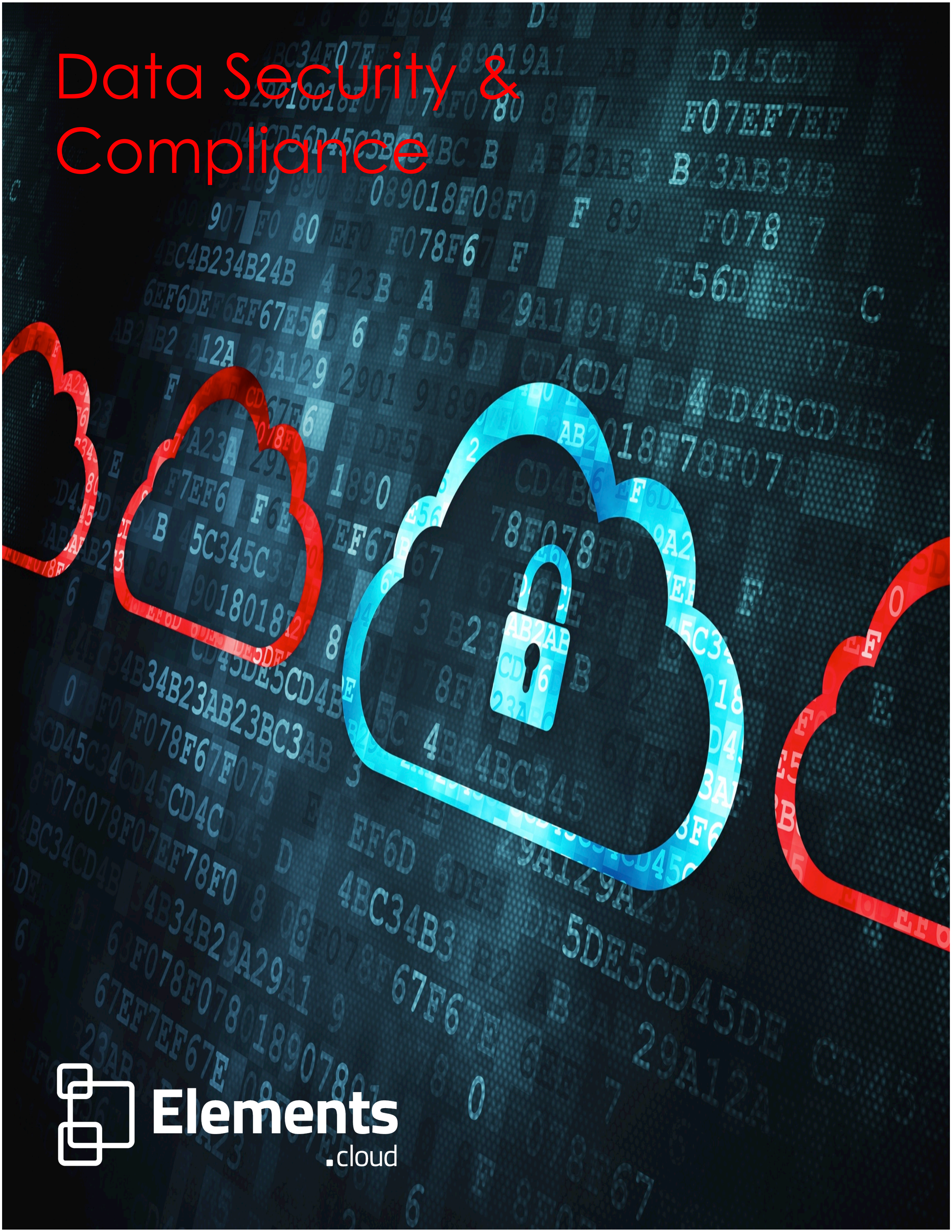
Data Security & Compliance



Elements
.cloud

Corporate Operational Security

ISO27001

ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems. In order to maintain this certification, we must demonstrate that we have systematic policies in place to maintain an on-going approach of managing information security risks that affect the confidentiality and availability of customer information.

Our ISO 27001 certification verifies that they have these systematic policies in place

Information Security Management System
ISO
27001
Certified

System and operational security

Elements protects its system infrastructure by using dedicated firewalls to block unauthorized system access. Servers are patched based on vendor recommendations and hardened by removing unnecessary processes and open ports.

Employee data access

Tight system access security is enforced and no Elements employee is able to access customer data unless specifically required to do so for support reasons. Then only specially designated senior technical employees have the necessary access permissions. Any systems access is logged and tracked for auditing purposes.

Employee data access

Tight system access security is enforced and no Elements employee is able to access customer data unless specifically required to do so for support reasons. Then only specially designated senior technical employees have the necessary access permissions. Any systems access is logged and tracked for auditing purposes.

Software security

All new features are deigned and tested to prevent potential attacks such as SQL injection and cross-site-scripting.

Network security

Elements encrypts all communication between customers and our data center using TLS. The browser based application and all data transferred to the applications use HTTPS. Any unencrypted access is first redirected to HTTPS before completing. All passwords are stored one-way hashed in the database.

Service reliability and file system backup

We operate active-active from multiple, distributed data centers and maintain a real-time, streaming replica of all customer data on separate hardware. We use real-time backup of customer data to allow recovery to a specific point in time.

Elements is engineered for the enterprise

Elements has been built from the ground up with the security and integrity of your data as paramount. We use best industry practice to deliver a software and security infrastructure that provides an extremely scalable, and highly reliable platform for our customers.

Data Centre Compliance: AWS

We use the industry leading Amazon Web Services (AWS) data centres, which are considered to be the world's best by industry analyst firm Forrester. They provide a broad set of capabilities in terms of data center security, network security, and a significant number of certifications. This level of data center and operational security allows us to be compliant with many of the most stringent industry standards.

We also comply with the US & EU Safe Harbor Frameworks for protecting the privacy of data flowing from the EU to the United States, as set forth by the US Department of Commerce.

We comply with the US & EU Safe Harbor Frameworks for protecting the privacy of data flowing from the EU to the United States, as set forth by the US Department of Commerce. In providing our Service, we do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers, and in fact we are largely unaware of what information is being stored on our platform and only access such information as authorized by our customers or as required by law. Only you or your customers are entitled to access, retrieve and direct the use of such information. As such, we are only the "data processors" and not the "data controllers" of the information on our platform for purposes of the EU Directive on Data Protection (Directive 95/46/EC). To learn more about the Safe Harbor program please visit http://www.export.gov/safeharbor/

Data Security & Compliance: Elements.cloud infrastructure

Our datacenter partner Amazon publishes a Service Organization Controls 1 (SOC 1), Type II report. The SOC 1 Type II report covers controls in place at a Service Organization intended to meet the needs of the user entity. The type II report additionally includes an auditors overview of the operating effectiveness of the controls in place to achieve the control objectives.

In addition to the SOC 1 report, Amazon publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations.

You can also review the Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a public summary of Amazon's SOC 2 report.

ISO 9001:2008 is the international standard for Quality Management Systems (QMS), published by ISO (the International Organization for Standardization). AWS has undergone a systematic, independent examination of their quality system to determine whether the activities and activity outputs comply with ISO 9001 requirements.

ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems. In order to maintain this certification, a company must demonstrate that it has systematic policies in place to maintain an on-going approach of managing information security risks that affect the confidentiality and availability of customer information. The AWS ISO 27001 certification verifies that they have these systematic policies in place.

Penetration and Vulnerability Testing

We take data security very seriously and proactively monitors and tests the network, data center infrastructure, and application.

Penetration and vulnerability testing

We undergoes regular network perimeter and web application vulnerability scanning using leading third party providers. The scans are designed to pre-emptively notify us of any potential vulnerabilities.

Customer penetration and vulnerability testing

If our customers wishes to do their own penetration test and security vulnerability scan this can be requested. A specific fee will be charged for this service. Since penetration tests are often indistinguishable from network attacks, all customer-initiated tests must have permission requested and granted in writing by our technical staff prior to being run.

Elements Software security features

The Elements application suite has had security designed into it from the bottom up. The software and systems architecture team has decades of experience in designing and building secure scalable applications.

Application Security

The following features are built into the software to support all of our customers.

Secure network access

All customer communications are over secure HTTP access (HTTPS) so that you can establish secure communication sessions with your Elements account using TLS.

Encryption of data at rest

All account data that is not moving through the network is encrypted while "at rest" in the database. We encrypt all data using 256-bit AES encryption.

Single sign-on (SSO)

Customers can configure single sign-on for their Elements account, allowing their existing identity provider to control access to the Elements application.

User permissions

Access to data within your Elements account is on a per user basis allowing account administrators to restrict access to data.

Elements Salesforce integration

The Elements application consists of two components.

- core Elements application is a native Web application written using the MEAN stack (MongoDB, Express, AngularJS, Node) and runs on the AWS environment.
- Elements Documentation Hub for Salesforce managed package that is installed into the Salesforce Org that is connected to the Elements application.

Elements application

The Elements application runs in the AWS Dublin data centre. The primary database is an Atlas MongoDB cluster that is provided as a service by MongoDB. The cluster is split with the primary nodes in the AWS Dublin data centre and a secondary in the AWS Frankfurt data centre to provide cross region disaster recovery capability.

The Elements application is a multi tenanted application with a single database instance. The tenancy based on the concept of a Space with users able to be members of multiple Spaces. An individual Space can connect to multiple Salesforce Orgs but an Org can only connect to a single Space. Elements is a Salesforce connected app.

Managed Package

The Elements Documentation Hub for Salesforce is a managed package. It provides a number of capabilities including:

- Provisioning of Users into Elements and providing SSO
- Capability to fetch the metadata structure of the Org from Salesforce and store it in the Elements database
- Display of process content into Salesforce pages using either Visualforce or Lightning components
- Ability run the Elements application within a Salesforce tab

Salesforce Security Review

The Elements Documentation Hub for Salesforce managed package has passed the Salesforce security review and is on the AppExchange. This extensive process not only evaluates the managed package but covers any connected apps as well. The entire Elements application suite and website was rigorously security tested in order for the managed package to be signed off and made available from the AppExchange.

Salesforce data held by Elements

Elements fetches data about the Org in order to allow users to document their configuration. It fetches the metadata of the Org but does not query or fetch any operational data. However, for example, picklist values on Fields are considered metadata as are query parameters on sharing rules.

The managed package does query the operational records but only to perform a count of which fields have data populated and none of this data is returned to the Elements application.

The following are queried:

- Report configuration
- Dashboard configuration
- Email template configuration
- Salesforce Users

The Salesforce Users data is stored so that details on access to fields can be calculated and shown.

Process by which Data is Fetched

The data is fetched using a number of approaches. Primarily, Elements makes API calls into the Elements Managed Package which then uses a combination of DML calls and REST api to Salesforce. This requires a remote site setting to be set upfor the specific Salesforce instance to call itself, to collect the required data which is returned to Elements. In addition Elements makes direct calls to the SOAP api to fetch specific data that is only available through this mechanism.

The Elements application suite has had security designed into it from the bottom up. The software and systems architecture team has decades of experience in designing and building secure scalable applications.

www.elements.cloud
success@elements.cloud

DocID: 68978, V8.0, 2018