EIDOSMEDIA

Eidtorial Platform Security

INTEGRITY AND CONTINUITY IN THE EDITORIAL ENVIRONMENT

March 2021

EidosMedia S.p.A.
Via C. Imbonati 18
20159 Milano, Italy

Tel. +39 02 36732000
Fax +39 02 36732999
info@eidosmedia.com
http://www.eidosmedia.com

Contents

EIDOSMEDIA

Securing the distributed operation

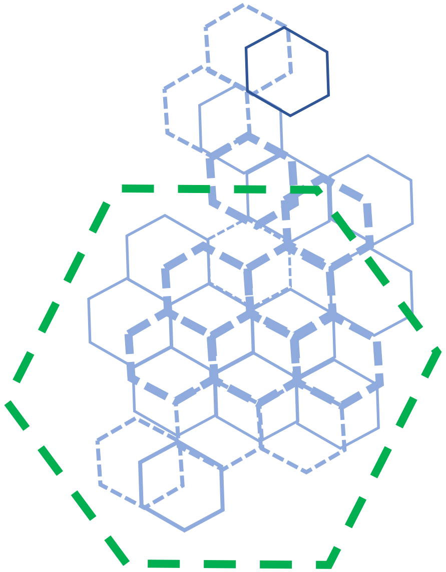
Editorial operations requiring collaboration and asset sharing between users are prime targets for malicious attacks and data breaches. The recent public health crisis, in forcing entire newsrooms and offices to move into remote working mode, has further contributed to the vulnerabilities of these operations.

Points of weakness

Much of this vulnerability derives from the attempt to use standard desktop software to provide distributed editorial functionality. The recent high-profile security breaches in Europe and in North America have revealed the weaknesses of conventional desktop applications and the difficulty of securing them adequately.

Demanding environments

Eidosmedia editorial platforms have always been mission-critical resources for customers in the news-media and financial sectors and this has resulted in products with particular resilience and continuity characteristics.



This ebook looks at the way Eidosmedia solutions are able to safeguard the integrity and continuity of their users' operations, both through specific security features, as well as through their intrinsic architecture and design.

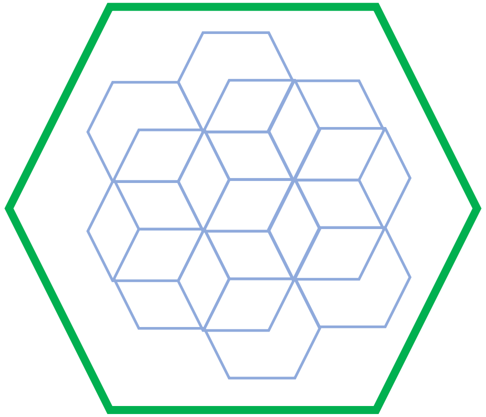
Security - active and intrinsic

In thinking about the resilience of information systems, it's useful to make a distinction between two sources of security:

> **Active security** is that provided by the tools and policies adopted to prevent unauthorized access to the system: authentication procedures, user permissions, encryption, firewalls etc.
>
> **Intrinsic security** is the resistance to attack that comes from the way the system is built and the absence of weak spots or vulnerable elements.

In-built resilience

In the case of Eidosmedia platforms, their intrinsic security comes from the unified platform architecture, the elimination of email as a collaborative channel and, in the case of cloud deployments, the possibility of moving beyond local desktop software with its multiple vulnerabilities.



Taken together, these sources of security place Eidosmedia solutions well in advance of solutions based on confederations of standard desktop applications.

Active security- ASL

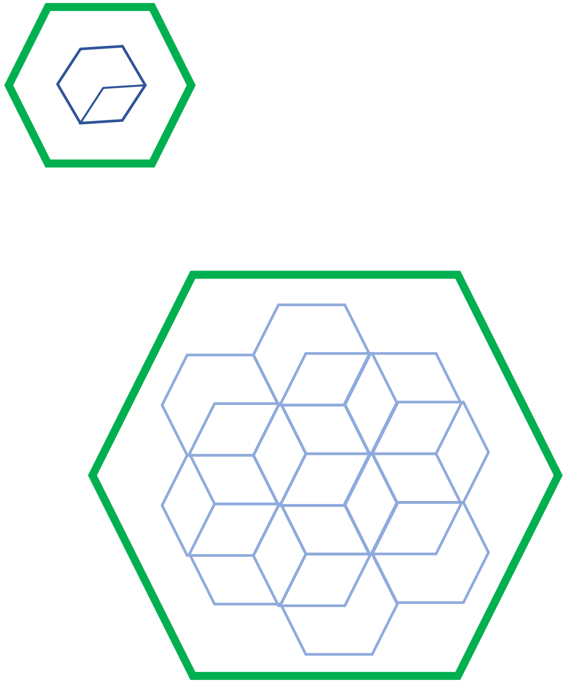
The Advanced Security Layer (ASL) is an optional set of security enhancements that provides additional protection for Eidosmedia platforms.

ASL incorporates a number of best practices in access control from multi-factor authentication and single sign-on to internal password encryption.

Controlling access

Multi-factor authentication (MFA) prevents unauthorized access through passwords obtained by processes such as cracking or keylogging.

Single sign-on (SSO) improves the usability of the security procedures by requiring the user to authenticate only once, after which they may access all of the resources permitted to their user profile.



Multi-factor authentication

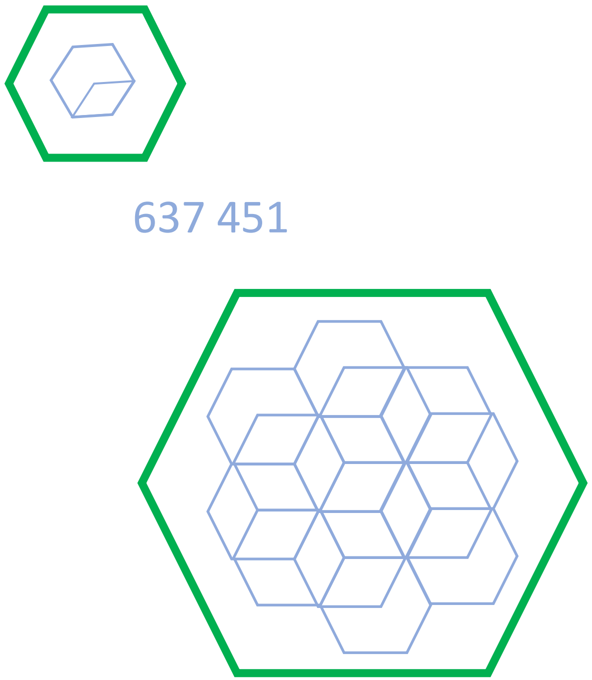
Multi-factor authentication (MFA) overcomes the shortcomings of conventional, static, password-based systems.

MFA requires the user to prove their identity by providing two or more separate pieces of evidence.

Beyond the passive password

In addition to a password or pass-code, the user may be asked to provide a one-time password generated by a small portable device. Alternatively, the one-time password may be generated by a smartphone app such as Google Authenticator using a shared secret key.

By requiring something that only the user possesses in addition to the password, MFA prevents unauthorized access if password security has been compromised through hacking or fraudulent approaches such as phishing.



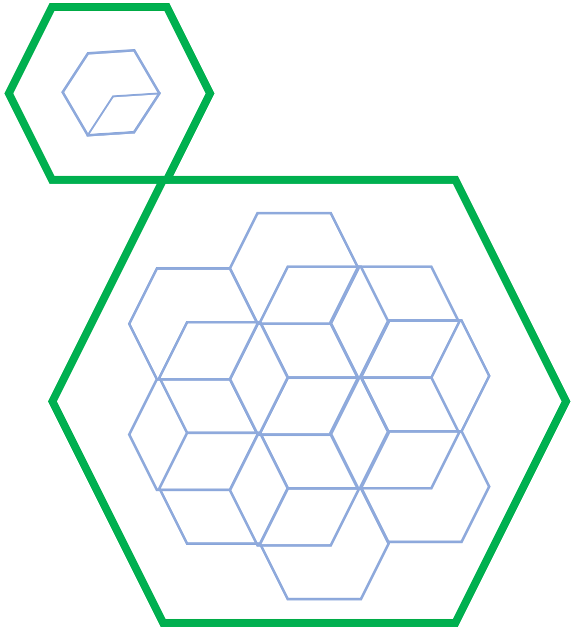
Single sign-on

Single sign-on compensates for the more complex MFA procedures by giving the user access to all permitted services and applications during the session through a single authentication procedure.

This centralized point of access is easier to administrate and update securely than multiple access points distributed throughout the environment.

SAML 2.0 support

It also provides support for Security Assertion Markup Language 2.0 (SAML 2.0), a common standard for exchanging authentication and authorization data. This allows full integration with commercial implementations of SAML, such as Okta.



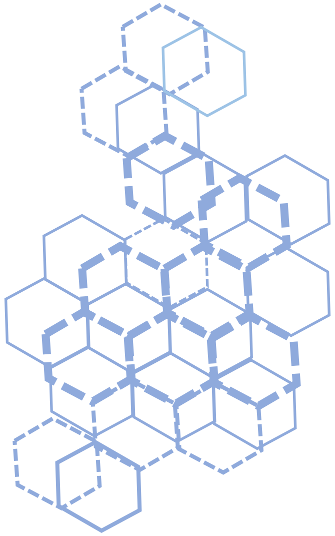
The loose federation

The introduction of active security features, however, is of little value if the operation makes use of software components that remain intrinsically vulnerable.

To provide the functionalities their distributed workforce needs, organizations increasingly find themselves forced to adopt a loose federation of platforms and apps.

Such federations typically consist of:

- desktop text and graphics applications
- a shared repository
- chat applications - often on a BYO device
- an email client
- a publishing solution.



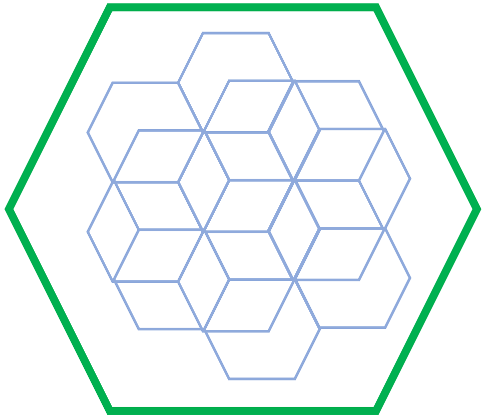
Any one of these applications, together with the collection of plug-ins and extensions that typically accompanies them, is a potential point of entry - especially email and messaging applications.

Intrinsic security and the Unified Platform

Intrinsic security

Intrinsic security is the resistance to attack that a system has by virtue of its basic architecture and design.

As unified platforms, Eidosmedia solutions are easier to secure than a collection of separate applications.



Integrated development

This resilience comes from an integrated approach to product development, ensuring that each platform component complies with the global security standards of the platform as a whole.

Integrated communications

At the same time, the availability of a complete range of collaborative functions within the workspace allows users to work together effectively - even at different locations - without recourse to external messaging applications.

Beyond email

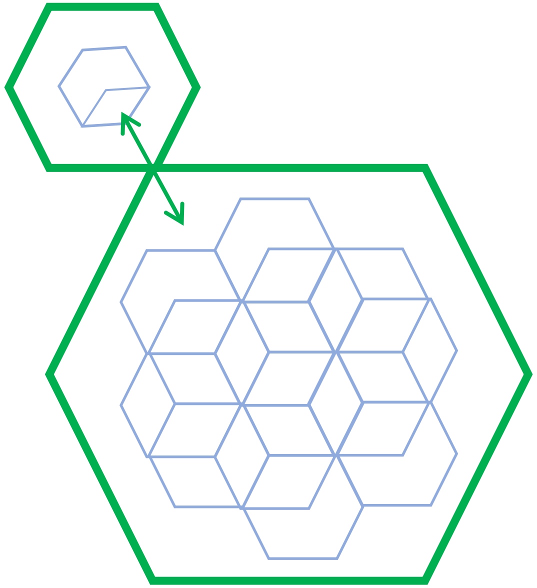
Email is usually the most vulnerable part of any organization’s IT environment - each user account is a potential source of data breaches or malicous entry.

Watertight collaboration

Eidosmedia users have no need of email or other external applications because they have a rich set of communications channels available within their workspace:

- **Notifications** inform users automatically as soon as something requires their action or attention.
- **In-platform messaging** replaces emailing**.**
- **Task-based planning** and **in-story chatboxes** speed collaboration within a totally secure environment - even across multiple geographies.

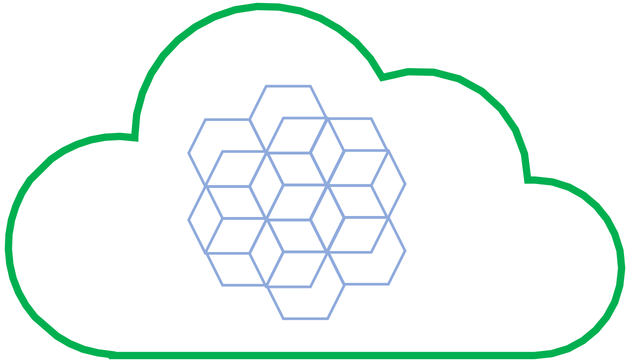
All communications channels work across all workspaces from desktop to mobile devices.



Cloud deployment

Security in the cloud

As well as freeing users from many of the constraints involved in housing and maintaining physical infrastructure, cloud deployment also improves the intrinsic security of the solution.



Safer than local

Cloud hosted solutions enjoy a level of protection and continuity which would be difficult and costly to achieve in a local installation. All user data is held in encrypted format. Only Eidosmedia and the customer hold the encryption keys.

Towards zero footprint

Moving server installation to the cloud is also the first step in creating a ‘zero footprint’ solution in which all local software installation, with its attendant vulnerabilities, is eliminated.

Eliminating the PC

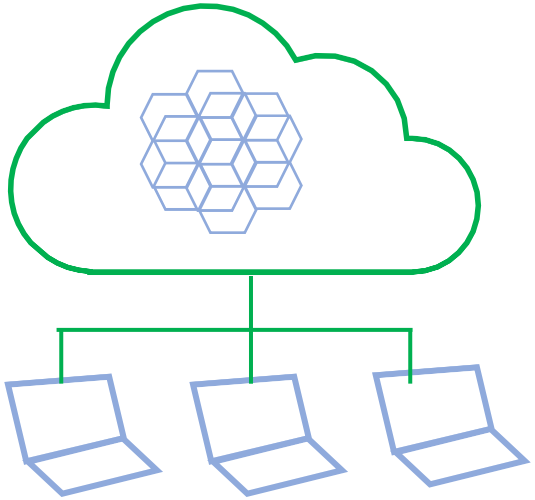
The user PC in a local installation is the source of a number of system risks, ranging from poorly secured desktop software to email and messaging applications.

Eidosmedia's *Swing* remote working applications offer a secure alternative to the Windows client. They provide a complete range of authoring and coordinating functions over a fully encrypted network connection.

Used together with a cloud-hosted server installation, *Swing* mobile apps eliminate the need for all local software installation.

Swing in the office

As well as its strengths as a mobile workspace, *Swing* is also a viable on-premise alternative to Windows desktop installations. Its ease of management and intrinsically secure architecture allow it to handle all but the most layout-intensive editorial tasks.



Virtual desktops

As an alternative to remote working applications, users with cloud-hosted platforms can use the ‘virtual desktops’ offered by cloud providers such as AWS and MS Azure.

PC applications can be installed on these desktops, providing similar functionality to locally installed software, without its vulnerabilities.

Eidosmedia cloud partners offer two such solutions:

- **Amazon AppStream,** allowing applications such as *Prime* to be accessed through high-performance data connections.
- **Microsoft Azure Windows Virtual Desktop**, a similar service that offers access to a Windows desktop, together with virtualized MS Office applications.

Eidosmedia’s *Prime* client is fully deployable using these services.

Disaster recovery in the cloud

Cloud hosting has several benefits when it comes to enhancing the security of a solution. It can also, should the unthinkable happen, provide a means of rapidly recovering lost data and functionality following an attack.

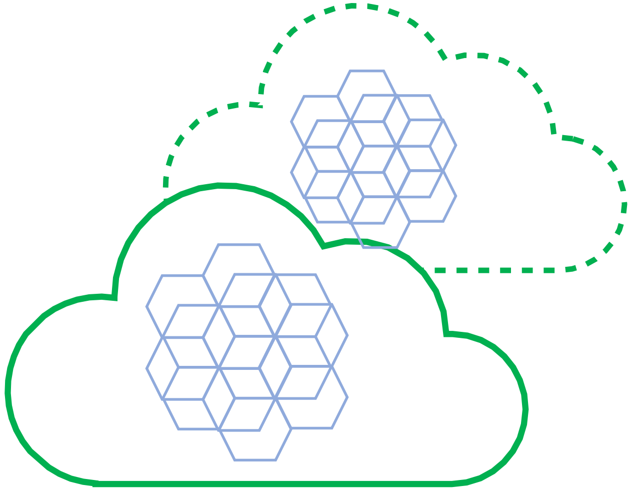
Cost-effective backup

A cloud installation provides a cost-effective automatic backup of data and production content, allowing rapid restoration of operations following a data breach.

Anti-ransomware

'Ransomware' attacks can put PC clients out of action by locking up data and applications on users' PC platforms.

Rapid deployment of *Swing* requires only a functional web browser on users' machines and can allow users to resume editorial work in emergency mode until other applications have been restored.

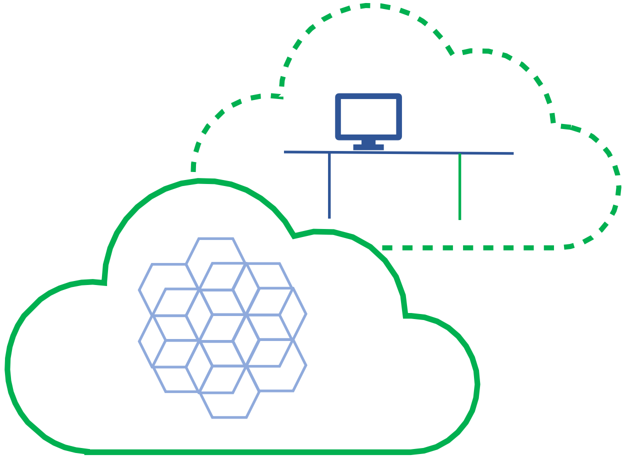


Disaster recovery using virtual desktops

Virtual desktop solutions (*see page 11)* provide an even more complete recovery solution for cloud-hosted users - especially from ransomeware attacks (*see page 12*) .

By deploying a new virtual desktop for each user, together with applications, a full range of software functionalities can be restored.

This solution can be rolled out immediately across a very large numbers of users - in far less time than that required for a complete reinstallation of the user's local OS and applications.



Security certification and audit

ISO 27001 and DoD certification

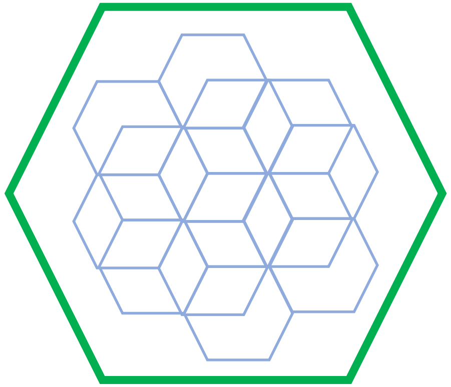
ISO27001 is an internationally recognized standard of comprehensive security control for organizations managing information assets.

Eidosmedia design and development processes are completing certification to ISO 27001 standards (completion in Q2 2021). Their platforms are also compliant with the Risk Management Framework for the NIPR and SIPR networks of the United States Department of Defense.

The Eidosmedia Security Check

Before going live, all Eidosmedia deployments are subject to a comprehensive security audit based on the NIST Security Technical Implementation Guide (STIG). Its aim is to close all potential access routes except those needed for operation.

This procedure can also be applied to existing customer installations at any time to reveal points of weakness and opportunities to reinforce platform security.



Contacts

Eidosmedia Milano

Eidosmedia S.p.A.
Mac 7, Via C. Imbonati 18
20159 Milano, Italy
Phone: +39 02 36732000

Eidosmedia London

Eidosmedia Ltd
23 Austin Friars
London, EC2N 2QP, UK
Phone: +44 (0) 207 002 1097

Eidosmedia Paris

Eidosmedia S.a.r.l.
55, Rue de Rivoli
75001 Paris, France
Phone: +33-1-53.05.34.70

Eidosmedia Frankfurt

Eidosmedia GmbH
Voltastraße 31
60486 Frankfurt, Germany
Phone: +49-(0)69-260.106.450

Eidosmedia New York

Eidosmedia Inc.
14 Wall Street, Suite 1602
New York, NY 10005, USA
Phone: +1 212 227 6025

Eidosmedia Sydney

Eidosmedia Pty Ltd
66 Clarence Street
Sydney, NSW 2000, Australia
Phone: +61 (02) 8705 5438

Eidosmedia Shanghai

Eidosmedia China - 意巅科技
The Center, Suite 2059
989 ChangLe Road
Shanghai, China 200031
Phone: +86 (0)21 8017 5042

info@eidosmedia.com
http://www.eidosmedia.com

EIDOSMEDIA