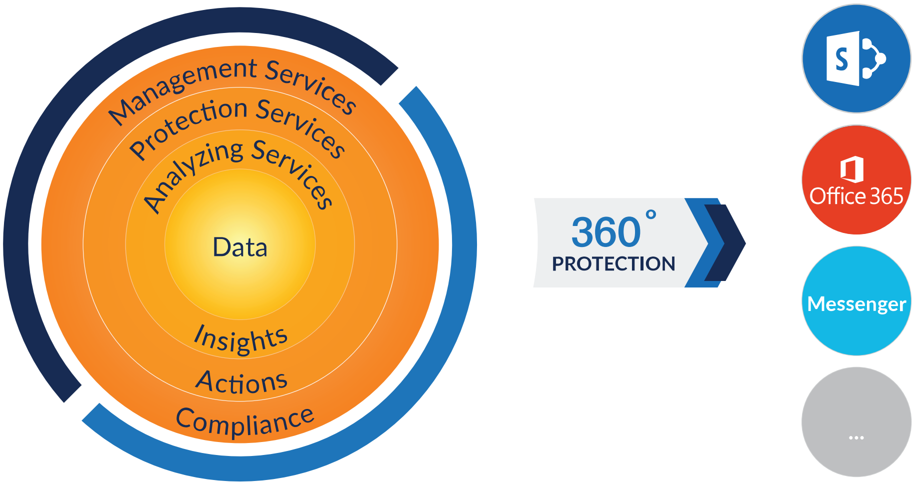
iQ.Suite 360

Centralized protection of collaboration and communication platforms

Communication and collaboration in companies are shifting more and more towards modern collaboration and meeting platforms and the requirements for the necessary security measurements are changing too. The increasing number of channels, more complex IT infrastructures and a majority of platforms running completely in the Cloud result in new gateways and attack vectors.

With iQ.Suite 360 we present you a modern Cloud solution that helps you to protect your collaboration and communication platforms from a central point in an easy and effective way. It is available as Cloud service so you are well protected against dynamic, always evolving threats. iQ.Suite 360 is the right solution for enterprise environments as well as for small companies.



The Highlights

- **One-Policy approach**
  Security policies can be configured once and then applied to all supported channels
- **360° protection**
  Secure communication and information exchange between own employees but also external communication partners
- **Simplicity first**
  Secure communication and information exchange between own employees but also external communication partners
- **Private Cloud version**
  In case of regulations or internal guidelines, iQ.Suite 360 can be operated on premise as well
- **Multitenancy**
  Enables the segregation of subsidiaries, legal entities, etc.
- **Attractive pricing model**
  Flexible, affordable and predictable payment for platform usage

iQ.Suite 360

Threat Protection for SharePoint

Multi-level malware protection for SharePoint

iQ.Suite 360 Threat Protection for SharePoint is a service of iQ.Suite 360, which enables companies to protect their SharePoint environment from malware in a compliant way and in line with Microsoft‘s recommendations

Relying on one scanning engine is risky, therefore we are introducing cascaded malware scanning mechanisms for reliable recognition and even greater protection.

Scanning files in real time can be time-consuming and cause delays in user operations, which leads to frustration and business interruption. Our asynchronous scanning allows users to quickly upload their files in SharePoint, which are then scanned and marked accordingly. Our scheduled scanning capability allows companies to perform complete SharePoint scans with the latest definitions, during non-peak hours of usage. Suspicious files can be placed in the iQ.Suite 360 quarantine for further investigation, rather than be blocked or deleted. All activities are logged and can easily be traced and reported on.

Malware
iQ.Suite 360
S

Features

- **Multi-level protection**
  Multi-layered threat protection from malicious files via the use of multiple scan engines from well-known premium vendors
- **Versioning**
  Full support of versioning document libraries to scan current and also older file versions and therefore maximize protection
- **Scheduled scanning**
  Scanning of the whole SharePoint environment with the latest malware definitions outside working hours
- **Auditing and reporting**
  Detailed and comprehensive auditing and reporting capabilities enable necessary insights on the security environment to meet the GDPR requirements