

ProTEQ MS

ProTEQ MS is a subscription based service that includes everything required to keep your information systems running smoothly – Whether on site or our iQloud Platform. ProTEQ MS provides around-the-clock monitoring to prevent and eliminate outages and/or other technical problems before they impact your business. ProTEQ MS includes unlimited, remote technical support to respond quickly to emergency issues and keep your team productive. ProTEQ MS leverages the experience, tools and expertise of our entire organization and aims it directly at your business objectives.

ProTEQ MS advantages over traditional IT services include:

- Direct Access to World Class Technology Strategists
- Proactive vs Reactive Problem Solving
- Immediate Technical Support
- Ongoing Preventive Maintenance
- Fixed Monthly Payments

What's included?

ProTEQ MS includes comprehensive 24/7 monitoring of all of your servers, PCs and network-based equipment. Your systems are continuously optimized and secured by performing daily, weekly and monthly maintenance.

Key ProTEQ MS components include:

- Real-Time Monitoring – Monitor all Windows Event Logs, network devices
- Asset Management - Complete hardware, software and user security audit
- Backup / Disaster Recovery – With SpinBAQ Virtualized Backup & Recovery
- Security Management – Remove and prevent security threats
- Patch Management – Install and manage all operating system updates



- Disk Defragmentation - Perform hard disk maintenance on a scheduled basis
- Unlimited Remote Tech Support - Direct access to our helpdesk for immediate support
- Executive Reports – Weekly, monthly and quarterly reports

How Does It Work?

ProTEQ MS remote agents monitor all of your servers, desktops and client side carrier/connectivity devices and systems in real-time providing our engineers with critical information when a failure has, or is about to occur. When a problem is discovered, our management software can resolve the problem automatically or notify us when further action is required. Our client support teams interact with client organizations, as required, diagnosing and resolving issues quickly without waiting for a technician to physically arrive on site.

ProTEQ MS Features

Desktop Management

Desktop management is a resource intensive and time consuming task. Desktop down time significantly impacts employee productivity and business revenue. ProTEQ MS is comprised of world class remote management and control software blended with proactive engineering and real-time help desk services.

- **Antivirus Monitoring**

ProTEQ MS provides antivirus software monitoring and detection. Every four hours ProTEQ MS performs a check to see if definitions are updated. Alerts are sent if definitions fall three (3) days behind. ProTEQ MS is also able to detect and managed many industry leading malware products.

- **Patch Management**

ProTEQ MS's patch deployment engine automatically deploys all Microsoft Security Patches and ProTEQ MS's white-listed Microsoft Patches. Microsoft Patch Assessments are scheduled and performed each week; comparing patches already deployed to the desktop with patches available from Microsoft. For the next five days, ProTEQ MS attempts to deploy the missing patches based on customized schedules developed with our clients.

Failed patch installs are reported to ProTEQ MS's Patch Master. Patch Master is an intelligent patch redeployment engine. Patch Master will attempt to redeploy failed patches based on the published schedule. Reports for both ProTEQ MS failed patching and Patch Master failed patching are available to our engineers for evaluation and remediation.

- **Malware Scanning**

Spybot is a separate, optional, component to ProTEQ MS. Scans are run on a static schedule or on an ad hoc basis as determined with our clients.

- **Temp File Cleanup**

ProTEQ MS performs weekly scheduled temp file removal. If left unchecked these folders can grow and cause low disk space errors or affect the paging file causing the computer to run slow.

- **S.M.A.R.T. Analysis**

ProTEQ MS is able to capture information provided by S.M.A.R.T. hard drives. S.M.A.R.T. alerts are vendor specific and usually report precursors to hardware failure.

- **Logical Disk Checks**

ProTEQ MS checks each logical disk on the Desktop to assure there is appropriate disk space available to assure systems performance and availability.

- **VIPRE Enterprise**

Sunbelt Software's VIPRE Enterprise antivirus protection is available for deployment with each installed ProTEQ MS agent as no additional charge.

Server Monitoring and Management

ProTEQ MS's IntelliQ monitoring system identifies a myriad of server problems by monitoring multiple server metrics and provides corresponding best practice resolution (BPR) recommendations. This solution driven monitoring system saves our engineers hundreds of hours normally invested monitoring, researching, and troubleshooting Server problems each month. As specific alerts are raised and escalated many issues are resolved in minutes not hours before the business is impacted because pre-engineered BPRs are already in place.

IntelliQ is constantly evolving with over 2500 specific monitors already in place. Support experiences and 'known issues' from sites around the world provide early warning capabilities to further eliminate impact causing outages.

Proactive Alerts

HALOTEQ help desk technicians and client management teams receive email and/or phone notifications for alerts that fall into one of the three critical alert families.

Alert families are predefined groups relating similar alerts together. For example, critical alerts that have an impact on a Server where users will notice the problem (e.g. Exchange service stopped) are Critical User Impact Alerts. These alerts are handled as the highest priority by our engineers in order to minimize the impact to client productivity.

Some critical alerts, however, can have an impact on a Server but the users do not immediately notice the problem (e.g. Exchange takes longer than normal to read from the hard disk). These Critical User Non-Impact Alerts can cause problems over time even though users are unaware they are occurring. Critical User Non-Impact Alerts still need resolution as a high priority, but can usually wait until the Critical User Impact Alerts have been resolved.

Backup Monitoring

Backups are no good if they don't work. ProTEQ MS monitors HALOTEQ's SpinBAQ Virtualized Backup and Recovery (VBR) appliance as well as Symantec Backup Exec (previously Veritas). ProTEQ MS backup monitoring software can analyze the log files to help determine the root cause of the backup failure. Failures are flagged immediately as "Failed yet to be analyzed" and an automatic analysis is conducted. Once the backup failure is analyzed the status updates to "Failed" and our engineers receive the analysis in order to fix the problem. even though users are unaware they are occurring. Critical User Non-Impact Alerts still need resolution as a high priority, but can usually wait until the Critical User Impact Alerts have been resolved.

Exchange Server Monitoring

ProTEQ MS Exchange Server Monitoring is for clients who run their own Exchange server instead of using HALOLINQ Unified Communication and Collaboration services. ProTEQ MS will send, on your configured schedule, emails to the client's Exchange Email Servers. The email's round trip is then analyzed by an Exchange specific IntelliQ monitor. The monitor also analyzes the server metrics for Exchange failures. Specific transaction alerts are raised when monitoring thresholds are exceeded. Additional services include several database maintenance tasks currently conducted by in house engineers.

Network Management and Monitoring

HALOTEQ provides network design services for all of our client's data and voice requirements. We work with all of the major network providers to assure our client's get the most reliable service available for the best value. Dealing with these vendors can be frustrating and time consuming. Our years of experience and in depth knowledge of network technology and specific provider capabilities as well as their organizations prove to be of tremendous value to our clients.

Once in place, all network devices are managed and monitored through the ProTEQ MS Portal. This is a "client side" network device monitoring feature designed to assess overall health and availability of the network. If problems arise, HALOTEQ engineers interface on the client's behalf with the network provider to develop and implement a solution as quickly as possible. Scheduled reports on the network are produced as desired by the client as well as 'event specific' reporting in the case of unplanned outages.

**Learn more about our approach and our solutions by contacting
a HALOTEQ Sales Representative:**

1.877.442.5633

email: sales@haloteq.com

website: www.haloteq.com