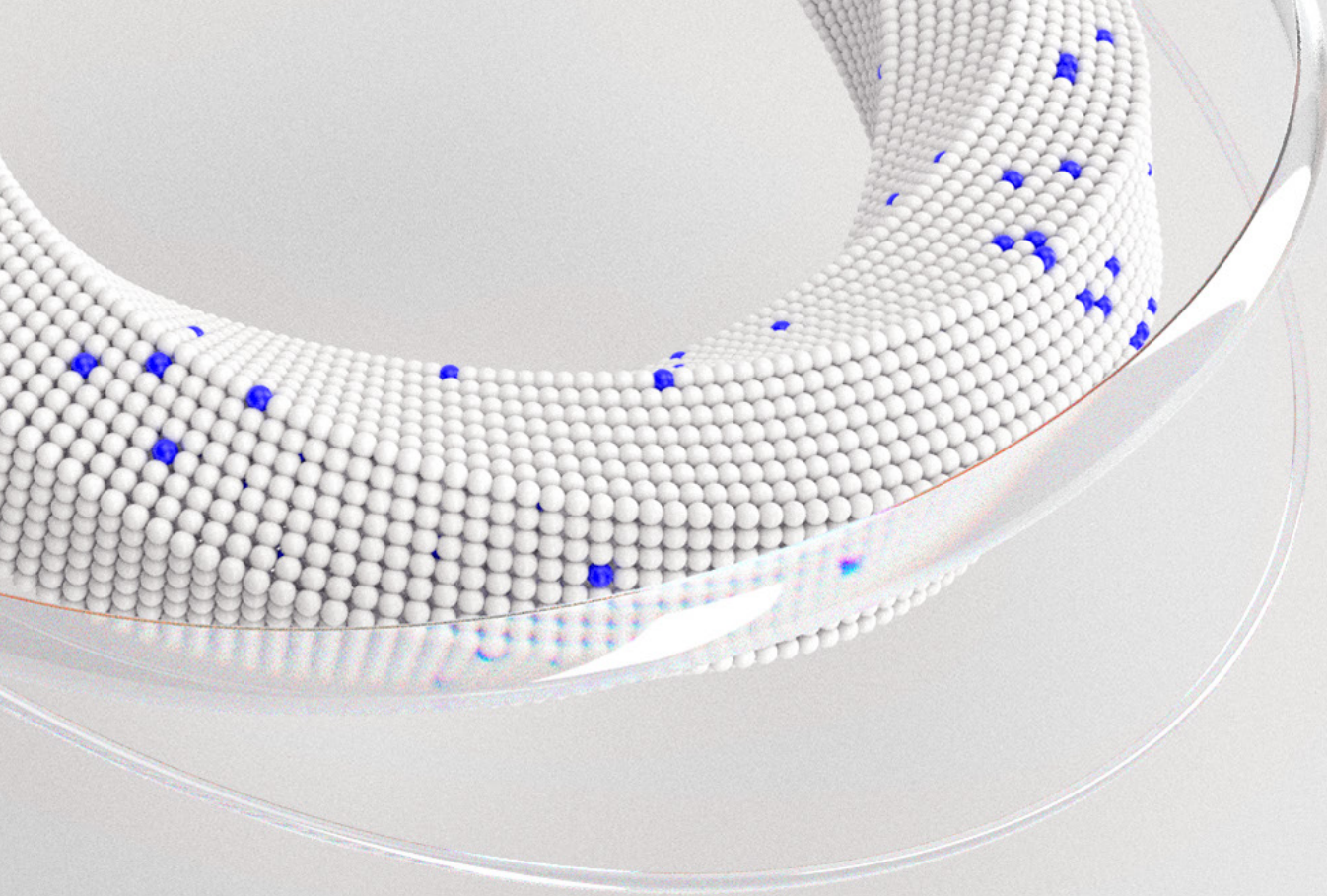




# Cyber Security in the Delfi Digital Platform

Securing your digital performance





---

The Delfi™ digital platform with leading security, innovation, and quality at its core.

# The digital platform for energy

The Delfi™ digital platform combines energy domain expertise with advanced artificial intelligence (AI) and digital technologies, in a secure, cloud-based software environment.

Open, scalable, and with 24/7 operational support, the Delfi platform brings you the world's best apps, data, AI, and physics-based science for exploration, development, drilling, production, and midstream, as well as new solutions for the energy transition—all delivered via a flexible and personalized SaaS subscription model.

Seamlessly connecting people, data, and leading software applications, the Delfi platform enables teams to collaborate more effectively, reduce cycle times, and innovate faster, to deliver significantly increased business performance.



## Continuously updated to counter new threats

The Delfi platform protects your operations from a wide variety of threats, including network breaches from unauthorized users, unapproved changes to operational procedures, malware, and computer viruses.

The platform is built using an agile secure development life cycle (SDL) and is continuously updated to account for new security threats. A wide range of embedded features are employed to provide unparalleled system and operational security, identity management, and network and data protection.

## Secure by design

Our multi-pronged approach to security development implements secure coding, security qualification, and tenant isolation. This embeds key security measures into the code and processes for each application in the Delfi platform.

## Security community and security culture

Security is a core attribute of SLB culture. This enables us to reinforce security of the Delfi platform with continuous training and awareness exercises, supported by our community of security experts and architects.

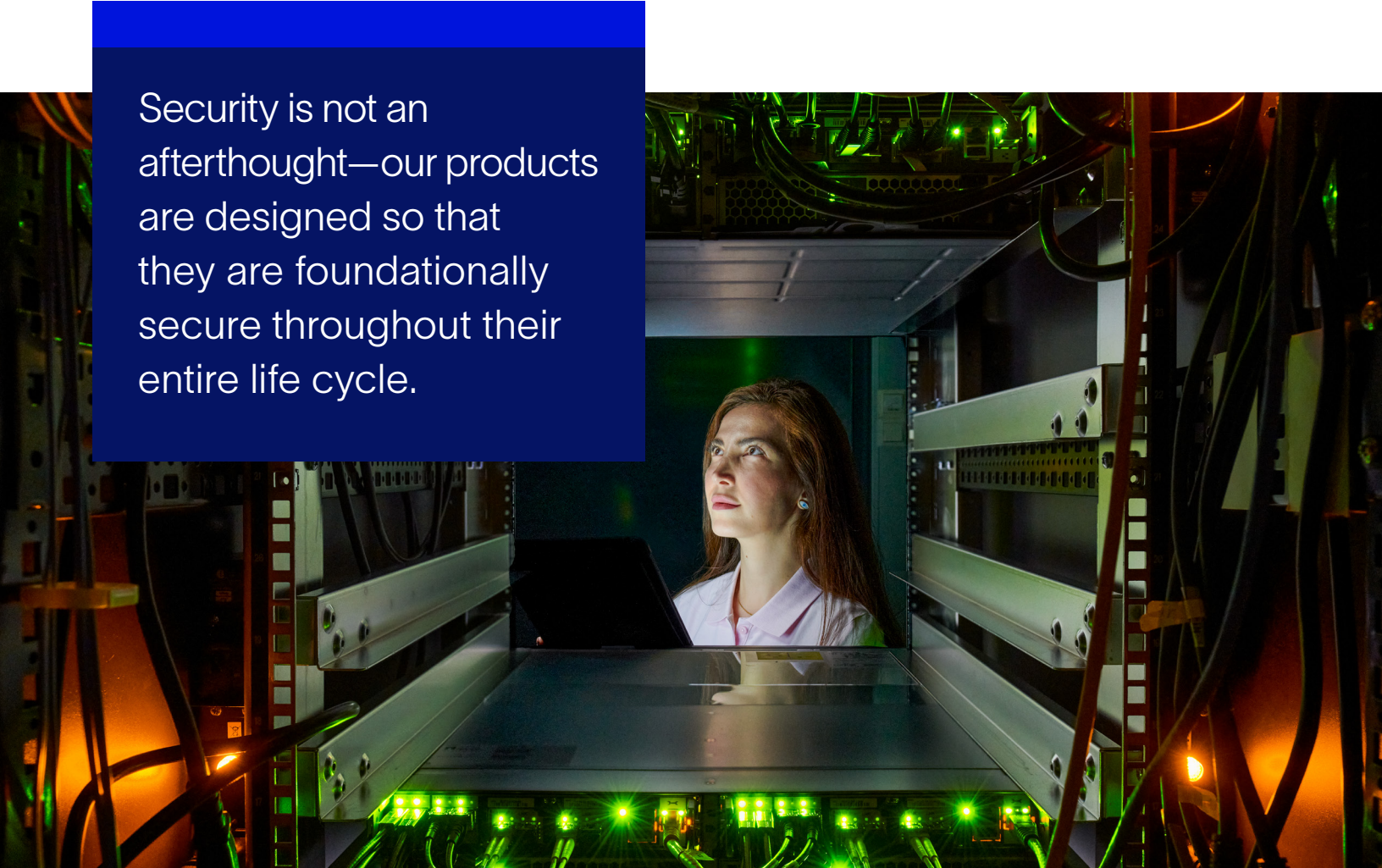
Security begins at the pre-employment stage. Our global hiring and recruitment standard is followed across SLB locations, with accommodation to local law requirements in various jurisdictions.

All SLB personnel are required to complete security training on IT security and customer data handling. Training records are captured and maintained, with periodic refresher training required to ensure that competency is up to date.

The SLB performance management process encompasses quarterly performance reviews, including a review of security training and reminders for compliance.

## Secure development life cycle

Requirements for the secure development (SDL) life cycle include secure architecture, secure coding, testing, and third-party validation at all stages.



Security is not an afterthought—our products are designed so that they are foundationally secure throughout their entire life cycle.

SLB has a comprehensive software development life cycle framework called software life cycle management (SLM). Secure development lifecycle (SDL) is fully embedded into SLM and includes the following practices:

- Security review of architecture documents, design documents, and threat model
- Static application security testing (SAST)
- Dynamic application security testing (DAST)
- Source code review for code quality and third-party vulnerabilities
- Penetration testing

### Tenant isolation

Tenant isolation helps us optimize utilization, maximize efficiency, and minimize cost. The Delfi platform achieves this by implementing logical isolation at the application layer, network layer, or data layer. Tenant isolation ensures that the data is not accessible across tenants.

### Zero-trust architecture

The Delfi platform has zero-trust architecture focused on modern identity, multifactor authentication, fine-grained access control, and strong data protection, to ensure only authorized users have access to the data they need at the precise moment they need it.

Automated development, security and operations (DevSecOps) platform with modern security tooling and dashboards identify, track, and remediate security issues.



### Security qualification

Security qualification is a process standard that checks the readiness of an application for deployment against the security standard. Application teams are expected to maintain compliance throughout development and are audited at certain development stages. If necessary, third-party security consultants are used to perform security validations.

### Unified identity

The Delfi platform leverages a centralized authentication service for customers to access services using a single set of credentials. Unified identity provides improved security and efficiency and a richer user experience.

### Identity and authentication

The digital platform supports single sign-on (SSO) with federated authentication to grant access, leveraging the customer's corporate credentials securely and



## Cyber Security in the Delfi Digital Platform

conveniently. We recommend that our customers opt for this mechanism because it enables them to have complete control of their identities. An alternative option is to register directly with the Delfi platform. Once registered, users can log in and access Delfi platform services. Both options support multifactor authentication to protect from credential theft.

### Self-service authorization

Customers control the access entitlements through their customer account. Authorized personnel can approve or reject requests to access subscriptions. Only users with an active subscription can access the Delfi platform.

## Secure in operations

Keeping your data safe with more than 20 years of internal investment, focused expertise, and key technology partners, we are constantly adapting with the rapid advancements of digital technology.

Your data is protected through physical security, endpoint protection and hardening, and is always encrypted in transit and at rest.

### Physical security

The cloud infrastructure for the Delfi digital platform is deployed on the Google Cloud Platform and Microsoft Azure. These cloud service providers (CSPs) have 24x7 staffed security at their facilities, fully redundant power backup systems, physical access controls, and digital surveillance systems. More information about the physical security of the Google Cloud Platform and Microsoft Azure is available on the Google and Microsoft websites.

### Network protection

Threats to the Delfi platform are mitigated with a multilayered approach to network security that keeps your data safe and accessible. Our approach focuses on perimeter protection and network segmentation to keep unauthorized users out and isolate threats.

### Perimeter protection

The Delfi platform has implemented industry-standard mechanisms to protect and monitor the network



perimeter. All services and resources are protected using firewall policies designed to allow only necessary network traffic and block all other traffic.

### Network segmentation

The network architecture of the Delfi platform is based on the principle of network segmentation. Various components of the environment are deployed in isolated network segments and only desired network traffic is allowed.

### System security

System security is the process of ensuring system integrity, confidentiality, and availability. It involves specific steps or measures to protect the system from threats, viruses, worms, malware, or remote hacker intrusions.

### Endpoint protection

The Delfi platform uses a range of security software to safeguard from malicious code. Antivirus, antimalware, and vulnerability monitoring agents are deployed on every server and virtual machine.

### Patch management

We follow industry standard practices for patch management. This ensures the latest versions of operating systems, software frameworks, and libraries are applied to the Delfi platform. Servers and virtual machines are deployed with validated patches and updates.

### Hardening

Every server and virtual machine is hardened and locked down by default. The Delfi platform uses the Center for Internet Security (CIS) benchmark for operating system hardening. For Delfi platform cloud infrastructure, our CSPs provide endpoint protection, patch management, and hardening.

### Data protection

Safeguards, including encryption and backup and restore processes, are in place at every stage of the data life cycle to protect and secure your data and mitigate data loss.

### Encryption

Customer data is always protected by end-to-end encryption (AES128 bit or better), both at rest and in transit. The Delfi platform uses key management solutions provided by our CSPs for encryption keys and other credentials.

### Backup and restore

Different backup and restore processes are used depending on the categorization of the data that needs protection. Some data categories use snapshots whereas others can be fully redeployed in case of a major failure. Encrypted backups are used for encrypted data.

Our CSPs run real-time data replication to ensure that your data is both backed up and available on redundant and geographically dispersed servers to enable fault tolerance.







## Operational security

Operational security comprises a comprehensive set of policies, standards, and controls to ensure secure delivery of service.

### Privileged access management

Privileged access is managed through a centralized privileged access management (PAM) tool. This enables SLB personnel to securely perform operational and support activities. All privileged access accounts are reported and reviewed regularly. All activities are recorded for audit purposes. The PAM process is based on the least privilege principle and provided in a just-in-time (JIT) fashion.

### Change management

SLB leverages the Information Technology Infrastructure Library (ITIL) framework for change management. Every change is evaluated, approved, and recorded in the change management system. Only authorized operations team members can execute a change, which is controlled and monitored by a change management system.

## Global 24x7 protection and monitoring

### Monitoring

Monitoring is built into each service in the Delfi platform. Different monitoring tools are used depending on the service and cloud service provider. Any service component that has log-on service is monitored for brute force attacks and other suspicious events, such as repeated failures to log onto accounts with elevated privileges.

## Threat intelligence and hunting

The platform leverages real-time global threat intelligence to identify potential threats or exploits before they happen, allowing timely resolution or mitigation.

### Alerts

Alerting tools are used to generate alerts of unusual or suspicious activity in the system. All alerts are serviced by a 24/7 team that processes and investigates each event. Alerts are processed in accordance with the appropriate incident management process for that service. This includes escalation as required to security specialists or escalation as a recognized cyberattack.

### Incident management

When an incident happens, we are ready. Our teams use practiced procedures to rapidly respond and mitigate incidents. All employees complete a controlled training plan that gives them the skills to handle incidents efficiently and professionally.

Continuous monitoring by our global Cyber Security Operations Centre is further enhanced with advanced AI and machine learning methods.

### Drills

Regular cyber security drills measure the readiness of support teams to manage incidents and validate security controls and processes. These drills are fully documented with root cause analyses, lessons learned, and improvement actions. Each drill is used as an opportunity to improve cyber security incident response processes.

Cyber security incident response teams are trained in managing a wide array of cyber security threats to mitigate risks to your data and get your operations back in business as soon as possible.

## Certified and compliant

Continuous benchmarking against established industry standards and best practices to remain a step ahead.

## Alignment with security best practices

Our processes align with globally recognized industry best practices, ensuring breadth and depth of product and data protection.

### SOC 2 Type 2 accreditation



Assertion, by an independent external auditor of the suitability and effectiveness of the controls that have been designed, developed, and implemented.

This ensures that all industry-standard practices are followed relative to the design suitability and operational effectiveness of the controls— giving you increased confidence in the security and availability of the Delfi platform.

SLB strives to achieve the SOC 2 Type 2 accreditation for Delfi applications as new services move to general commercial availability, a current list is in the SOC3 report available at:

[www.software.slb.com/delfi/security](http://www.software.slb.com/delfi/security)

### ITIL

ITIL is a widely accepted approach to IT service management. It contains a set of best practices describing processes, procedures, and functions for high-quality service delivery and management, and it is articulated around a life cycle, including service strategy, design, transition, operations, and continual service improvement. ITIL is the basis of the ISO/IEC 20000 standard.

The Delfi platform's operating processes are aligned with the ITIL framework and are supported by engineers who are ITIL certified. Operations and service management toolsets used by the SLB support organization are aligned with ITIL to provide consistent customer service with a strong focus on quality. SLB has more than 500 ITIL-certified professionals companywide.

### Cyber security risk program

We have a comprehensive global cyber security risk management (CSRM) program that is designed to identify, assess, manage, mitigate, and respond to information security risks. The program is based on industry best practices and standards, such as the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). We verify and drive improvements using an annual external maturity assessment of our CSRM against the NIST CSF.

### Penetration testing

Validation of the implementation of our security policies is regularly performed by independently qualified third parties.

### Partnership with wider industry engagement

We partner with leading cyber security companies and organizations leveraging best-in-class technologies and expertise.





## Securing your digital performance

[slb.com/Delfi](https://slb.com/Delfi)

