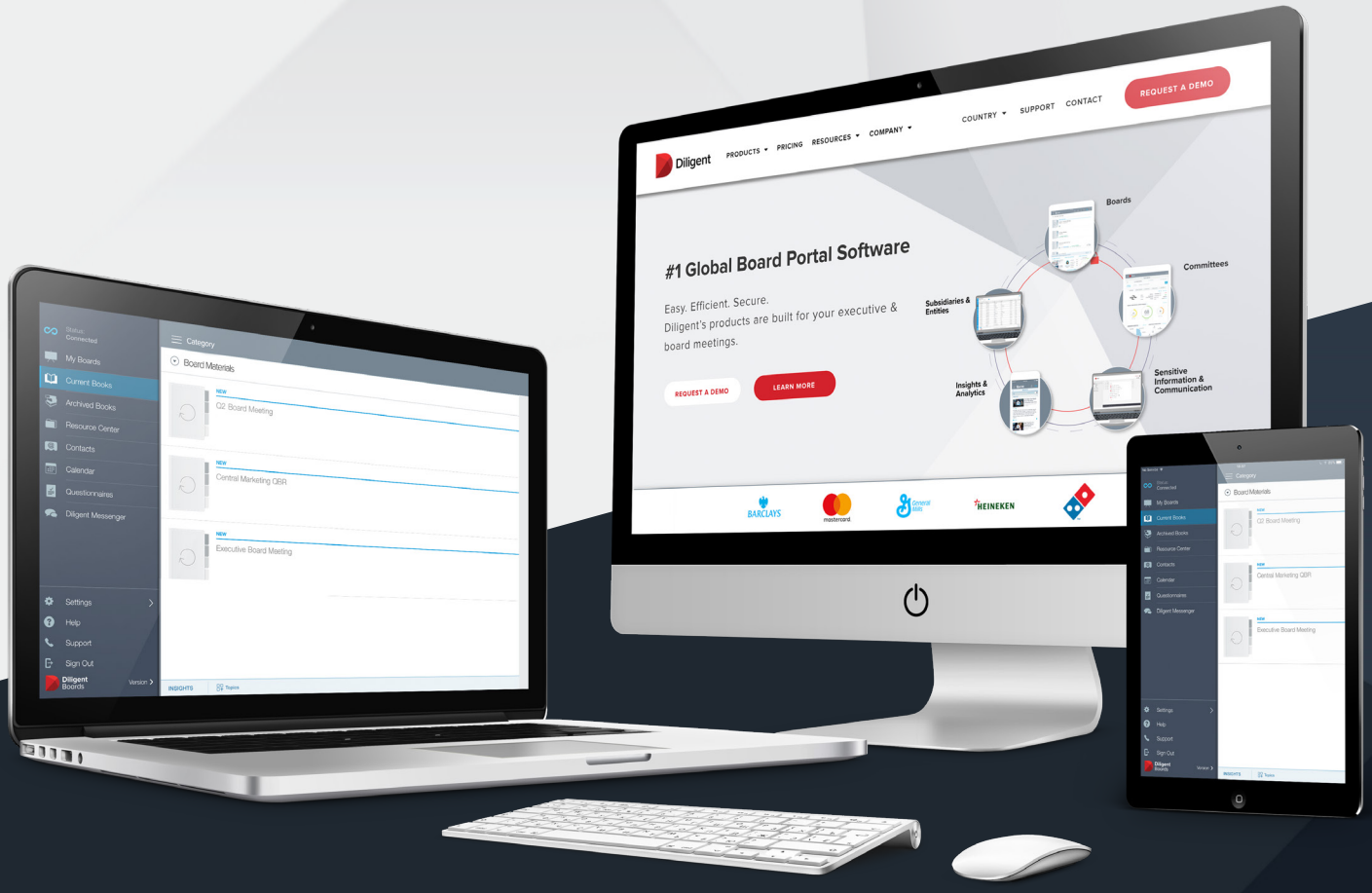
Diligent

DILIGENT SECURE FILE SHARING AND MEETING WORKFLOW

SECURITY FACT SHEET



Diligent's Security Solutions

Collaboration across functions and individuals is an imperative to modern governance, but it has to happen in a locked-down environment that mitigates the risk of data leakage, human error or attack. Diligent solutions provide an enhanced security ecosystem for the sharing and collaboration around sensitive documents, classified workflows and confidential information that happens across the board and senior management teams. Our solutions have been architected with the most aggressive security and privacy standards and are protected above the enterprise networks to mitigate risk and exposure. System integrations allow configurable access controls and enable customers to set their own parameters on exchanges and data workflows.

Security Features that Strengthen Your Defenses

ORGANISATIONAL SECURITY

Diligent has established a security program based on industry standard frameworks that is dedicated to ensuring customers have the highest confidence in our custodianship of their data. Our Diligent Security Management System (ISMS) is ISO 27001:2013 certified and our cybersecurity framework is governed by the NIST Cyber Security Framework. Diligent has defined roles and responsibilities for operating the ISMS. The security department consists of more than a dozen security professionals focusing on Product Security, Security Operations, Computer Security Incident Response, and Risk and Compliance.

Diligent is fully committed to providing assurance of its security controls and practices through third-party certifications and audits, is ISO 27001:2013 certified and holds a SOC 2 Type 1 Report. Diligent ensures your data can be managed on a per-user and/or per-data room basis. This gives administrators on multiple levels complete control of who has access to what data, setting individuals' rights to content and processes based on the instance of the platform.

Diligent is undergoing ISO 27001 and SOC 2 Type 1 audit for Secure File Sharing (SFS), and we expect to receive the reports and certifications in Q2 2020. SFS as a product specifically has not received ISO 27001 certification or SOC 2 Type 1 audit reporting yet. However, Diligent's platform is currently ISO 27001 certified and receives SOC audit reports.

Members of Diligent's Security Team are active participants in the information security community in order to maintain up-to-date knowledge and expertise.

DATA HOSTING

Diligent owns and operates its own equipment, and the system is housed in world-class hosting data centers that are ISO 27001:2013 certified and that have appropriate SOC audit reports. Customers can choose the location in which they would like their data hosted; currently, the options are the United States, Canada, the United Kingdom, Germany or Australia.

DATA HOSTING (CONT.)

All our data centers provide physical, environmental, communications and access to security with the following controls in place:

- Intruder and door alarms with infrared detectors
- A fully monitored proximity/biometric access control system
- Heat and smoke detectors
- Local backup power generators
- External secure perimeter fencing with controlled access
- External and internal CCTV recording
- Airlock entry doors to the data center zone
- Equipment housed in cages leased to Diligent
- 24/7 onsite security presence
- Access is only granted if pre-booked by pre-authorized people
- Government-issued photo ID required for entry

DATA ENCRYPTION

Data rests on encrypted hard drives using AES 256-bit encryption. All data transmission between client and server (document upload and download, content display and synchronization) runs via HTTPS and provides client-dependent protection with 256-bit TLS V1.2 encryption.

APPLICATION ARCHITECTURE ELEMENTS

Encrypted storage and guarantee of data integrity: All documents are encrypted with 256-bit AES. The integrity of the encrypted data is ensured with AES-GCM.

Certificate pinning: In future, certificate pinning will enable clients and mobile apps to validate a server's customer certificate. This prevents man-in-the-middle attacks.

Firewall and load balancing: The load balancer and the firewall are exclusively managed by Diligent staff. The configuration of the firewall in front of the Diligent system is restricted and uses secure communications protocols. The minimum required includes:

- **HTTPS access:** All external data communication from the client to the server uses HTTPS.
- A network-based IDS (Intrusion Detection System) is positioned in front of external firewall clusters to detect and alert us to potential cyberattacks.

Secure operations management and provider shielding: No staff from Diligent or the data center have any access to document content.

Administrator shielding: IT Administrators on the customer side cannot access content, if not explicitly permissioned to do so like any other user in the organization.

Authentication of microservices: Diligent's Secure File Sharing and Meeting Workflow architecture is based on the microservice concept. This provides multiple benefits, including scalability and resilience. The microservices used in the solution can only access each other once they have authenticated themselves correctly.

Encapsulated user administration: Administrators cannot change critical user data such as email addresses and mobile numbers. This ensures that they cannot change a user account to give themselves access to the user's documents.

Monitoring/application monitoring: The system detects errors in microservices and restarts them automatically. The monitoring system ensures the solution is running correctly and alerts the operations team in an emergency.

Data backups: Various backups are carried out to ensure data availability:

- **System backup:** run daily. A system backup can only be used for a complete system recovery.
- **Database backup**: run continuously.

APPLICATION ACCESS CONTROLS

Two-factor authentication: Access to Diligent Secure File Sharing and Meeting Workflow application is protected by token-based authentication. The user is sent a one-time PIN by SMS or email. Alternatively, an authenticator app creates a temporary PIN (Time-based One-Time Password, or TOTP), which provides access to the platform.

Session timeouts: After 60 minutes of inactivity, the session closes down automatically in order to prevent attacks on an unattended computer.

Password security: Passwords must comprise at least eight characters and two of the following three attributes: upper- and lower-case letters, numbers and punctuation marks. Administrators are also able to define password policies, such as password strength, validity period and user lockout for five minutes after three failed access attempts. The rules set for password use also apply to passwords for access to protected links.

Single sign-on (SSO): A single sign-on facility is available for clients with the necessary infrastructure. This enables users to transparently log onto their Diligent Secure File Sharing and Meeting Workflow system as if it were located within their own environment. Diligent supports the industry standard SAML V2-based SSO

COMPLIANCE

Diligent has the following security-related audits and certifications applicable to the Diligent Secure File Sharing and Meeting Workflow service:

- **Sharing and Meeting Workflow service:** Diligent undergoes a SSAE 18 SOC audit annually. The data centers in which Diligent co-locates also undergo their own SSAE 18 SOC and/or ISO audits.
- **Certifications:** Diligent's Platform is ISO 27001:2013 certified. A copy of the certification is available upon request from your Sales or Customer Success Manager. Diligent is also Privacy Shield certified, demonstrating our EU-US & Swiss-US Privacy Shield Compliance.
- **External Security Testing:** Diligent contracts with respected third-party security firms to perform regular vulnerability scanning of the infrastructure, dynamic automated security scanning of the service, and network penetration testing.
- **Customization:** Diligent Boards offers various configurable options, such as data room storage, password complexity and flow transfer sites, to further ensure data security. Clients can set their security options based on evolving business needs or potential threats.

INCIDENT MANAGEMENT & RESPONSE

Taking the highest precautions: Diligent has a documented Security Incident Response Program in place to handle a security incident. Incident response procedures are updated at least annually. All incidents are managed by Diligent's Security Incident Response Team. Diligent classifies the event and determines the incident response process. In the event of a security breach, Diligent will promptly notify customers of any unauthorized access to customer data.