Create secure financial forecasts with Cortana Intelligence Suite

Microsoft relies on financial forecasting to inform critical business decisions such as resource allocation, performance management, and inventory optimization. Like at many other organizations, financial forecasting at Microsoft was a resource-intensive, mostly manual process; forecasts were created in spreadsheets, and insights were based on a significant amount of human judgment. Microsoft IT worked with the finance and data sciences organizations to design and build a secure and automated forecasting solution based on machine learning that combines the best of human and machine intelligence by taking advantage of Cortana Intelligence Suite on Azure. The solution, used to forecast Microsoft revenue, provides accurate and automated forecasts as frequently as needed by the business—and financial leaders can judge data-driven baseline forecasts based on their business domain expertise.

The goal of this project was to securely configure an Azure financial forecasting solution and prove to ourselves and to our Finance leaders that the final Azure forecasting application was secure enough to host highly confidential data. We achieved success by partnering with the product teams and Finance to drive new security controls into the underlying services. Together, we deployed a secure, machine-learning forecasting application that is now an integral part of our financial planning and budgeting process.

—Bret Arsenault, Corporate Vice President and CISO, Microsoft

Moving financial forecasting to the cloud

Microsoft Azure has become the default environment for all Microsoft IT solutions—when we need to develop new solutions, we look to Azure first. Cloud solutions are easier to manage, scale to our needs, and can be developed without significant hardware investments. Like many of the other solutions that Microsoft relies on for critical business functions, financial forecasting involves working with sensitive data. Services in Azure can be securely configured to include our required security controls to protect sensitive and financial data.

Historically, financial analysts created data extracts and saved them on their local machines to produce forecasts. Storing sensitive data and forecast models on local devices can make it challenging to protect that data. Devices can be lost or stolen and are vulnerable to viruses and zero-day malware attacks. Moving these functions to the cloud greatly reduces risk and makes it easier for us to detect and respond to data leakage. There are fewer points of vulnerability, and data scientists and analysts can now work with Microsoft sales data using services from Cortana Intelligence Suite that protects data and monitors access.

The solution uses data from the currently on-premises Microsoft sales database and Azure Machine Learning, a cloud-based predictive analytics service, from Cortana Intelligence Suite. By moving to Azure Machine Learning, our data scientists can be more agile with their data modeling and experiments, and both our data scientists and financial analysts can now use the data visualizations in Power BI to extract useful insights.

By moving financial forecasting to the cloud, Microsoft financial analysts produce quicker, more frequent forecasts with consistent forecasting algorithms and less analyst bias by using automated data feeds pulled from the Microsoft sales database in Azure Machine Learning.

Assessing end-to-end security

As a prerequisite for moving our financial forecasting processes to the cloud, we needed to ensure end-to-end data protection. As we designed the financial forecast solution, we reviewed every component that could represent a potential risk.
Using the services in Cortana Intelligence Suite, we designed an end-to-end solution that could help protect data at rest and data in transit from unauthorized access or data leakage. We assessed the security of the data that is stored in the currently on-premises sales database, and then we looked at how the data was ingested into the cloud through scheduled jobs by using Azure Data Factory. We also looked at every step in the process, from building the machine learning data models using Azure Machine Learning, deploying the data models as web services, and the consumption of dashboards through Power BI.

Protecting highly confidential data

The Microsoft Information Security and Risk Management (ISRM) group evaluated the architecture and design of the solution. That evaluation included looking at all of the data involved and completing a threat model to identify vulnerabilities that could lead to inadvertent or premature disclosure. The ISRM group then specified the security controls required to protect the data and services that comprise the financial forecasting application. We went through an extensive process to deploy, validate, and test the prescribed security configurations. The evaluation helped provide the confidence that we could build cloud applications that are secure enough to host sensitive data such as financial information.

Within the system, we used encryption to protect the data stored (at rest) in the Azure SQL database and data in transit from the on-premises Microsoft sales database to Azure. We configured Azure SQL Database and Azure Storage Data Movement Library to encrypt data. We added several security controls to Azure Machine Learning, including encrypting data at rest in Azure Machine Learning workspaces. Technically, workspaces can be configured to use consumer email accounts to share data with external users. The information in our financial forecasting system is considered highly confidential, so we configured Azure Machine Learning workspaces to block access from consumer, or non-corporate, accounts.

Implementing user access roles and audit logs in Azure Resource Manager

We recreated all of our Azure services for this solution using Azure Resource Manager. Azure Resource Manager made it easy for us to implement user access roles security and audit access logs based on the support plans that we created. By using Azure Resource Manager, we can securely work with the resources in our financial forecasting solution in a group. It provides security, auditing, and tagging features that help us manage our Azure resources.

For information about using Azure Resource Manager to configure secure cloud solutions, see Security considerations for Azure Resource Manager.

Creating the financial forecasting solution

We used four main data and intelligence services in Azure to create our financial forecasting solution:

- Azure Data Factory
- Azure SQL Database
- Azure Machine Learning service
- Power BI
Financial forecasting solution architecture

Figure 1 shows a diagram of how these components work together in our financial forecasting solution.

Azure Data Factory

Azure Data Factory is the transport service that moves data from the currently on-premises sales database into the Azure SQL database, and back. It helps orchestrate, or build, analytic workflows in the cloud.

Azure Data Factory uses a data gateway service that’s installed on an on-premises server. The data gateway service copies the data from the currently on-premises sales database to the Azure SQL database. To protect the data, it was critical to ensure the security of both the gateway service and the physical database. We “hardened” the Windows Server that was hosting the gateway. We did this by installing all the latest security and feature updates and ensuring that the only accounts that could access the server were the accounts needed to operate and manage it. We configured Windows Update to install all updates monthly, and we have monitoring in place that scans for vulnerabilities and provides alerts to help us remediate potential issues.

Azure SQL Database

Data from the currently on-premises sales database is copied daily into the Azure SQL database. We enabled encryption for data at rest for the Azure SQL database using Transparent Data Encryption. Encryption helps protect the data from disk failure loss of disk. We also configured Azure SQL Database firewall rules to accept connections from only the data scientists’ client machines. This helps to ensure that the database has network-level protection in addition to user sign-in credentials.
Azure Machine Learning service

Azure Machine Learning offers a way to collaborate with other data scientists by sharing the workspace with fellow data scientists. Azure Machine Learning performs the predictive modeling, based on algorithms and stored trends. We’re using Azure Machine Learning encryption and have blocked the use of consumer email accounts for sign in, thereby allowing only users with a corporate email account to sign in. We created an encryption key in Azure Key Vault that’s backed by hardware security modules (HSMs). The Azure Key Vault offers both software-based keys and HSM keys. We used HSM-based keys because they provide a higher level of security. We also created an encrypted workspace in Azure Machine Learning, which encrypts the intermediate data, models, and other sensitive information during persistent storage of data.

We configured our Azure Machine Learning subscriptions so that signing in to workspaces requires multifactor authentication and workspaces can’t be shared to anyone without a corporate email address. Blocking the use of consumer accounts helps ensure that access is automatically managed through Azure Active Directory. When a user leaves the organization, their access to the solution is revoked as soon as their corporate credential are.

Power BI

We use Power BI to query and pull data into the primary user interface and into reporting dashboards. At Microsoft, we use data classifications to implement security controls for our business data. As you can imagine, much of the data used in the financial forecasting activities is classified as highly confidential. We have very strict policies and guidelines about how this type of data is transmitted, stored, and shared. When we started considering moving our financial forecasting processes to the cloud, Power BI wasn’t ready to protect data at a level that met our data standard for highly confidential data. We added built-in data classification controls or signals in Power BI to inform users that a dashboard they were viewing contained highly confidential data and should not be shared with others.

Improving the standard security offerings in Power BI

Now, the standard Power BI offering includes some of the main security enhancements that we require, such as:

- **Access controls.** We use multifactor authentication and conditional access for authentication to all of the services. We also configured Power BI to block the use of non-corporate email accounts and implemented row-level security with Power BI. Row-level security can be used to restrict data access for specified users. Filters restrict data at the row level and we can define filters within roles.

- **Encryption and key management.** Data is encrypted at rest and in transit. Encryption keys are stored only in approved key vaults.

- **Audit logs and forensics analysis.** Logs are stored in a central service that provides audit reporting and forensics analysis.

- **Data leak prevention.** We use data classification to signal users to be cautious when viewing and sharing sensitive data. In addition to row-level security, in Power BI we can also restrict sharing based on data classification level, and we have blocked non-corporate email accounts.

- **Secure gateways.** An on-premises data gateway provides the live connections between the currently on-premises sales database and the Azure SQL database. We use a Power BI enterprise gateway between the Power BI service and the Azure SQL database. Both gateways use service account credentials, and activities are logged, audited, and monitored for security events, including admin activity and direct queries.
Supporting services

We used a couple supporting security services to further protect the Azure financial forecasting solution, including:

- **Azure Key Vault service.** This is where secrets—such as encryption keys—are stored.
- **Azure Security Center.** This is the security monitoring service that provides alerts on misconfigurations and anomalous behaviors.

Best practices for moving highly confidential data to the cloud

Based on our experience in developing and testing our hybrid cloud financial forecasting solution, we developed a few best practices that might be useful to other organizations that are considering moving financial forecasting, or other sensitive data analytics solutions, to the cloud:

- **Don’t share too much; limit sharing to just enough.** Power BI creators can share a dashboard, report, or a content pack. Content packs include dashboards, reports, Excel workbooks, and datasets, and should be shared only with co-workers who require that much access. Dashboards that include sensitive information shouldn’t be broadly shared. We have documented guidance for dashboard owners to help them understand the configurations that signal users about information classification levels and provides sharing and handling guidance. Individual reports can be customized to share a read-only subset of data results.

- **Ensure that employees use strong passwords and multifactor authentication.** Administrative accounts should be used only on secured workstations, and users should not use the same password across multiple systems.

- **Communication before and during the transition.** It’s important to foster iterative communication with data stewards and owners throughout the process. Adoption of new tools can take a while—users are notorious for using what they know. Guidance and communication are key in reducing the amount of financial forecasting work that’s performed on local user machines.

Conclusion

Protecting financial data in our financial forecasting application required examining all of the services that comprise the Financial Forecasting application, starting with source database currently on-premises through our network gateways and into cloud services. Microsoft IT partnered with the finance and data sciences teams to deploy, validate, and test the ISRM-prescribed security configurations. Exhaustive testing helped instill a high level of confidence in the security controls of each service—and helped to affirm to our executive leadership that the solution would help keep sensitive financial information secure from cyberattacks.

An additional benefit from this partnership, our forecasting solution—which passed our security policy and compliance requirements—has become a reference architecture for other business groups at Microsoft that want to build secure analytics applications on Azure using Cortana Intelligence Suite.
For more information

**Microsoft IT**

[microsoft.com/itshowcase](http://microsoft.com/itshowcase)

*Using predictive analytics to improve financial forecasting*

*Using predictive analytics to improve sales processes and forecasting*

*Optimizing predictive analytics using Cortana Intelligence Suite on Azure*

*Cutting costs and improving service with Microsoft Dynamics CRM Online*

*Transforming our digital workplace with Office 365 Enterprise E5*

**Related content**

*Microsoft’s world-class finance organization digitally transforms forecasting with innovative machine learning solution*

*Introduction to machine learning in the cloud*

© 2017 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only: MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.