state or province. This exclusive localization of data guarantees compliance with local data laws, shielding it from external governmental interference or access by external agencies.

d. Integrated Security Features

Integrating these essential features Carbonio digital workplace brings numerous benefits to both the organization and its users. One of the key benefits of integrating these solutions directly into Carbonio is that you can avoid relying on external tools or spending time configuring them to fit your digital workplace requirements. These solutions can be used straight out of the box, offering the assurance that they will function seamlessly with the rest of your system.

Integrating essential features into Carbonio brings numerous benefits to both the organization and its users. These features include:

- **Integrated Anti-virus and Antispam**
- **Two-factor Authentication (2FA)**
- **Carbonio Service Mesh**
- **Securing LDAP Password**
- **SPF, DKIM, and DMARC**
- **Protected Communication (TLS, HTTPS, WebRTC, etc)**
- **Integrated Real-time Blacklists (RBL) Checks**

e. Integration with Third-Party Security Solutions

Carbonio empowers seamless and secure collaboration, transcending boundaries of time and location, while offering inherent protection and seamless integration with leading third-party software providers. Elevating the security standards to unparalleled heights, Carbonio incorporates a multitude of cutting-edge features, including:

- **SAML Integration:** Support for single sign-on (SSO) solution SAML integration and trusted third-party pre-authentication
- **Integration of Let’s Encrypt Certificate Authority (CA):** Using standard ACME clients
- **External LDAP/AD Integration:** Support for external LDAP and active directory solutions
- **External Anti-virus/Antispam Engines:** Support for third-party antivirus and antispam solutions (AV/AS)

Secure Deployment Options: Private Cloud and On-Premises

In today's digital landscape, the issue of email privacy has emerged as a hot topic, fueling growing concerns among users regarding the **confidentiality** of their electronic messages. Recognizing the importance of safeguarding sensitive information, Carbonio offers a range of **flexible deployment options** to ensure the utmost privacy and security for your email communications.

With Carbonio, you have **the freedom to choose where your data resides**, providing you with peace of mind. Whether you opt for an on-premises deployment, where your data remains within your organization's data center or a private cloud-based service, Carbonio helps you protect your valuable data.

- For those who prefer to keep their data under their direct control, the **on-premises deployment** option allows you to retain **full sovereignty over your information**. Your confidential **emails, files, and communications** stay securely stored within your trusted infrastructure, ensuring that they never leave the confines of your organization.

- Alternatively, Carbonio offers **private cloud-based services** for those seeking the agility and scalability that the cloud provides. In these deployments, Carbonio prioritizes your privacy, implementing rigorous security measures to secure your data and prevent unauthorized access. You can enjoy the benefits of remote accessibility and seamless collaboration while maintaining the highest level of confidentiality.

When choosing Carbonio, you are placing your trust in a reputable and reliable partner dedicated to upholding the highest standards of security. Our team of professionals remains vigilant, continuously monitoring and updating our systems to address any potential vulnerabilities promptly.

Whether you are an organization looking to **protect sensitive client communications** or an individual concerned about the privacy of personal assets, Carbonio's secure deployment options cater to your unique requirements. Furthermore, Carbonio offers the flexibility and security you need by enabling you to securely **store your computing resources, storage resources, and backup resources in distinct locations**.

Whether you opt for an on-premises deployment, where your data remains within your organization's data center, or a private cloud-based service, Carbonio helps you protect your valuable data.

Mobile Device Governance

Zextras integrates the ActiveSync protocol into Carbonio, thereby achieving full compatibility with contemporary mobile devices. By leveraging ActiveSync, users are guaranteed an optimal mobile experience characterized by **rapid synchronization and native support** for push notifications, calendars, contacts, and emails while maintaining the **utmost security** on mobile devices.

To enhance security measures, Zextras introduces a specialized password for mobile users, granting access exclusively to the ActiveSync protocol while preventing access to other services such as Webmail, POP, IMAP, and SMTP.

Data Encryption

Data encryption plays a crucial role in enhancing the security of mobile apps in a digital workplace like Carbonio. Encryption provides a strong layer of **protection against data breaches, unauthorized access, and potential data leaks.** It safeguards sensitive information such as **user credentials, documents, and communication** exchanged within the digital workplace.

By encrypting data, information is transformed into a format that can only be accessed or deciphered with the appropriate encryption key. This ensures that even if unauthorized individuals gain access to the encrypted data, they won't be able to understand or utilize it.

By implementing data encryption in mobile apps, Carbonio can significantly enhance the security of the entire system and instill trust in its users regarding the confidentiality and integrity of their data.

Dedicated Passwords

The mobile password assures maximum security and avoids credentials theft: it is managed by a dedicated policy in order to avoid credentials change causing a locked account due to multiple failed login attempts.

The Mobile Password feature empowers users and administrators to establish an additional password exclusively dedicated to mobile apps for a given account. This feature offers several key advantages, including:

Enforcing secure “set-and-forget” passwords independently of any other password policies. Consequently, in the event of an account password change, there will be no need to modify the password saved on all mobile devices synchronized with the account.

Safeguarding against unauthorized access to the device or client by preventing the disclosure of the actual account password.

A dedicated password significantly reduces the risk of credential theft and unauthorized access by enabling users to access their mobile apps with a separate password, rather than relying on their primary account credentials.

Support for QR Codes

Support for QR code authentication in mobile app offers enhanced convenience and security for users. QR codes provide a quick and efficient way to authenticate users **without the need for manual input of usernames and passwords.** When logging in, users can scan a unique QR code displayed on the screen using their mobile devices, which automatically authenticates their identity.

The use of QR codes streamlines the login process, reducing the chances of errors during manual input and saving users’ time. It eliminates the need to remember or type in complex passwords, which can often be a source of frustration and security risks. With QR code authentication, users simply need to scan the code to gain access to the digital workplace.

Moreover, authentication on Carbonio mobile applications using QR codes eliminates the need to manually enter a username and password. This reduces the risk of keyloggers or phishing attacks that attempt to capture login credentials.

The use of QR codes streamlines the login process, reducing the chances of errors during manual input of users’ credentials.

ActiveSycn ABQ Device Control

The “Allow/Block/Quarantine” feature provides meticulous access control over mobile devices that connect to the server. Acting as a “pre-emptive” security measure, this feature takes effect upon the initial connection to the server, ensuring that only authorized devices can successfully complete synchronization. This capability empowers administrators to maintain comprehensive oversight of all mobile devices utilized within their network.

In Allow mode, all devices are permitted to connect, whereas, in Block mobile mode, the administrator specifies which devices are allowed to connect. Finally, in Quarantine mode, the device is directed to a simulated mailbox and must wait for authorization to proceed.

Acting as a “pre-emptive” security measure, this feature takes effect upon the initial connection to the server, ensuring that only authorized devices can successfully complete synchronization.

ActiveSync DoS Filter

Carbonio incorporates a dedicated ActiveSync Denial of Service (DoS) Filter component, which effectively enhances both security and stability. Whenever a device surpasses the predetermined connection rate within a specified timeframe, the filter will activate and “jail” the device, thereby rejecting any further connections from it.

This feature serves the dual purpose of fortifying security measures, safeguarding against Denial of Service attacks, and promoting system stability. By blocking clients that generate an excessive number of requests, whether due to bugs or malfunctions, valuable resources are conserved for all other clients, ensuring optimal performance.

This feature serves the dual purpose of fortifying security measures, safeguarding against Denial of Service attacks, and promoting system stability.

Obligatory Measures by Government Decree

Security and privacy have become **indispensable legal prerequisites** for numerous **government agencies.** Carbonio deployments are conducted within the jurisdiction, whether hosted in the private cloud or on-premises, guaranteeing the **confidentiality of data and preventing its transfer** beyond the boundaries of the respective state or province. As a result, the data is exclusively subject to local data protection regulations such as GDPR, CCPA, PIPEDA, and LGDP, ensuring that it remains inaccessible to external governments or agencies.

Compliance with such regulations holds immense significance in terms of both privacy and security. These regulations set stringent guidelines and requirements to safeguard personal data, ensuring that **individuals' privacy rights are respected and protected**. By adhering to these regulations, organizations demonstrate their commitment to maintaining the confidentiality, integrity, and availability of sensitive information.

Your data might be subject to local data protection regulations such as GDPR, CCPA, PIPEDA, and LGDP, ensuring that it remains inaccessible to external governments or agencies. Compliance with such regulations holds immense significance in terms of both privacy and security.

Non-compliance with these regulations can result in **severe consequences, including hefty fines and reputational damage**. Regulatory bodies have the authority to impose significant penalties on organizations that fail to meet their obligations. For instance, under GDPR, organizations can be fined up to €20 million or 4% of their global annual turnover, whichever is higher. Similarly, CCPA empowers consumers to seek damages ranging from $100 to $750 per individual, per incident, in case of non-compliance.

These substantial penalties serve as a deterrent, compelling organizations to prioritize privacy and security measures, adopt robust data protection practices, and implement comprehensive compliance frameworks. By doing so, organizations not only mitigate the risk of financial penalties but also **foster trust and confidence among their customers, partners, and stakeholders**, ultimately enhancing their reputation and competitive advantage in the market.

Integrated Security Features

Within the Carbonio digital workplace, the integration of these essential features brings a multitude of advantages for both your organization and its users. One key benefit is the avoidance of reliance on external tools or the need to invest time in configuring them to align with your specific digital workplace requirements. Instead, these solutions seamlessly blend into Carbonio without too much additional effort to set up. They are readily available and can be utilized straight out of the box, ensuring they seamlessly operate in harmony with your existing system. This streamlined approach saves valuable time, effort, and resources, guaranteeing optimal functionality and a hassle-free experience within your digital workplace while assuring security.

Integrated Anti-virus and Antispam Solutions

Anti-virus and anti-spam measures play a pivotal role in fortifying the security of a platform. In today's digital landscape, the proliferation of viruses and spam poses significant threats to the **confidentiality, integrity, and availability of sensitive information**. Malicious actors use viruses to exploit vulnerabilities, gain unauthorized access, and compromise systems, potentially leading to data breaches, unauthorized use of personal information, and financial losses. By integrating robust anti-virus software, a platform can proactively **detect, quarantine, and eliminate viruses,** preventing potential harm to users' devices and the platform as a whole. Similarly, anti-spam protection helps mitigate the risks associated with **unsolicited commercial email (spam) and malicious content**.

Anti-virus and anti-spam measures reduce the likelihood of users falling victim to phishing attempts, scams, or malware-laden attachments that can compromise sensitive data or lead to credential theft or even data breaches.

Carbonio comes with robust anti-virus protection through **ClamAV** and is equipped with dedicated spam filters using **SpamAssassin, Postscreen, and Cluebringer** integration.

ClamAV, renowned as the leading Open Source standard for antivirus software, serves as the primary virus protection engine integrated into each Carbonio server. By incorporating ClamAV, Carbonio ensures robust defense against malware and viruses, bolstering the overall security of the platform. Messages identified as carrying a virus are intelligently redirected from the inbox to a dedicated virus quarantine mailbox, preventing potential harm to users' systems. Additionally, to ensure the latest protection against emerging threats, ClamAV downloads the extended/commercial **virus signatures** and it **updates automatically every two hours** to reinforce Carbonio's proactive security measures.

Carbonio's ClamAV has the ability to utilize various commercial signature databases in addition to the default one, resulting in a significant improvement in efficiency. This is particularly crucial as these **supplementary signature databases** allow for the detection of more recent viruses and other malicious items.

Carbonio leverages the power of **SpamAssassin** to combat unsolicited commercial emails (spam) and emails containing malicious content. Using predefined - and customizable - regular expressions, user-defined white and black lists, and a self-trained Bayesian filter, SpamAssassin efficiently **identifies and filters out potentially harmful emails**, enhancing the security and integrity of users' email communications within the Carbonio environment. By effectively identifying and mitigating spam and malicious content, Carbonio's anti-spam protection ensures a safer and more reliable email experience for its users.

For additional protection against mail server overload and potential attacks, Carbonio offers the **option to activate the Postscreen and Cluebringer functions.** These act as an additional layer of defense, safeguarding the mail server from excessive loads and potential threats. By implementing Postscreen, Carbonio proactively enhances its security measures, fortifying the platform's resilience and stability in the face of potential email-related attacks or server overload scenarios.

Featuring:

- **ClamAV**
- **SpamAssassin**
- **Postscreen**
- **Cluebringer**

One of the notable aspects of the security features in this system is its admin & user-tuneable functionality.

This means that **both the global administrator and individual users** have the ability to **whitelist and blacklist** email addresses based on their preferences. This feature empowers users to have control over their own email security, allowing them to designate trusted senders and block potential threats. Additionally, custom rules determined by the administrator's confidence level can be set, enabling them to adjust the message score and establish specific criteria for categorizing emails. This versatility ensures that the **security measures can be tailored** to meet the unique needs and preferences of both the organization and its users.

Support for Two-Factor Authentication

2-factor authentication (2FA) is a robust security measure that can significantly enhance the overall security of Carbonio. By implementing 2FA, Carbonio adds **an additional layer of protection to user accounts beyond just a username and password.** This method requires users to provide a second form of authentication, typically through a unique code generated by an authentication app. This extra step acts as a **strong deterrent against unauthorized access**, even if passwords are compromised.

With 2FA, the risk of unauthorized account access due to weak or stolen passwords is mitigated, providing an extra safeguard for sensitive data and resources within the Carbonio platform. This added level of security instills confidence in users, protecting their digital workplace activities and reinforcing the overall security posture of Carbonio.

Furthermore, Carbonio 2FA intelligently avoids inconveniencing users with a second authentication factor while they are connected to the Office LAN or using well-known and trusted IPs unless these specific configurations are enforced by the administrator.

With 2FA, the risk of unauthorized account access due to weak or stolen passwords is mitigated, providing an extra safeguard for sensitive data and resources within the Carbonio platform.

Within Carbonio, this supplementary security layer is implemented through the use of a **One-Time Password (OTP)**, conveniently presented as a **QR code** to be easily used by Carbonio mobile applications.

Carbonio Service Mesh

It is worth noting that Carbonio's state-of-the-art technology not only offers exceptional functionality but also guarantees **absolute security in communications between services and servers** through the utilization of a well-established service mesh. This feature is particularly essential in the context of a **multiserver environment** where the physical separation of servers may pose a challenge.

Carbonio Mesh is an innovative solution that facilitates service discovery and service mesh. The mesh is a distributed liquid network that provides secure and ACL-based connections. This innovative technology allows the system to establish **secure channels between services**, instead of relying on IP-based connections between individual nodes.

This mechanism guarantees the secure communication of registered applications and implements access control to both on-premises and external resources with a single solution. In addition, Carbonio Mesh manages SSL encryption certificates to ensure the highest level of security.

This technology also enables Carbonio to add **health checking and fault detection** capabilities, as well as **dynamic and secure routing** between its components, excluding faulty instances. Furthermore, Carbonio Mesh acts as an application-level firewall, allowing only the exchange of necessary information for the proper functioning of Carbonio.

The mesh is a distributed liquid network that provides secure and ACL-based connections. This innovative technology allows the system to establish secure channels between services, instead of relying on IP-based connections between individual nodes.

Securing LDAP Passwords

One of the main features of Carbonio LDAP is **user authentication using an internal authentication mechanism**. It is in LDAP that user password hashes are stored, which are verified when users try to log into Carbonio.

Securing LDAP passwords is of utmost importance as it directly impacts the protection of highly sensitive and confidential data. Carbonio prioritizes security and understands the criticality of safeguarding user passwords. To ensure robust security measures, Carbonio has implemented the **SHA-512 algorithm as the default encryption standard for password storage.**

The SHA-512 algorithm is widely recognized and respected in the industry for its strong cryptographic properties. It offers a high level of security, making it exceptionally difficult for unauthorized individuals to retrieve or decipher passwords. This encryption standard is regarded as **virtually impregnable**, as there are currently no known vulnerabilities or weaknesses that pose a significant challenge to systems utilizing SHA-512.

However, we acknowledge that certain institutions and organizations may have even more stringent security requirements or face unique threat landscapes. In recognition of this, Carbonio provides **support for the advanced Argon2 algorithm for password storage.**

The Argon2 algorithm excels in handling key derivation gradually over time, ensuring steady and reliable protection against password attacks. It incorporates memory-hardness capabilities, which significantly **enhance resistance to various types of attacks**, including those that exploit parallel processing or specialized hardware. By utilizing the Argon2 algorithm, Carbonio effectively reduces the risk exposure associated with password storage, bolstering the overall security posture of our platform.

Featuring Algorithms

- **SHA-512**
- **Argon2**

DKIM, SPF, and DMARC Authentication Methods

DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) are **three crucial authentication methods** that play a vital role in maintaining the security of an email system.

Featuring

- **DKIM**
- **SPF**
- **DMARC**

DKIM adds a digital signature to outgoing emails, allowing the recipient's server to verify the message's authenticity and integrity.

SPF enables domain owners to specify which servers are authorized to send emails on their behalf, preventing unauthorized sources from spoofing their domain.

DMARC builds upon DKIM and SPF by providing a comprehensive policy framework that specifies how email servers should handle messages that fail authentication checks.

Carbonio supports SPF IP validation and DKIM authenticated signature control for incoming and applying DKIM signatures for outgoing emails out of the box.

By implementing **DKIM, SPF, and DMARC**, organizations can significantly reduce the risk of email fraud, phishing attacks, and unauthorized use of their domain, thereby safeguarding their reputation and ensuring that legitimate emails reach their intended recipients while **fraudulent or malicious emails** are detected and properly handled.

Implementing DKIM, SPF, and DMARC authentication methods on Carbonio email servers is a straightforward process that enhances the security and trustworthiness of the email system.

By implementing DKIM, SPF, and DMARC, organizations can significantly reduce the risk of email fraud, phishing attacks, and unauthorized use of their domain.

Protected Communication

Security is of utmost importance for **chat systems and video meetings**, especially for businesses and organizations. Unlike many other communication solutions, which have gained notoriety due to security breaches and privacy concerns, it is crucial for users to feel safe and secure while using these platforms. These breaches can lead to sensitive data being compromised, resulting in a **damaged reputation and financial losses for the organization.**

When an organization's communication channels are not secure, it can lead to several negative consequences. For instance, if employees share sensitive information over unsecured chat systems or video meetings, such as financial data or personally identifiable information (PII), they risk exposing that private content to unauthorized third parties.

Breaches can lead to sensitive data being compromised, resulting in a damaged reputation and financial losses for the organization.

Consequently, the company could experience reputational damage when clients and customers lose faith in their ability to handle confidential matters effectively - this is frequently associated with **large-scale cyber-attacks** aimed specifically at a particular firm which makes crises more severe than just one employee mistakenly leaking some valued files without any malignant intent.

Additionally, **businesses may incur significant legal expenses due to privacy violations** leading toward **hefty fines imposed by regulators** alongside fees for harm compensation for those whose PII was exposed since employers have obligations about protecting these customer's details while maintaining them confidentially safe per pertinent regulatory regimes. These outcomes stress why communicating safely within organizations must be part of regular security practices.

Featuring Security Protocols

- **TLS**
- **HTTPS**
- **WebRTC**

Carbonio values users' security profoundly; this digital workplace deploys several tools to secure communications such as **TLS,** which encrypts data transmission between the server and client, guaranteeing that the data cannot be tampered with or intercepted by anyone else.
Carbonio also employs **HTTPS**; this secure protocol limits unauthorized access to website data adding an extra layer of protection.

Finally, thanks to **WebRTC** -a trustworthy protocol for real-time communication - that allows users to communicate without any server intermediation. All these measures combined make Carbonio a very secure platform for chat and video meetings, giving users peace of mind when using the platform.

Integrated Real-time Blacklists (RBL) Checks

RBL checks, also known as Real-time Blacklists Checks, play a crucial role in enhancing the security of Carbonio email servers. These checks act as a protective layer by preventing **potentially harmful emails** from reaching the users' inboxes.

RBLs are **databases** that contain lists of **IP addresses or domains** that have been identified as sources of **spam or other malicious activities.** When an email server receives a new email, it can perform an RBL check to compare the sender's IP address against these lists. If a match is found, the email is flagged as questionable or rejected altogether.

Implementing RBL checks on Carbonio helps with security in several ways:

Reduced spam: RBL checks effectively filter out spam emails originating from known spam sources. By utilizing trusted RBL databases, Carbonio can automatically reject or tag emails from these sources, reducing the amount of unwanted spam cluttering users' inboxes.

Preventing phishing attempts: RBL checks can help identify IP addresses and domains associated with phishing attacks. Phishing emails often impersonate legitimate entities and **attempt to deceive users into revealing sensitive information.** By blocking or flagging emails from these known phishing sources, Carbonio protects users from falling victim to such scams.

Blocking malware distribution: RBL checks can also play a crucial role in blocking emails that are known to distribute malware or viruses. Malicious actors often use compromised IP addresses or domains to distribute harmful attachments or links. By comparing incoming emails against RBL databases, Carbonio can identify and block emails from these sources, ensuring that users are protected from inadvertently downloading malicious content.

Enhanced reputation protection: Carbonio can proactively monitor and protect the reputation of its email server by implementing RBL checks. If an email server becomes a source of spam or malicious activities, its IP address or domain can get listed on RBL databases. Regular RBL checks **help identify if the server's IP address has been blacklisted,** allowing administrators to take appropriate actions to remediate the issue and improve the server's reputation.

Quick response to emerging threats: RBL databases are continuously updated with new sources of spam, phishing, and malware distribution. By regularly checking emails against these **updated lists**, Carbonio can quickly identify and block emerging threats. This proactive approach helps to ensure that users are protected from the latest techniques and tactics used by cybercriminals.

RBLs are databases that contain lists of IP addresses or domains that have been identified as sources of spam or other malicious activities. When an email server receives a new email, if a match is found, the email is flagged as questionable or rejected altogether.

Integration with Third-Party Security Solutions

Carbonio offers inherent protection and seamless integration with leading third-party software providers, making it a highly versatile tool for businesses of all sizes. What truly sets Carbonio apart from other collaboration tools is its **unparalleled security standards**.

Let's delve deeper into these third-party solutions and explore how they assist Carbonio in achieving this high level of security.

SAML Integration

SAML (Security Assertion Markup Language) is a widely adopted XML-based open standard that facilitates the exchange of authentication information. It enables secure web-based authentication and authorization scenarios, including the convenience of **cross-domain Single Sign-On (SSO)**, allowing users to access multiple applications with a single set of credentials.

The incorporation of SAML authentication within Carbonio significantly enhances the security of the platform. By leveraging the SAML standard, Carbonio ensures a robust and reliable exchange of authentication information, promoting secure web-based authentication and authorization scenarios **without requiring users to enter their credentials**. This reduces the risk of compromising and exposing credentials, ensuring a more secure experience for users.

Reducing the risk of compromising and exposing credentials, ensuring a more secure experience for users.

Generally, SAML implementation relies on an external Identity Provider (IdP), which users identify themselves. The IdP then passes the authorization credentials to the Service Provider (SP). SAML authentication involves the verification of user identity and credentials. Carbonio simplifies SAML configuration by allowing administrators to import SAML metadata from the IdP, reducing the need for extensive manual setup. **It supports both SP and IdP SAML authentication, allowing different domains to have distinct SAML endpoints.**

Key components of SAML authentication include the Service Provider (SP), responsible for delivering the service, and the Identity Provider (IdP), responsible for providing user identities. During the authentication process, a SAML Request is generated by the SP to initiate the authentication, and a SAML Response is generated by the IdP containing the assertion of the authenticated user.

Furthermore, the Assertion Consumer Service (ACS) endpoint serves as the destination for SSO tokens, adhering to partner requirements.

Advanced Features

- **Identity provider-initiated authentication**
- **Service provider-initiated authentication**
- **Distinct SAML endpoints for each domain**

Integration of Let’s Encrypt Certificate Authority (CA)

An SSL/TLS certificate is a crucial security component. It provides a critical layer of encryption and authentication, ensuring secure communication between clients and servers. Carbonio provides a hassle-free integration solution that caters to your needs, including the request and automatic renewal (set-and-forget) of free and open-source Certificate Authorities (CA) like **Let’s Encrypt** or any other certificates that adhere to the **standard ACME protocol**. This can be easily achieved through the use of the **Admin Panel**, a user-friendly graphical interface designed to manage Carbonio servers.

Featuring

- **Commercial Certificate Authorities**
- **Nonprofit Certificate Authorities such as Let’s Encrypt**
- **Easy implementation via the Admin Panel**

A single server SSL/TLS certificate is specifically issued for a particular domain or subdomain, validating its authenticity and enabling secure connections for that specific entity. It verifies the ownership and identity of the server, encrypts data transmitted over the network, and establishes trust with users. On the other hand, a wildcard SSL/TLS certificate offers expanded coverage by securing **multiple subdomains under a single domain**. This flexibility simplifies certificate management and provides **cost and time savings** compared to obtaining individual certificates for each subdomain. With a wildcard certificate, organizations can secure various subdomains while maintaining the benefits of strong encryption, authentication, and trust.

Whether utilizing a single server SSL/TLS certificate or a wildcard certificate, the adoption of SSL/TLS technology elevates the security of data transmission, protects sensitive information, and instills confidence in users by establishing a secure and trusted connection.

The significance of **SSL/TLS certificates** for the security of platforms like Carbonio cannot be overstated. As **digital workplaces** become increasingly interconnected and handle sensitive information, the implementation of SSL/TLS certificates becomes paramount.

These certificates establish encrypted channels, ensuring that data transmitted between users and the platform remains confidential and **protected from interception or unauthorized access**. By validating the authenticity of the server and encrypting data in transit, SSL/TLS certificates safeguard against potential threats such as **man-in-the-middle attacks, data tampering, and eavesdropping.** Furthermore, SSL/TLS certificates inspire trust and confidence among users, assuring them that their interactions with the platform are secure. Given the critical nature of secure communication and the potential risks associated with unencrypted connections, SSL/TLS certificates are essential for bolstering the overall security posture of platforms like Carbonio, protecting user data, and maintaining the integrity of the digital workspace environment.

External LDAP/AD Integration

With Carbonio, you have the flexibility to integrate external Active Directory (AD) or LDAP solutions for **seamless identity management**. This integration allows users to utilize the same credentials across multiple services, enabling for example, single sign-on (SSO) functionality. By leveraging an external Identity Provider (IdP) like Active Directory (AD) or OpenLDAP, you can **avoid the need to duplicate or store passwords within Carbonio**.

This enhances security and reduces the risk of password-related vulnerabilities. Furthermore, **integrating an external IdP enables the convenient auto-provisioning of users**. This means that user accounts can be automatically created and synchronized **from the remote system**, eliminating the manual effort required to provision accounts individually. These advantages of Carbonio's support for external AD or LDAP integration ensure enhanced security, streamlined user experience, and efficient management of user accounts across various services.

Advantages:

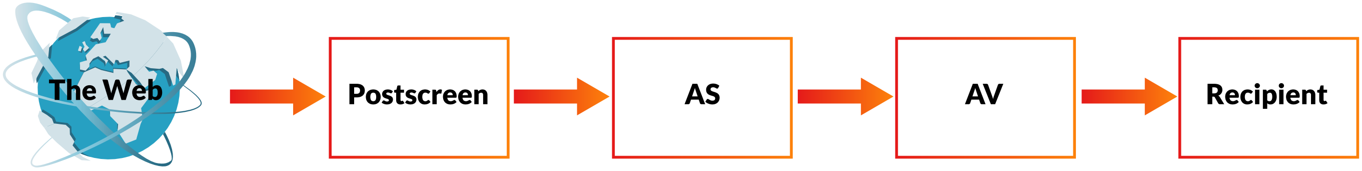
- **Utilize a single set of credentials across all services for seamless Single Sign-On (SSO) experience;**
- **Avoid duplicating and storing passwords to enhance security;**
- **Enable "auto-provisioning" of users to streamline the account creation process and eliminate the need for manual provisioning from the remote system.**

External Anti-virus/Antispam Engines

We acknowledge the importance of entrusting external providers for anti-virus (AV) and antispam (AS) services, and therefore, we provide the flexibility to seamlessly integrate external solutions for such purposes.

While Carbonio's built-in antivirus is highly effective, it can be easily turned off by organizations who need to use a **specific external antivirus** engine due to organizational requirements or personal trust. By disabling the built-in antivirus, you can ensure that the external antivirus program works effectively without any conflicts or interference.

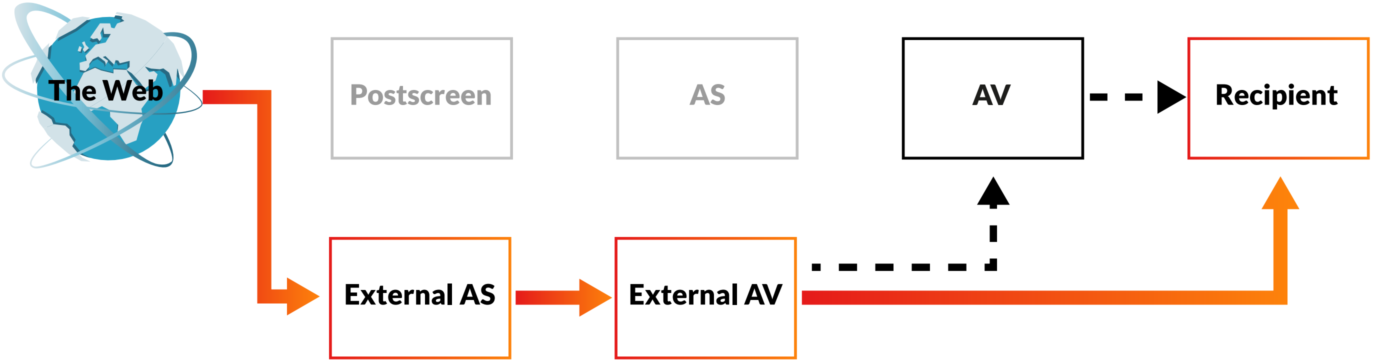
To gain a better understanding of these scenarios, it is necessary to first comprehend the hierarchy of AV/ AS components in Carbonio:



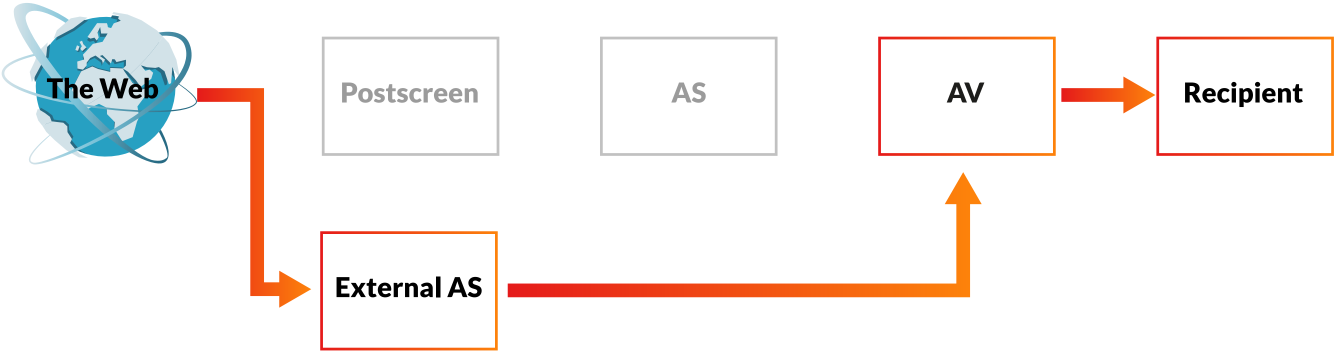
The Web → Postscreen → AS → AV → Recipient

There are essentially **two possible scenarios to integrate external anti-virus** solutions, which are outlined below.

1 Use an external antispam and anti-virus and directly go to the recipient (alternatively, you may use the integrated anti-virus on Carbonio in addition to the external anti-virus service)



2 Use an external antispam and directly go to the integrated anti-virus in Carbonio



Carbonio Approach to Security

With the surge of mobile and cloud computing, prioritizing security over user experience is no longer acceptable. The traditional methods of business communication have shifted **from personal computers to mobile devices**. Consequently, organizations must modernize their outdated messaging and collaboration systems to effectively **adapt to evolving threats and technologies**.

Carbonio, serving as a **messaging and collaboration platform**, plays a pivotal role in business communication and serves as a **vital component of the organization's information infrastructure**. As every organization is unique, the importance of flexible and adaptable software cannot be overstated when it comes to the success of information security and technology initiatives.

Open Core Design

Carbonio's back-end code is available as open source, which guarantees responsibility and openness.

Carbonio adheres to a thoroughly documented development procedure as change logs documentation on GitHub repositories. The community is welcome to participate by signing a contributor license agreement. The Carbonio open-core design has numerous advantages. With its efficient and optimized design, it even outperforms its proprietary counterparts in most areas. Additionally, it utilizes the **Linux platform as its foundation, offering scalability and manageability**. This, in turn, enables a wide range of implementation scenarios in your data center. Moreover, open-source communities provide a continuous cycle of **feedback and improvement**, ensuring that software quality and security stay optimized over time.

Open Standards Philosophy

Carbonio incorporates industry-standard technologies that are widely accepted and adopted, including:

IMAP/POP
(Internet Messaging Access Protocol/Post Office Protocol)

ICS
(Internet Calendar Scheduling)

LMTP
(Local Mail Transfer Protocol)

LDAP
(Lightweight Directory Access Protocol)

SSL/TLS
(Secure Sockets Layer/Transport Layer Security)

SMTP
(Simple Mail Transfer Protocol)

SAML 2.0
(Security Assertion Markup Language)

Embracing well-established standards not only improves **compatibility across diverse platforms** such as mobile, desktop, and cloud environments but also enables partners to interact seamlessly with a **unified set of APIs**. Moreover, this commitment to open standards empowers experienced users to exercise their creativity by developing personalized security and privacy tools or effortlessly integrating third-party solutions.

Open Architecture

Carbonio adopts a **modular architecture**, enabling organizations to deploy the software in a flexible and secure manner, seamlessly fitting it into their specific information infrastructure. Moreover, this modular platform empowers organizations to **leverage their existing infrastructure components**, **minimizing the requirement for extensive replacements**. This ultimately leads to a more secure environment for organizations, ensuring a **smooth integration** process and minimizing potential vulnerabilities.

Features - Acronyms

2FA	Two-factor Authentication
ABQ	Allow, Block, Quarantine
AD	Active Directory
AS	Antispam
AV	Antivirus
CA	Certificate Authority
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DoS	Denyal of Service
HTTPS	Hypertext Transfer Protocol Secure
IdP	Identity Provider
IMAP	Internet Messaging Access Protocol
LDAP	Lightweight Directory Access Protocol
POP	Point of Presence
QRcodes	Quick Response Codes
RBL	Real-time Blacklists
SAML	Security Assertion Markup Language
SMTP	Simple Mail Transfer Protocol
SP	Service Provider
SPF	Sender Policy Framework
SSL	Secure Socket Layer
SSO	Single Sign On
TLS	Transport Layer Security
WebRTC	Web Real-Time Communications

ZEXTRAS®

Want to know more?

Visit zextras.com