What security guidance does Microsoft provide?

02/11/2019 • 5 minutes to read • Contributors

In this article

Security guidance and tools

Microsoft introduced the Service Trust Platform and Compliance Manager to help with the following:

- Overcome compliance management challenges.
- Fulfill responsibilities of meeting regulatory requirements.
- Conduct self-service audits and risk assessments of enterprise cloud service utilization.

These tools are designed to help organizations meet complex compliance obligations and improve data protection capabilities when choosing and using Microsoft Cloud services.

Service Trust Platform (STP) provides in-depth information and tools to help meet your needs for using Microsoft Cloud services, including Azure, Office 365, Dynamics 365, and Windows. STP is a one-stop shop for security, regulatory, compliance, and privacy information related to the Microsoft Cloud. It is where we publish the information and resources needed to perform self-service risk assessments of cloud services and tools. STP was created to help track regulatory compliance activities within Azure, including:

- **Compliance Manager:** Compliance Manager, a workflow-based risk assessment tool in the Microsoft Service Trust Platform, enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft Cloud services, such as Office 365, Dynamics 365 and Azure. You can find more details in the next section.
- **Trust documents:** Currently there are three categories of guides that provide you with abundant resources to assess Microsoft Cloud; learn about Microsoft operations in security, compliance, and privacy; and help you act on improving your data protection capabilities. These include:
- **Audit reports:** Audit reports allow you to stay current on the latest privacy, security, and compliance-related information for Microsoft Cloud services. This includes ISO, SOC, FedRAMP and other audit reports, bridge letters, and materials related to independent third-party audits of Microsoft Cloud services such as Azure, Office 365, Dynamics 365, and others.
- **Data protection guides:** Data protection guides provide information about how Microsoft Cloud services protect your data, and how you can manage cloud data security and compliance for your organization. This includes deep-dive white papers that provide details on how Microsoft designs and operates cloud services, FAQs, reports of end-of-year security assessments, penetration test results, and guidance to help you conduct risk assessment and improve your data protection capabilities.
- **Azure security and compliance blueprint:** Blueprints provide resources to assist you in building and launching cloud-powered applications that help you comply with stringent regulations and standards. With more

certifications than any other cloud provider, you can have confidence deploying your critical workloads to Azure, with blueprints that include:
    - Industry-specific overview and guidance.
    - Customer responsibilities matrix.
    - Reference architectures with threat models.
    - Control implementation matrices.
    - Automation to deploy reference architectures.
    - Privacy resources: Documentation for Data Protection Impact Assessments, Data Subject Requests (DSRs), and Data Breach Notification is provided to incorporate into your own accountability program in support of the General Data Protection Regulation (GDPR).
- **Get started with GDPR:** Microsoft products and services help organizations meet GDPR requirements while collecting or processing personal data. STP is designed to give you information about the capabilities in Microsoft services that you can use to address specific requirements of the GDPR. The documentation can help your GDPR accountability and your understanding of technical and organizational measures. Documentation for Data Protection Impact Assessments, Data Subject Requests (DSRs), and Data Breach Notification is provided to incorporate into your own accountability program in support of the GDPR.
    - **Data subject requests:** The GDPR grants individuals (or data subjects) certain rights in connection with the processing of their personal data. This includes the right to correct inaccurate data, erase data, or restrict its processing, as well as receive their data and fulfill a request to transmit their data to another controller.
    - **Data breach:** The GDPR mandates notification requirements for data controllers and processors in the event of a breach of personal data. STP provides you with information about how Microsoft tries to prevent breaches in the first place, how Microsoft detects a breach, and how Microsoft will respond in the event of a breach and notify you as a data controller.
    - **Data protection impact assessment:** Microsoft helps controllers complete GDPR Data Protection Impact Assessments. The GDPR provides an in-exhaustive list of cases in which DPIAs must be carried out, such as automated processing for the purposes of profiling and similar activities; processing on a large scale of special categories of personal data, and systematic monitoring of a publicly accessible area on a large scale.
    - **Other resources:** In addition to tools guidance discussed in the above sections, STP also provides other resources including regional compliance, additional resources for the Security and Compliance Center, and frequently asked questions about the Service Trust Platform, Compliance Manager, and privacy/GDPR.
- **Regional compliance:** STP provides numerous compliance documents and guidance for Microsoft online services to meet compliance requirements for different regions including Czech Republic, Poland, and Romania.

Unique intelligent insights

As the volume and complexity of security signals grow, determining if those signals are credible threats, and then acting, takes far too long. Microsoft offers an unparalleled breadth of security intelligence delivered at cloud scale to help quickly detect and remediate threats.

Azure threat intelligence

By using the threat intelligence option available in Security Center, IT administrators can identify security threats against the environment. For example, they can identify whether a particular computer is part of a botnet. Computers can become nodes in a botnet when attackers illicitly install malware that secretly connects the computer to the command and control. Threat intelligence can also identify potential threats coming from underground communication channels, such as the dark web.

To build this threat intelligence, Security Center uses data that comes from multiple sources within Microsoft. Security Center uses this to identify potential threats against your environment. The Threat intelligence pane is composed of three major options:

- Detected threat types
- Threat origin

- Threat intelligence map

Machine learning in Azure Security Center

Azure Security Center deeply analyzes a wealth of data from a variety of Microsoft and partner solutions to help you achieve greater security. To take advantage of this data, the company use data science and machine learning for threat prevention, detection, and eventually investigation.

Broadly, Azure Machine Learning helps achieve two outcomes:

Next-generation detection

Attackers are increasingly automated and sophisticated. They use data science too. They reverse-engineer protections and build systems that support mutations in behavior. They masquerade their activities as noise, and learn quickly from mistakes. Machine learning helps us respond to these developments.

Simplified Security Baseline

Making effective security decisions is not easy. It requires security experience and expertise. While some large organizations have such experts on staff, many companies don't. Azure Machine Learning enables customers to benefit from the wisdom of other organizations when making security decisions.

Behavioral analytics

Behavioral analytics is a technique that analyzes and compares data to a collection of known patterns. However, these patterns are not simple signatures. They are determined through complex machine learning algorithms that are applied to massive data sets. They are also determined through careful analysis of malicious behaviors by expert analysts. Azure Security Center can use behavioral analytics to identify compromised resources based on analysis of virtual machine logs, virtual network device logs, fabric logs, crash dumps, and other sources.