Microsoft

Microsoft Visual Studio Online Data Protection

October 2014

Contents

Overview

Microsoft Visual Studio Online (VSO) is a cloud-hosted application for your development projects, from planning through deployment. Based on the capabilities of Team Foundation Server, with additional cloud services, VSO manages your source code, work items, builds, tests and much more. VSO uses Microsoft Azure's Platform as a Service infrastructure and many of Azure's services, including Azure SQL databases, to deliver a reliable, globally available service for your development projects. Because important data is at stake, this white paper discusses the steps that Microsoft takes to keep your VSO projects safe, available, secure and private. In addition, it describes the role you play in keeping your VSO projects safe and secure.

This white paper is part of our effort to illuminate how we manage and protect your data and is intended for account administrators and IT professionals who manage their project assets on a daily basis. It will be most useful to individuals who are already familiar with VSO and want to know more about how Microsoft protects the assets that are stored in VSO.

Our commitment

Microsoft is committed to ensuring that your VSO projects remain safe and secure, without exception. When stored in VSO, your projects benefit from multiple layers of security and governance technologies, operational practices and compliance policies. We enforce data privacy and integrity both at rest and in transit.

As we look at the broader landscape of threats facing VSO customers, they boil down to four basic categories: data availability, service availability, service security and data privacy. We will investigate each of these categories to explore specific threats and explain what VSO does to address them through both the technology that we use and the way we put it into practice. However, we will first describe how data is stored and how VSO manages access to your data.

Because proper data protection also requires active engagement of customer administrators and users, we also discuss steps you should take to protect your project assets from unauthorized disclosure and tampering. Much of this has to do with being explicit about granting permissions to user access points in order to have confidence that only the right people are accessing data within your VSO.

Regardless of your approach, you should consider all data potentially "at risk" no matter where it is or how it is being used; this is true for both data in the cloud as well as data stored in a private datacenter. Thus, it is important to classify your data, its sensitivity / risk horizon and the damage it could do if it is compromised. You should also categorize your data relative to an overall information security management policy.

Built on Microsoft Azure

VSO uses many of the core Azure services including Compute, Storage, Networking, SQL Database, Identity and Access Management Services, Service Bus. This lets us focus on the unique aspects of running VSO while taking advantage of the state of the art capabilities, protection and industry certifications available from the Azure platform.

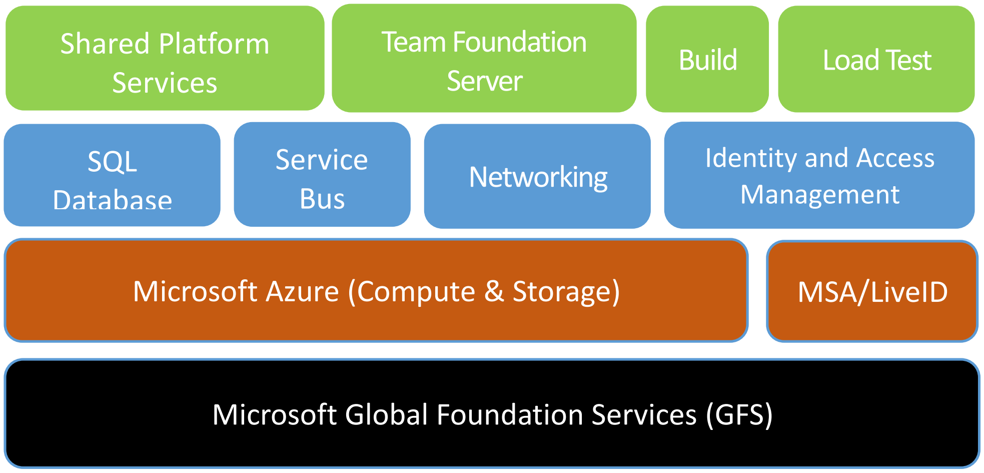

Shared Platform Services
Team Foundation Server
Build
Load Test
SQL Database
Service Bus
Networking
Identity and Access Management
Microsoft Azure (Compute & Storage)
MSA/LiveID
Microsoft Global Foundation Services (GFS)

Figure 1: High level Architecture Diagram of Visual Studio Online

VSO uses Azure Storage as the primary repository for service metadata and customer data. Depending on the type of data and the storage and retrieval needs, we use Azure Blob (binary large objects) storage and Azure SQL data storage. To provide a seamless experience, we work hard to abstract these details from the end user. However, to discuss the details surrounding VSO's approach to data protection, some background in these elements is important.

Azure Blob storage is generally used to store large chunks of unstructured data. All VSO projects use the Azure Blob storage service. This data includes potentially sensitive or private information such as the contents of source files and the attachments on work items. For most VSO projects, the majority of storage in use is this type of unstructured blob storage. For more information, see documentation on Azure Blob Storage.

Azure SQL database storage is used to store the structured and transactional aspects of your account, including project metadata, the versioned source control history, and work item details. Database storage gives you fast access to the important elements of your project and provides indexes into the blob storage to look up files and attachments. For more information, see documentation on Azure SQL Database.

Administrators can manage access to resources by granting or restricting permissions on user identities or groups. VSO uses federated authentication of user identities via Azure Active Directory (AAD) and Microsoft Account (MSA, formerly LiveID). During authentication, the user is routed to the authentication provider (AAD or MSA) where they provide their credentials. Once the authentication provider has verified the user's credentials, VSO issues an authentication cookie to the user, which allows them to remain authenticated against VSO. In this way, the user's credential information is never shared directly with VSO. For each VSO resource the user attempts to access, permissions are validated based on the user's explicit permissions as well as permissions inherited through group membership. Administrators can leverage access controls to protect access to account, team project collection, team project, and team scoped data and functionality, as well as to more specific assets like version control folders and work item area paths.

Data availability

Visual Studio Online leverages many of the Microsoft Azure storage features to ensure data availability in the case of hardware failure, service disruption or data center disasters. Additionally, the VSO team has procedures to protect data from accidental or malicious deletion.

Data redundancy

To protect data in the case of hardware or service failures, Microsoft Azure storage geo-replicates customer data between two locations within the same region that are hundreds of miles apart; for instance, between North and West Europe or between North and South United States. For Azure blobs, customer data is replicated three times within a single data center and is replicated asynchronously to a second data center hundreds of miles away. As such, Azure maintains the equivalent of six copies of your data at all times. This enables us to failover to a separate data center in the case of a major outage or disaster while also providing local redundancy for hardware failures within a data center. For Azure SQL database storage, daily backups are maintained offsite in the case of data center disasters.

Mistakes happen

To protect against accidental deletion of data either by our customers or by our operation team, we also take point-in-time backups of both the Azure blob and the SQL databases. In addition, we perform a "soft delete" for account deletion operations. This lets us recover entire accounts for up to 90 days after deletion.

Service availability

Ensuring that VSO is available for you to access your account and associated assets is of utmost importance to us.

DDoS protections

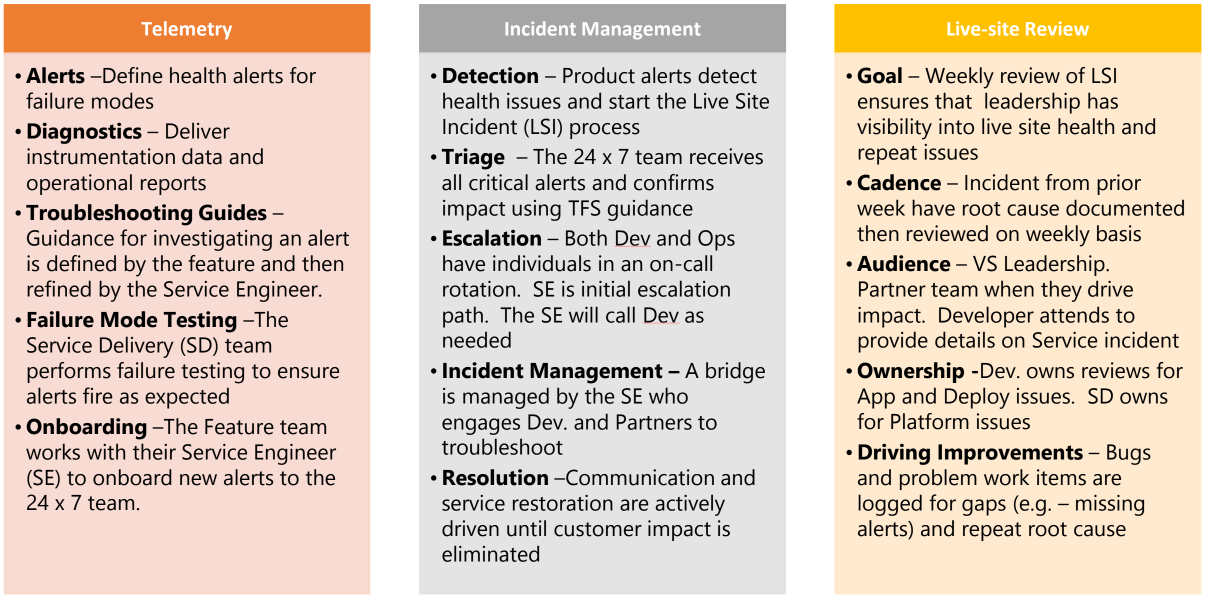
In some cases, a malicious distributed denial-of-service (DDoS) attack can affect service availability. Azure has a DDoS defense system that helps prevent attacks against our service. It uses standard detection and mitigation techniques such as SYN cookies, rate limiting and connection limits. The system is designed not only to withstand attacks from the outside but also from within Azure. For application-specific attacks that are able to penetrate the Azure defense systems, VSO establishes application and account level quotas and throttling to prevent any overuse of key service resources during an attack or accidental misuse of resources.

Live site response

While we strive for the service to be available 100% of the time, sometimes things happen that prevent us from meeting that goal. When that happens, we provide transparency to our users throughout the incident. Our 24x7 operations team is always on hand to rapidly identify the issue and to engage the necessary development team resources. Those resources then address the problem. They also aim to update the service status page and blog within minutes of detecting an issue that affects the service.

Once the team has addressed an issue, our “live-site incident” process continues as we identify the root cause of the issue and track the necessary changes to ensure we prevent similar issues in the future.

VSO’s live-site management processes are crafted to ensure a deep focus on service health and customer experience. Our processes minimize our time to detect, respond to and mitigate impacting issues. Ownership for Live-site is a shared across all engineering disciplines, so there are continual improvements that evolve out of direct experience. This means that monitoring, diagnostics, resiliency and quality assurance process are improved over time. Live-site management in VSO is broken into three distinct tracks as shown here:



Telemetry

- **Alerts** –Define health alerts for failure modes
- **Diagnostics** – Deliver instrumentation data and operational reports
- **Troubleshooting Guides** – Guidance for investigating an alert is defined by the feature and then refined by the Service Engineer.
- **Failure Mode Testing** –The Service Delivery (SD) team performs failure testing to ensure alerts fire as expected
- **Onboarding** –The Feature team works with their Service Engineer (SE) to onboard new alerts to the 24 x 7 team.

Incident Management

- **Detection** – Product alerts detect health issues and start the Live Site Incident (LSI) process
- **Triage** – The 24 x 7 team receives all critical alerts and confirms impact using TFS guidance
- **Escalation** – Both Dev and Ops have individuals in an on-call rotation. SE is initial escalation path. The SE will call Dev as needed
- **Incident Management –** A bridge is managed by the SE who engages Dev. and Partners to troubleshoot
- **Resolution** –Communication and service restoration are actively driven until customer impact is eliminated

Live-site Review

- **Goal** – Weekly review of LSI ensures that leadership has visibility into live site health and repeat issues
- **Cadence** – Incident from prior week have root cause documented then reviewed on weekly basis
- **Audience** – VS Leadership. Partner team when they drive impact. Developer attends to provide details on Service incident
- **Ownership** -Dev. owns reviews for App and Deploy issues. SD owns for Platform issues
- **Driving Improvements** – Bugs and problem work items are logged for gaps (e.g. – missing alerts) and repeat root cause

Figure 2: VSO Live-site Management Process

The operations team also monitors the availability metrics for individual accounts. These metrics provide insights into specific conditions that might affect only some of our customers. Investigations into this data can often result in targeted improvements to address customer-specific issues. In some cases, we will even contact the customer directly to understand their experience and work with them to improve the service from their vantage point.

We understand that availability of our service is an integral part of your team's success. Because of this, we publish a service level agreement (SLA) and provide a financial guarantee to ensure we meet this agreement each month. For more specifics on our SLA and financial guarantees, please see Visual Studio Online SLAs.

Of course, sometimes our partner teams or dependencies have incidents that affect VSO. All our partner teams follow similar approaches to identifying, resolving and learning from these service outages.

Service security

Ensuring a secure service requires constant vigilance, from proper design and coding techniques, all the way through to the way we operate the service. Along those lines, we actively invest in the prevention of security holes and in breach detection. In the event of a breach, we use security response plans to minimize data leakage, loss or corruption.

Secure by design

To implement industry best practices and stay on the forefront of information security, we engage various teams within Microsoft including Azure, Global Foundation Services (GFS) and Trustworthy Computing. Microsoft's Security Development Lifecycle (SDL) is at the core of our development process and Microsoft's Operational Security Assurance (OSA) program guides our cloud operation procedures. The SDL and OSA methodologies address security threats throughout the development process and operation of VSO services. They specify requirements that include threat modeling during service design, following design and code best practices, verifying security with standard tooling and testing, limiting access to operational and customer data, and gating rollout of new features through a rigid approval process.

Because the security landscape is continually changing, it is important for our team to keep current with the latest in best practices. Towards that end, we have annual training requirements for all engineers and operations personnel working on VSO. In addition, we sponsor informal "brownbag" meetings. These meetings are hosted by our own engineers. After they've solved an issue, they share what they've learned with the rest of the team.

A cloud service is only as secure as the host platform. VSO uses Azure's Platform as a Service (PaaS) offering for much of our infrastructure. PaaS automatically provides regular updates for known security vulnerabilities. When we host virtual machines in Azure using their Infrastructure as a Service (IaaS) offering–such as for our hosted build service—we regularly update those images to include the latest security patches available from Windows Update. The same update rigor applies for our on-premises machines, including those used for deployment, monitoring and reporting.

Our team conducts regular security-focused penetration testing of VSO. Using the same techniques and mechanisms as real malicious attackers, penetration testing tries to exploit the live production VSO services and infrastructure. The goal is to identify real-world vulnerabilities, configurations errors or other security gaps in a controlled process. The team reviews the results to identify other areas of improvement and to increase the quality of the preventative systems and training.

Restricting access

We maintain strict control over who has access to our production environment and customer data. Access is only granted at the level of least privilege required and only after proper justifications are provided and verified. If a team member needs access to resolve an urgent issue or deploy a configuration change, they must apply for "just in time" access to the production service. Access is revoked as soon as the situation is resolved. Access requests and approvals are tracked and monitored in a separate system. All access to the system is correlated against these approvals and if unapproved access is detected, an alert is raised for the operations team to investigate.

If the username and password for one of our developers or operation staff were ever stolen, data is still protected because we use two-factor authentication for all remote system access. This means that additional authentication checks via smart card or phone call to a pre-approved number must take place before any remote access to the service is permitted.

In addition, secrets that we use to manage and maintain the service, such as RDP passwords, SSL certificates and encryption keys are managed, stored, and transmitted securely through the Azure Management Portal. Any access to these secrets requires specific permission, which is logged and recorded in a secure manner. All secrets are rotated on a regular cadence and can be rotated on-demand in the case of a security event.

The VSO operations team uses hardened administrator workstations to manage the service. These machines run a minimal number of applications and operate in a logically segmented environment. Operations team members must provide specific credentials with two-factor authentication to access the workstations and all access is monitored and securely logged. To isolate the service from outside tampering, applications such as Outlook and Office, which are often targets of spear-phishing and other types of attacks, are not permitted in this environment.

Intrusion protection & response

To ensure data is not intercepted or modified while in transit between you and VSO services, we encrypt via HTTPS / SSL. In addition, Azure encrypts all connections to Azure Storage and SQL databases to protect the integrity of the data.

To ensure that activities within the service are legitimate as well as to detect breaches or attempted breaches, we leverage Azure's infrastructure to log and monitor key aspects of the service. In addition, all deployment and administrator activities are securely logged, as is operator access to production storage. Real-time alerts are raised because the log information is automatically analyzed to uncover potentially malicious or unauthorized behavior.

In the case where a possible intrusion has been detected or high priority security vulnerability has been identified, we have a clear security incident response plan. This plan outlines responsible parties, steps required to secure customer data, and how to engage with security experts in Microsoft Security Response Center (MSRC), Global Foundation Services (GFS), Azure and members of the VSO leadership team. We will also notify any account owners if we believe their data was disclosed or corrupted so that they can take appropriate steps to remedy the situation.

Data privacy

We want you to have confidence that your data is being handled appropriately and for legitimate uses. Part of that assurance involves appropriately restricting usage so that your data is used only for legitimate reasons.

Law enforcement access

In some cases, third parties such as law enforcement entities may approach us to obtain access to customer data stored within VSO. By policy, we will attempt to redirect the requests to the account owner for resolution. When we are compelled by court order to disclose customer data to a third party, we will make a reasonable effort to notify the account owner in advance unless we are legally prohibited from doing so.

Some customers require that their data be stored in a particular geographic location to ensure a specific legal jurisdiction for any law enforcement activities. At this time, VSO can host accounts in data centers in either the United States or the European Union regions. All customer data such as source code, work items and test results as well as the geo-redundant mirrors and offsite backups are maintained within the selected region.

Microsoft access

From time to time, Microsoft employees need to obtain access to customer data stored within VSO. As a precaution, all employees who have or may ever have access to customer data must pass a background check, which verifies previous employment and criminal convictions. In addition, we permit access to the production systems only when there's a live site incident or other approved maintenance activity, which is logged and monitored.

Since not all data within our system is treated the same, data is classified to distinguish between customer data (what you upload to VSO), account data (information used when signing up for or administering your account) and Microsoft data (information required for or collected through the operation of the service). Based on the classification we control usage scenarios, geolocation requirements, access restrictions and retention requirements.

Microsoft promotional use

From time to time, we want to contact customers to let them know about additional features and services that might be useful to them. Since not all customers want to be contacted about these offers, we allow you to opt-in and opt-out of marketing email communications. We never use customer data to target specific offers for specific users or accounts. Instead, we leverage account data and aggregate usage statistics at the VSO account level to determine groups of accounts that should receive specific offers.

Building confidence

In addition to these protections, we have also taken steps outside of the service itself to help you decide to move forward with VSO. These include Microsoft's own internal adoption policies, the level of transparency that we provide into the state of our service, and our progress towards receiving certification of our information security management systems. All of these efforts are designed to build your confidence in the VSO service.

Internal adoption

Teams across Microsoft have begun adopting VSO internally. In fact, parts of the VSO team have been using the service for the past 3 ½ years, long before it was a commercial service. In addition, over the past six months, all of the VSO teams have on-boarded to the service. More broadly, we have established guidelines to enable the adoption plans for other teams. Obviously large teams move more gradually than smaller ones, given their investments in existing application lifecycle management systems. For teams that can move more quickly, we have established a project classification approach. It assesses our risk tolerance, based on project characteristics, to determine if the project is appropriate for VSO. Not all internal projects should use VSO. Projects that, if disclosed, modified or destroyed would result in severe loss to Microsoft, our shareholders, partners or customers, should not use VSO. Additional requirements for internal projects include associating the account with the Microsoft.com Azure Active Directory to ensure proper user account lifecycle and password complexity along with enabling the use of two-factor authentication for more sensitive projects.

Transparency

We are convinced that transparency around how we design and operate our service is critical to establishing trust with our customers. This white paper is part of our effort to shed light on how we manage and protect your data. In addition, we maintain a blog that provides real time updates whenever a service disruption, planned or unplanned, takes place so you can adjust your activities as needed. Furthermore, Brian Harry, the corporate vice-president in charge of VSO, maintains a very active blog addressing, among other things, lessons learned by operating the service.

Certification

Finally, for some customers, it is important to understand third-party evaluation of our data security procedures. Towards that end, we are in the final stages of the audit process for ISO 27001:2013 certification. We expect that process to complete by the end of 2014. The audit materials will be available upon request.

Steps you can take

Proper data protection requires active engagement of customer administrators and users. Your project data stored within VSO is only as secure as the end user access points. So it is important to match the level of permission strictness and granularity for those accounts with the level of sensitivity of your project.

Classify your data

The first step is to classify your data based on its sensitivity / risk horizon, and the damage it could do if it is compromised. Many enterprises have existing classification methods that can be reused when projects move to VSO. Refer to these materials for more information on how to classify your data.

Adopt Azure Active Directory

Another action you can take to improve the security of end user logins is to use Azure Active Directory (AAD) instead of Microsoft Accounts (MSA) to manage your organization's access to VSO. This allows your IT department to manage various aspects of the end user's access including password complexity, password refreshes and expiration if the user leaves your organization. Through Active Directory federation, you can directly link Azure Active Directory to your organization's central directory so you have only one location to manage these details for your enterprise. Here is a brief comparison between MSA and AAD characteristics relative to VSO access:

Properties	MSA	AAD
Identity creator	User	Organization
Single user name / password for all work assets	No	Yes
Password lifetime & complexity control	User	Organization
VSO account membership limits	Any MSA	Organization's directory
Traceable identity	No	Yes
Account & IP ownership	Unclear	Organization
2-factor authentication enrollment	User	Organization

You can learn more about how to configure this support for your VSO account here.

Require two-factor authentication

In some cases, you might want to restrict access to your VSO account by requiring more than one factor to sign in. AAD lets you require multiple factors, such as phone authentication in addition to a username and password, for all authentication requests. You can learn more about turning on multifactor authentication for AAD here.

Use BitLocker

For sensitive projects, we also recommend use of BitLocker on your Windows laptop or desktop computer. BitLocker encrypts the entire drive on which Windows and your data reside, keeping everything safe. Once BitLocker is enabled, it will automatically encrypt any file you save on that drive. If your laptop or desktop machine were to fall into the wrong hands, BitLocker prevents unauthorized access of local copies of data from your VSO projects.

Additional resources

In addition to this white paper, there are other resources available for your review and education. These include:

- Visual Studio Online home page
- VSO service status
- Developer Services privacy statement
- Developer Services Agreement
- Brian Harry's blog
- Azure trust center
- Microsoft Security Development Lifecycle