Gain valuable insight into the security of your Microsoft SQL Server environment by proactively diagnosing issues and risks, reviewing your results locally, and receiving continuous updates to best practice guidance.

**Key Benefits**
- Complete privacy in which the data remains at your facility
- Onsite delivery with a Microsoft accredited engineer
- Assessment results available with the offline client
- Reduce the likelihood of successful compromise, increase your security posture, prevent the costs which accompany a compromise
- Re-assess your environment to track progress
- Offline client tool license for one year
- Access to best practice updates for one year with an active Premier Support contract

**Overview**

The Offline Assessment for SQL Server Security is a proactive service delivered by a Microsoft accredited engineer to diagnose potential issues with the security of your SQL Server environment. This service is recommended for customers with high privacy restrictions and compliance processes in which the data must remain at their facilities. This service is available for a single server or failover cluster running SQL Server 2017, 2016, 2014, 2012, and SQL Server 2008/2008R2 instances. Windows Server 2008/R2, Windows Server 2012/R2, 2016, 2019 Failover Clusters or standalone server installations are supported.

**What is Offline Assessment?**

This is a streamline experience to enable you to assess your environment offline maintaining all data at your facility. The data is collected onsite allowing you to maintain privacy and run the assessment on your own schedule. A Microsoft accredited engineer while onsite will analyze the data, review the findings, provide recommendations, focus on knowledge transfer, and build a remediation plan with your staff and your Technical Account Manager (TAM).

**Practical Recommendations**

The Offline Assessment for SQL Security collects information on the key technology, people, and process areas in your environment and analyzes this information against best practices obtained from over thousands of customer assessments. Solutions for each of the issues are identified and articulated in the Technical Findings report. All critical and important issues are explained by the Microsoft accredited engineer and a remediation plan is provided as one of the key deliverables.
Offline Assessment

The key technology, people, and process areas in your SQL Server environment are analyzed against recommended security practices established from over thousands of customer assessments and from Microsoft guidance.

Key Focus Areas
- SPN
- Data Transmission
- Cluster
- Firewall
- Surface Area Configuration
- Active Directory
- Catalog Security
- Groups
- Agent
- Backups
- Size Limits
- Data Encryption
- Code Encryption
- Code Signing
- User Schema Separation
- CLR Security
- Dynamic SQL & Injection Attacks
- Operational Excellence

The Offline Assessment for SQL Server Security is performed via a series of both technical and non-technical components. The technical component of the engagement leverages automated data collection to gather in-depth information about the configuration of the SQL Server installations. In addition to the technical information gathering, structured interviews are performed with key teams involved in managing SQL Server and supporting infrastructures, are performed to identify gaps in process or governance that may also expose the installations to risk.

Deliverables Include
- Assessment tooling and access to an online portal to download updates
- Regular updates to best practice guidance
- Use of the tools for one year with an active Microsoft Premier Support contract
- Knowledge transfer of issues found
- Remediation plan
- Technical Findings report

For more information, visit: https://services.premier.microsoft.com

This datasheet was last updated July 1, 2019. To ensure you have the latest version of this datasheet, check here: https://go.microsoft.com/fwlink/?Linkid=619061