3E Cloud

Security Information Guide

Document Version 1.2
Date of issue: 2022-01-17

THOMSON REUTERS®

Contents

About this document

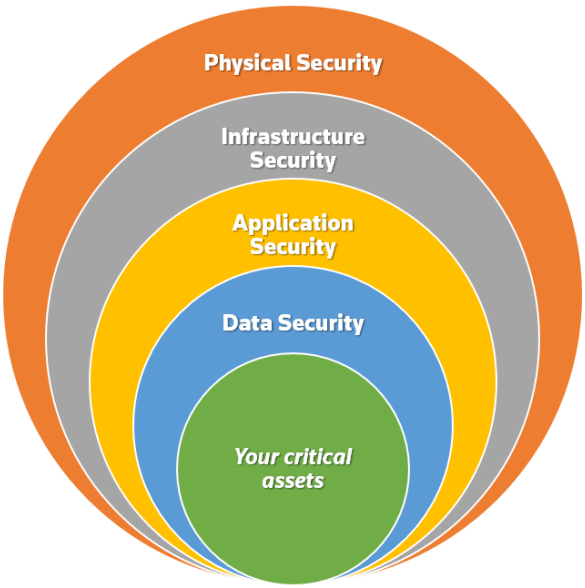
INTENDED READERSHIP

This guide is intended for current and potential customers who have technical roles such as CTO, IT Director, and the like.

IN THIS GUIDE

This guide provides security-related details pertaining to the 3E Cloud offering. Among the topics covered in this guide are:

- Details on the following layers of security:



- Testing and auditing
- Security information and event management (SIEM)

If you are an existing customer, you can find more information regarding 3E Cloud in the Knowledge Base.

Security Is a Top Priority

For firms like yours, security is a top priority. Security is a top priority for us as well.

We all know about the large variety of threats out there. Good security practices can help you protect data, comply with government regulations, and maintain a competitive edge.

At Thomson Reuters, we know how to build secure, enterprise-scale applications. We have been doing it for decades.

OUR PEOPLE

Meeting security standards begins with the people we have building and developing the products.

As part of our standard new hire process, Thomson Reuters verifies an individual's education and previous employment, and performs internal and external reference checks. All Thomson Reuters employees undergo security training as part of the onboarding process and receive ongoing security training throughout their careers. New employees agree to our Code of Business Conduct and Ethics, which highlights our commitment to keep customer information safe and secure, and complete a mandatory security and data protection course. Depending on their job role, additional training on specific aspects of security may be required.

OUR PROCESSES

Thomson Reuters has a global team of certified security and privacy subject matter experts dedicated to the security of our products and services. This extended team is committed to our Information Security Risk Management (ISRM) program, which is endorsed by the Thomson Reuters Executive Committee.

Thomson Reuters' cloud applications are required to perform a security assessment prior to production launch to validate all security requirements and ensure active controls are in place to protect cloud resources.

OUR PLATFORM

3E Cloud is deployed in Microsoft Azure, taking advantage of state-of-the-art platform security services.

Microsoft Azure spends more than $1 billion each year on security research and development, and has a team devoted to network security. Cloud databases lie within intricate, multi-tiered security networks that are regularly upgraded and tested for potential weaknesses. There are backups within backups, all meant to protect your information in the event of a hack or a natural disaster. Cloud computing offers far more extensive security than any law firm could provide on its own.

Physical Security

One of the first defenses in protecting any asset is establishing physical security measures designed to prevent unwanted parties from gaining physical access to the asset. As the cloud provider, Microsoft is responsible for physical security and has invested heavily in strict physical access controls where your data is stored.

DATA CENTERS

Microsoft's data centers are designed to control physical access to your data.

The data centers have multiple layers of protection, from the facility's perimeter to the building's perimeter to inside the building to the actual data center floor. For example, permission to enter a data center is approved on a "need to access" basis to keep the number of approved individuals to a minimum. Controls inside the building include two-factor authentication with biometrics and full-body metal detection screening.

Microsoft conducts physical security reviews of the facilities on a regular basis.

For more information about physical security, visit: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

HARDWARE DISPOSAL

An important aspect of physical security is hardware disposal. When hard drives start to fail out, they need to be decommissioned. This process should include procedures to address destruction of customer data.

Microsoft's data destruction procedures cover hard drives, solid state drives, and other storage devices.

A device will undergo one of the following processes:

- **Clear** – Sanitize data against simple data recovery techniques.
- **Purge** – Protect data against state-of-the-art laboratory techniques.
- **Destroy** – Same as purge, with the addition of making it no longer possible to use the device for data storage.

Microsoft follows the US Department of Commerce's NIST SP-800-88 guidelines for media sanitization.

You can learn more about these procedures at: https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

Infrastructure Security

Infrastructure security measures, such as protecting the network, ensuring devices and applications communicate within that environment in a secure manner, and limiting who can gain access to these underlying systems, are also in place. Microsoft and Thomson Reuters are jointly responsible for this infrastructure security.

NETWORK

To protect the overall network, Microsoft and Thomson Reuters employ a blended strategy of passive, interactive, and proactive defensive technologies across our environment.

One such technology is network segmentation and route isolation in key or strategic locations of the network. In addition, as 3E Cloud is built on top of Microsoft Azure, we benefit from Azure's built-in Distributed Denial of Service (DDoS) monitoring and prevention, as well as Thomson Reuters' additional ingest traffic monitoring and remediation.

ENDPOINT SECURITY

To ensure devices and applications communicate within the environment in a secure manner, token-based security with OAuth2 that has limited access is used for inter-module communications. Communication between the 3E Cloud modules is always authenticated, and any data sent between the modules is encrypted. 3E Cloud modules also follow the principle of least privileged access to prevent broad sharing and access of data between modules.

ACCESS MANAGEMENT

To limit who can gain access to these underlying systems, Thomson Reuters has a privileged access management capability within 3E Cloud. A three-pronged approach has been implemented for privileged access management.

- Firstly, we reduced the need to access production resources for outlier tasks like software upgrades, hardware commissioning, and monitoring that typically would have required human intervention and access to underlying resources. We have automated tasks, so upgrades are done through CI/CD pipelines, scaling up and down is automated, and monitoring is done with dashboards and alerts, thereby reducing the need for direct or physical access.
- Secondly, we have limited the number of authorized personnel that can access production infrastructure. Their access is controlled through a vault that has expiring password and multi-factor authentication (MFA) enabled.
- Thirdly, all access to resources is tracked through an audit trail, providing visibility for infrastructure access.

SECURITY PATCHES

Part of infrastructure security is also ensuring it is evolving and continuing to provide protection as better practices and methods are discovered and as new threats are uncovered. Microsoft and Thomson Reuters employ automated patching policies and procedures to keep systems up to date, including zero-day security patches.

Application Security

Application security includes an identity and user access layer. Application security is designed to ensure identities are secure, access granted to the applications is only what is needed, and changes are tracked and logged. Partnering with Thomson Reuters, the customer has primary responsibility for identity and user access.

Thomson Reuters provides the capabilities to enforce identity and user access security controls to the 3E Cloud resources, product environments, and applications. These controls adhere to established industry standards including least privilege, segregation of duties, unique IDs, password management, and strong authentication.

Customers are responsible for ensuring that the right people are assigned the right level of access and privileges and access privileges are managed to reflect changes in position and employment status.

AUTHENTICATION

Authentication can be summarized as the process of verifying who someone is. This section outlines how this authentication is achieved within 3E Cloud, including our support of other associated components such as Multi-Factor Authentication (MFA) and Single Sign On (SSO).

Federation

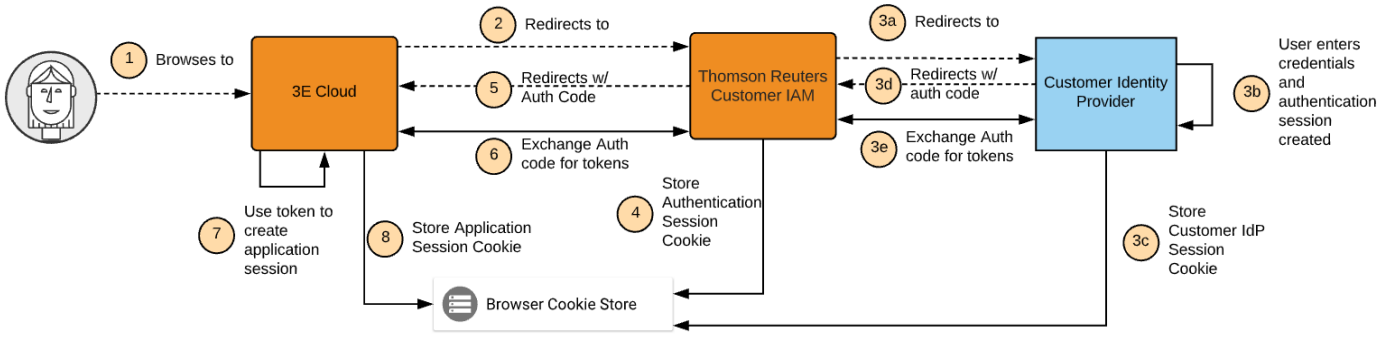
Federation leverages standards and protocols to map user identities between identity providers (IdP) across organizations by means of trusted relationships. To access 3E Cloud, each customer federates their identity provider (e.g., Azure Active Directory, etc.) with Thomson Reuters' federation provider.

Once the federation has been established, the customer can control access to 3E Cloud for users through its identity provider. This provides many benefits. For example, users at the firm do not have to create a separate user profile with Thomson Reuters or worry about remembering yet another username and password. These users will use their identity provider credentials to log in to 3E Cloud.

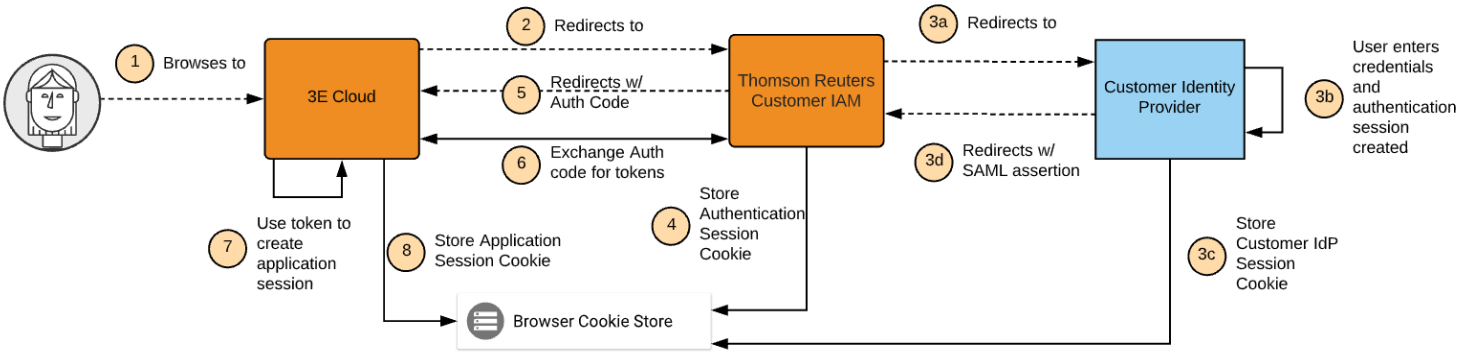
Because of federation, customers themselves can easily apply and manage multi-factor authentication (MFA), password policies, joiners and leavers, and other features offered by their identity provider to control 3E access.

3E Cloud supports federation through OpenID Connect (OIDC) and Security Assertion Markup Language (SAML).

Here is an example authentication flow with OIDC federation:



Here is an example authentication flow with SAML federation:



Multi-Factor Authentication

Multi-Factor Authentication (MFA) adds an extra layer of protection, in addition to usernames and passwords. Users are required to perform an additional step, such as a one-time passcode or a fingerprint, to confirm their identity. 3E Cloud customers can set up multi-factor authentication (MFA) using their identity provider and setting up MFA is recommended for all user accounts that access 3E applications. As mentioned above, federation allows the customer to control access to 3E Cloud themselves for their users through their directory. Customers can thus apply and manage multi-factor authentication and other features offered by their identity provider themselves to control 3E Cloud access.

Single Sign On

Single Sign On (SSO) is a capability to use the same username and password across multiple systems and applications or to sign in without credentials at all (a.k.a seamless single sign-on). Azure Active Directory and other identity providers support a variety of authentication methods to simplify login for end-users, including logging in to 3E Cloud. This is a configuration that a customer will need to configure/manage themselves however if they wish to set up SSO.

AUTHORIZATION

Authorization can be summarized as the process of defining and verifying what permissions and abilities (such as usage of specific applications, file locations, and data) an authenticated user has access to, or shouldn't have access to.

The 3E Cloud security model is user and role based. We recommend that customers set this security at the role level. We start with a common model for the security tree and train the customer to adjust it to their needs. It is flexible enough to allow firms' system administrators themselves to grant general access to specific areas of 3E Cloud. For example, an administrator can grant a billing clerk role access to billing processes and reports, while at the same time restrict the role's ability to edit historical data.

It is also granular enough to restrict a single user's access to a specific control on a form. For example, the model allows a user to be granted the ability to access the Timekeeper Maintenance process but be restricted from the Timekeeper Rate controls on the process itself.

Furthermore, customers can restrict access in 3E Cloud to a specific record. For example, a customer can restrict access to a matter based on an ethical conflict or restrict access to a confidential, high-profile client.

Much deeper details can be found in our Knowledge Base, such as KB Article TR-5377 - Security Configuration in Elite 3E, and KB Article TR-7390 - User and Role Setup Roadmap for 3E Process Level Security.

Data Security

Data security is a combination of both practices and processes that are designed to protect your critical business information. Microsoft and Thomson Reuters are jointly responsible for data security. This section focuses on how your data is isolated and encrypted, where it resides, and how access to it is controlled.

DATA ISOLATION

While we may use a combination of single and multi-tenant services, your data will never co-mingle with the data of other customers. To ensure this, 3E Cloud customer data is stored in a single-tenant database, and secrets are held in a separate key vault.

DATA ENCRYPTION

All data stored on disk (e.g., file attachments, PDF report output) is encrypted through 256-bit AES encryption. Communication with the storage system is encrypted via HTTPS. Data stored in Azure SQL Database is encrypted with Microsoft's Transparent Data Encryption (TDE) using 256-bit AES encryption. Communication between the application services and the database is encrypted with Transport Layer Security (TLS). Encryption keys and certificates are managed consistent with industry practices and are rotated periodically.

Azure Key Vault is used to manage and safeguard application secrets, keys, and certificates (TLS), providing access controls during tenant registration and while logged into the 3E system. This also allows all data streams to be encrypted while in transit.

In Microsoft Azure, all clients' access to web services and integration services is via encrypted HTTPS to an application gateway. The application gateway is located behind Azure's layers of external-facing firewalls, intrusion detection, and denial-of-service protections. The application gateway is a Layer 7 device that, in addition to load balancing for high availability, allows us to configure additional application-level protections for many kinds of injection and overflow types of attacks. The application gateway ensures that 3E Cloud users are routed to the appropriate endpoint to run processes.

3E Cloud data is stored in Azure SQL Database, using its built-in security composed of Transparent Data Encryption (TDE) and Always Encrypted settings and securing and encrypting data at rest. Azure storage provides blob storage containers for all the internal files used by 3E Cloud, such as attachments, billing output, and other sensitive documents. Azure Storage Services Encryption (SSE) is coupled with Azure Blob Storage to further enhance security.

Bring Your Own Key (BYOK)

3E Cloud does not currently offer BYOK. As mentioned above, customer data isolation allows us to use separate keys for each customer's data. We use a separate key vault for the keys and secrets of each customer. Key management and rotation are automated and tested.

We do not support client-supplied encryption keys. We need the encryption keys to display the data on the screen. If the customer supplied the keys, we would need to go to the client to obtain the key, decrypt it, and give the key back, which would impact efficiency. We store the keys in an Azure key vault, which has a high level of security.

Many firms that use SaaS applications want to control the encryption keys used to protect their data. This concept is commonly called "Customer Managed Keys" (CMK) or "Bring Your Own Key" (BYOK). For the purposes of this document, the term BYOK will be used.

When deploying BYOK, the firm maintains control of the encryption keys and, therefore, could require explicit authorization of anyone accessing its data. There are a few common variations of the process involved, and there are instances when BYOK is not used. Below is a quick overview of different versions of BYOK.

Full Key Management

In this scheme, the firm implements a credentials management process to generate and store its keys. In most cases, this is accomplished with a tamper-resistant hardware security module (HSM). The firm grants access to the appropriate keys for the HSM to the firm's SaaS application provider (an example of a provider would be Thomson Reuters).

Key Creation and Ownership

In this scheme, the firm may not own or maintain an HSM. Instead, an independent certificate authority (CA) is used. The firm generates a key and binds it to a certificate issued by a CA, and then securely transmits the key material to the SaaS application provider. The key is valid only until the certificate expires or the certificate appears on a certificate revoke list. The SaaS application provider and cloud provider must write their software to frequently verify that the certificate is valid and not revoked. Because revoking the certificate results in permanent data loss, this option is not advisable.

Encryption Boundaries

In this scheme, the SaaS application provider creates and manages all the keys but is careful to generate separate keys for each of its customers' data. This scheme requires more trust than the previous two. If a firm wanted to revoke access to its data, it would request that the SaaS application provider destroy the keys. Because the firm does not maintain control over or manage the keys, this option is not considered BYOK. This option is available for 3E Cloud users.

Customer Expectations

BYOK has different implications for a SaaS provider, like Thomson Reuters, than for cloud providers like Microsoft Azure or Amazon AWS. Cloud providers often do not need to access their customers' data for routine operations. In virtual machines or even in platform databases, the cloud provider stores, manages, and backs up the data, but they do not process it. The cloud provider does not need to decrypt the data to perform these steps.

In contrast, a SaaS application like 3E Cloud must process the data. For example, 3E Cloud runs reports on behalf of the firm, processes workflows and other automation tasks, integrates with other applications, and performs many other tasks. That implies that the application must access the encryption keys, and by further implication, the application provider must have access to the encryption keys.

This does not imply that any application provider employee can gain access to its customers' data. Encryption keys do not control access to the data; instead, modern privileged access management procedures control data access.

Occasionally, there is a misconception in which a firm believes they have controls and protections that, in reality, are not provided to them—even with complete customer key management. For example, access to data does not require explicit customer approval.

Another common misconception with BYOK is the belief that the firm provides the key that encrypts the actual data. That is rarely the case. Typically, data is encrypted with a key, called the Data Encryption Key, supplied by the cloud provider or the application provider. That key is then encrypted with another key called the Key Encryption Key. That wrapped key is the one stored in the vault or HSM.

The 3E Cloud Approach

BYOK brings a certain level of risk. If a firm stores the keys as described in the Full Key Management scenario, then a sustained lost connection from 3E Cloud could result in a complete system outage.

With the other key management methods, a firm would need to generate the key materials and securely transmit them to Thomson Reuters. Extra tools, verification steps, and screens to help that process would need to be developed and injected in the flow. Any procedure involving handling a key has some risk of compromising the key or even destroying it and all the data with it.

With these considerations, 3E Cloud does not currently offer BYOK. As explained in the Encryption Boundaries section, we maintain customer data isolation, allowing us to use separate keys for each customer's data. We use a separate key vault for the keys and secrets of each customer. Key management and rotation are automated and thoroughly tested.

We have worked with our trusted partner, Microsoft, on this solution design. It provides the expected amount of control with the security, safety, and manageability required.

DATA RESIDENCY

We understand that clients may prefer to have their data reside in a certain location in Azure. Microsoft has more global Azure regions than any other cloud provider, which gives Thomson Reuters the flexibility to deploy applications where needed. Azure is generally available in 54 regions around the world. 3E Cloud is currently available in the US, Canada, UK, Europe, and Australia.

While Azure has more global regions and Azure customers may have the flexibility to store data in centers they choose, there are certain parameters that require some customers to store data in their country. As 3E Cloud expands globally, 3E Cloud is being deployed in the appropriate geo-political Azure data center to serve the target market.

DATA PRIVACY

Thomson Reuters places a high priority on meeting our customers' expectations of privacy. To meet these expectations, Thomson Reuters has a dedicated, global Privacy Office that is responsible for implementing, promoting, and overseeing our Privacy Program framework that supports Thomson Reuters' compliance with applicable privacy and data protection laws around the globe. The Thomson Reuters Privacy Program is composed of numerous controls and procedures to safeguard personal data across the enterprise.

For a full list of compliance standards that Microsoft Azure adheres to, see: https://docs.microsoft.com/en-us/compliance/regulatory/offering-home?view=o365-worldwide

DATA ACCESS

Does Thomson Reuters access my data?

By default, Thomson Reuters does *not* access your data. If a support case arises, Thomson Reuters follows the principles of Privileged Access Management (PAM) as mentioned earlier. PAM includes auditing processes designed to ensure that only authorized personnel are allowed into your environment when required and only for the length of time necessary to resolve issues on your behalf.

With regards to operations, we have a dedicated internal team called 3E Cloud Operations (Ops) who are responsible for provisioning resources in Azure and deploying Thomson Reuters (TR) software solutions which leverage those resources. Ops also maintains and updates those resources and solutions. Because of these responsibilities, it is necessary for Ops to have administrative privileges. Those privileges provide Ops the ability to access customer data.

Ops will use audited "management" accounts (currently in the TR MGMT domain) for all primary access. Primary access, for 3E Cloud products, includes accessing the Azure portal and Azure resources, including Azure SQL. In the event a resource must be accessed via a non-management account (e.g., a native Azure SQL login), Ops must make use of a "jump-box" via a management account to ensure an audit trail is created for that primary access before the non-management account (secondary access) is used. Other than by this two-step method, direct access by non-management accounts is prohibited by design, policy, and practice.

Ops users will only use these administrative privileges to view customer data in the following two scenarios:

Permission

Documented through a CRM (Customer Relationship Management) case (currently Salesforce), a customer may, directly or via TR Support, agree in writing to permit Ops to access their data.

Procedure: Ops will require TR Support to create an Azure DevOps work item, related to the CRM case, as a record which requests and defines the scope of the data access to be performed by Ops.

Necessity

Absent customer permission via CRM, Ops should never access customer data, except as is necessary to ensure the proper functioning of a TR software solution. Necessity and the scope of access may be determined by TR Support, the product development delivery team (DT), or by TR Services. Ops does not have any independent need to access customer data.

TR Support has its own policies and procedures governing its access to customer data. In the event a CRM case should require Ops to access customer data, Ops will do so at the direction of TR Support and/or the DT to facilitate the resolution of the case. TR Support and/or the DT guidance will determine the scope of Ops actions relative to the needs of the customer case. An example of

necessity would be validation of a customer 3E Cloud instance, after an update of the solution by Ops (such as applying a fix); this could involve limited manual validation by Ops, in addition to any automated validation procedures.

TR Services may require assistance from Ops in order to perform implementation services. In the event a TR Services engagement requires Ops to access customer data, Ops will do so at the direction of TR Services. TR Services will determine the scope of Ops actions relative to the needs of the customer implementation. An example of necessity would be Ops performing a backend operation to update application user records to support authorization and exercising the software to validate the success of the update.

Procedure: Ops will require TR Support to create an Azure DevOps work item, related to the CRM case, as a record which requests and defines the scope of the data access to be performed by Ops. Ops will require TR Services to create an Azure DevOps work item, related to the services engagement, as a record which requests and defines the scope of the data access to be performed by Ops.

How can customers access their data?

Customer can access their business information via the user interfaces of the 3E Cloud applications. But what if you require more direct access to this data?

For security reasons, 3E Cloud customers do not have *direct* access to the Azure SQL Database. Direct SQL access for queries, data updates, etc. and direct connection for SSRS reporting are not permitted. One benefit of a SaaS solution is the elimination of the need for advanced database expertise. The comprehensive solution of 3E Cloud enables firms to gather and present their data without commitment to long-term support of customizations, which will also enable Thomson Reuters to seamlessly upgrade 3E Cloud customers.

We recognize that customers may still wish to access their data to pull into their existing data warehouses for reporting. To meet this need, Thomson Reuters can provide an OData API to the Data Insights data mart (requires Data Insights). When this is enabled, customers can take advantage of this API to access data for reporting needs, including SSRS.

Customers can also use our public API endpoints, and the Elite Service Bus (ESB) integration architecture to import and export data to the 3E Cloud environment.

DATA LEVEL SECURITY

The 3E Cloud Core software also includes Data Level Security (DLS) capabilities designed to address data privacy requirements. (3E Cloud Core is the main business operations management solution, which includes the Billing, Collections, Accounts Payable, General Ledger, Conflicts, and Records features.)

DLS allows security to be managed at the database row level. A user's access rights can be restricted so that they can only view or add certain data. Typical users might be restricted to view-only statistics for their own office or be restricted from viewing information that is behind ethical walls. 3E Cloud handles this by using behind-the-scenes database level functionality: the ability to build special schemas and views for each user. When a user executes a database transaction, the user is connected to the database with their user identification and their view of the database is enforced. The database responds to the query with the data they are allowed to see. Although these views are administered within 3E Cloud, they are enforced by the database engine itself.

One advantage of this architecture is that it helps to prevent security from being bypassed with third-party tools. This level of security provides for very granular control. The firm must set the balance between their data security needs and the challenge of administering the data with security rules in place.

Currently with 3E Cloud, a Legal Professional Services engagement is required to work with the customer to perform data analysis and potential data updating requirements. In the future, we plan to deliver front-end data privacy capabilities so cloud customers can perform the data analysis and any desired updates to their data themselves.

For more information on 3E's DLS capabilities, please refer to the 3E Administration Guide (Knowledge Base article TR-18665).

Testing and Auditing

RISK ASSESSMENT

With dedicated resources focused on improving information security practices throughout Thomson Reuters, we strive to identify risks to our information assets and to guard against unauthorized access, loss, or misuse. The services performed during risk assessment activities include:

- Architecture reviews
- Vulnerability scans
- Application security testing
- Technical compliance reviews

Manual penetration tests are performed annually by Thomson Reuters internal penetration testing teams and/or by our authorized vendors. Penetration testing is done on a duplicate instance of 3E Cloud that contains no customer data.

Thomson Reuters utilizes a range of commercial and open-source intelligence sources to enable our teams to regularly monitor, analyze, and mitigate potential cyber threats to the company.

3E Cloud and all its infrastructure and components are regularly scanned by numerous threat assessment tools. These include assessments from Microsoft Azure and assessments developed internally by Thomson Reuters. The results of those assessments are reviewed periodically by Thomson Reuters' security and operations personnel.

AUDIT PROCEDURES

Our ISRM compliance team performs audits against policies, standards, and regulatory requirements, and registers findings for review and remediation initiatives within the business.

The Thomson Reuters Third Party Risk Management program includes undertaking due diligence designed to ensure that vendors and partners have the appropriate controls in place to protect our data and that of our customers. Third parties are contractually required to comply with the Thomson Reuters Data Processor Obligations (DPO), which encompass both our security and privacy standards. Risk-based assurance testing and audits are carried out on vendors and third parties to verify ongoing compliance with contractual terms and the DPO.

SECURITY SCANS

Veracode static and dynamic scans are performed regularly to check the application for vulnerabilities.

Static scans focus on the internal structure of the code while the application is offline. Dynamic scans look for functional vulnerabilities at runtime. Veracode recommends doing both types of scans for business-critical applications.

Vulnerabilities identified during the scans are prioritized and remediated.

Security Information and Event Management (SIEM)

PLATFORM TOOLS

Thomson Reuters increases cloud defense in the IaaS, PaaS, and SaaS environments by employing Azure Security Center, as well as custom detection telemetry in key locations.

Azure Security Center is a security management tool designed to help organizations improve their security posture. The main dashboard page contains a summary of key information, such as a "secure score" that aggregates the latest findings. Azure Security Center provides recommendations on how to improve the security of monitored resources.

THOMSON REUTERS TOOLS

The Thomson Reuters Information Security Risk Management (ISRM) team supports a comprehensive application security testing capability, which can include one or more of the following:

- Services to perform static and dynamic application security testing
- Internal and external infrastructure vulnerability scanning
- Third-party penetration testing

Thomson Reuters employs a tiered incident management and escalation model. Incidents are triaged based on criticality and assigned through incident leads in each region. Incident command follows documented response practices, as well as established communications and escalation practices. Coordination of incidents also involves IT and product teams and the use of outside communications expertise and general counsel, where necessary.