Protecting SAP S/4HANA data on Azure at Microsoft

At Microsoft, we recently migrated the enterprise’s SAP environment to Microsoft Azure, as part of our planned transition from SAP ECC 6.0 to the new SAP S/4HANA platform. We’re already gaining the numerous business and operational benefits that Azure cloud infrastructure affords—and seeing cost savings, too. Moving SAP, our longstanding enterprise resource planning (ERP) solution, onto Azure also marked the beginning of another new chapter: an expanded partnership with SAP. This collaboration enables customers to accelerate their business transformation with S/4HANA on Azure by leveraging SAP’s managed services and our robust Azure cloud infrastructure.

The future solution for SAP on Azure represents an exciting milestone for Microsoft and SAP. It also presents security challenges and opportunities because of the complexity of managing critical enterprise solutions. We’re taking this opportunity to design new capabilities and controls to protect our systems and data. We’re also enhancing existing compliance processes and creating new ones to meet our ever-changing obligations. This multifaceted initiative provides an ideal platform for us to use while showcasing the modern engineering approach that we’re developing at Microsoft.

Our goal is to create an optimal integrated cloud security and compliance strategy for hosting the more complex, configurable, and user-accessible SAP S/4HANA solution. Our strategy focuses on protecting Microsoft assets and data in a high-profile environment, while streamlining compliance with existing regulations such as Sarbanes-Oxley (SOX) and new ones such as the General Data Protection Regulation (GDPR).

Our S/4HANA security-redesign initiative is underway and incorporates the robust Microsoft enterprise-security framework and principles that we have developed over time. It also leverages the Azure-specific security framework that has positioned Azure as a cloud services leader, and it will incorporate the security tools and technology that SAP and its partners have developed. Furthermore, we will integrate industry best practices in every facet of the security infrastructure that we build for S/4HANA on Azure. This allows us to be agile, efficient, and provide scalability in our SAP environment.

Current SAP security structure at Microsoft

The current Microsoft SAP security design, developed over the past two decades, has been expanded and improved to meet our needs as our SAP-data footprint has grown. Like many large enterprise organizations, we use the SAP solution to run most of our business operations. Today, our SAP environment includes approximately 600 application servers and is our largest internal application running on Azure, supporting approximately 10,000 business users. Managing security and privacy has become increasingly more challenging, because of the sheer size of our SAP environment and the ever-evolving risk environment.

For Microsoft and other enterprises that are moving operations to cloud services and continually implementing technologies that expand user capabilities, security (cybersecurity in particular) is a chief concern. Mitigating those concerns is the driving factor behind the multifaceted approach that we’re taking in designing our future SAP security infrastructure and privacy capabilities.

S/4HANA framework future state: security and compliance by design

The transition to SAP S/4HANA gives Microsoft an ideal opportunity to modernize and streamline our overall security and governance, risk management, privacy, and compliance capabilities so that we can address current and future needs, and challenges as they arise. Our approach is to build and enhance security and compliance, by design, into
the entire SAP S/4HANA solution. At every step in the process, our Business, Compliance, Audit, Engineering/IT operations, and design teams have been working together with our product groups to ensure that the standards and processes we develop are seamlessly and effectively integrated into the final framework. This differs from the traditional approach that many enterprises use, which entails first developing products and then adding security layers or controls to the finished product.

In addition to incorporating Azure’s inherent security structure—Azure is already an industry leader in this realm and has more certifications than any other cloud provider—our future framework will feature a highly integrated compliance solution. We also plan to better use our technology capabilities and include automation wherever feasible. We will automate the following areas (and others as we identify them):

- Access request and provisioning
- Patch management and deployment
- Incident reporting and response
- High-risk data-access control and alerting

Because S/4HANA introduces new functionality, we are also using this opportunity to redesign SAP application security and interface authorizations and ensure that we deploy single sign-on (SSO) utilizing Azure Active Directory (Azure AD) across all systems and applications. The modernized authorization framework better aligns with our overall organizational structure. Additionally, it simplifies the S/4HANA user experience and provides us with more flexibility and scalability to adapt to changes and growth within Microsoft.

Although we’ll keep many of our traditional application-level security concepts in the future system, the new infrastructure must accommodate the additional complexities of S/4HANA database access as SAP interface options and user capabilities expand. These interfaces include Fiori Gateway, mobile devices, and the S4 application layer. Changing business practices, such as direct user database access and new cybersecurity risk vectors, also pose challenges in database security for all enterprises. We’ll accommodate this evolving environment with the design of our future-state SAP security and compliance framework.

The key driver of our SAP-on-Azure security strategy is ensuring that we create a highly flexible, scalable, and automated environment built on top of the Azure platform. Other objectives include:

- Tightly integrating security and controls, including patch management, real-time threat detection, and granular user-access and authorization controls.
- Utilizing new tools and capabilities, such as Microsoft Power BI and Azure AI, to enhance our reporting, controls automation, and security monitoring.
- Re-envisioning and redesigning security roles to help ensure data security and corporate-asset protection while mitigating risks.
- Ensuring that the Microsoft compliance teams play an integral role in driving security, privacy, and compliance across the future S/4HANA platform and in designing change-management functions.
- Reducing maintenance costs and ensuring greater consistency in our governance model through change-control automation.
Security and compliance drive design at each level

Our new S4/HANA security and compliance framework will apply the stringent enterprise security and compliance principles that underpin all Microsoft operations and activities. At every level, we’ll build advanced security controls and capabilities into the solution that we design and the proactive protection and monitoring systems that SAP incorporates into S4/HANA. These include the current Azure platform, the SUSE Linux operating system, the HANA database, the S4 application layer, the Fiori Gateway, and cybersecurity components.
Figure 2: The current Microsoft SAP environment and the future-state environment we’re developing to accommodate ever-changing security and compliance needs, and to help ensure risk mitigation

Azure

At the Azure level, the security framework will utilize our inherent industry-leading controls and capabilities, including Key Vault, Security Center, Azure AD, and Azure Advanced Threat Protection (Azure ATP). Azure also provides application and database security via web application firewalls (WAFs) and network security by using virtual networks. These capabilities help ensure data security and encryption at all points.

Security monitoring and threat detection are critical to Microsoft’s SAP security strategy. We will use Azure’s inherent logging and monitoring capabilities to provide Microsoft security services’ real-time visibility into the environment. We’ll also deploy Azure AI and machine learning to provide threat detection and event analysis. Today, we spend about $1 billion annually on Azure cloud security, to ensure that the enterprise-grade security and privacy protections we develop extend to our customers, which include many of the world’s largest financial institutions.

SAP

Building on Azure’s scalable and secure enterprise architecture, we’ll deploy the SUSE Linux operating system (OS). SUSE Linux’s inherent features including native malware protection and other features are designed to help secure SAP HANA. We will also apply our own Microsoft standard OS-level controls, including patch-management and OS hardening.

Additionally, we’ll apply standard database controls to the HANA database, in line with other databases in the Microsoft environment. However, unlike traditional databases, HANA is an in-memory columnar database that moves the calculation logic from the application layer to the database layer. End users may need direct access to the database to view reporting data, which is a deviation from legacy reporting and analytical processes and tools.

To facilitate end-user access to the database layer, HANA provides a role-based access architecture to deploy privileges to the user base. HANA creates or utilizes these privileges to restrict actions that specific users can perform in the HANA database and the data that they can view through reports.
The Fiori Gateway user interface (UI) introduces additional capabilities enabling user access via web or mobile devices. The ability to access SAP via the Fiori UI requires that we redesign our Microsoft SAP user-authorization model and processes to accommodate the new S/4HANA UI and help ensure that users are able to perform only the activities for which they are authorized.

As part of the S/4HANA deployment, we’ll redesign our SAP security role strategy to achieve a simple, business-friendly role design that enhances security and compliance, lowers maintenance costs, and helps Microsoft scale and adapt security as our environment changes.

Cybersecurity

Cybersecurity is another key component that Microsoft will address in the S/4HANA-on-Azure platform by using the key components of AI and automation. We have a comprehensive, end-to-end program strategy that incorporates sophisticated code-scanning capabilities, threat and vulnerability management, standards-based authorization design and development, and system hardening. This will help ensure that we meet all Microsoft network security standards.

Leveraging Microsoft best practices

Our future-state SAP security platform’s design will adhere to the Microsoft industry-recognized security principles and best practices that we use throughout the enterprise to drive risk identification and mitigation. Using analytics and automation, we’ll use these security principles in all operational and user-access domains and areas. Security principles range from information protection, platform health, and identity management, to data telemetry and monitoring. We’ll perform continuous risk management by using Azure security and compliance solutions and SAP’s governance, risk, and compliance (GRC) structures for application-access provisioning and control.

Since we began designing our future-state SAP security and compliance framework in November 2017, we have discovered new ways to leverage our existing capabilities and technologies. We’ve also identified novel approaches to improving collaboration among our own IT and product teams, and between Microsoft and SAP. Examples include:

• Integrating with Azure Active Directory to enable SSO.
• Leveraging the power of HANA and Power BI to provide rich data analytics and visualization.

Working in partnership with SAP, we’re designing a future-state SAP security and compliance structure for the SAP-on-Azure environment by using industry-leading technologies and practices, and security-by-design principles. When our comprehensive redesign is complete, we’re confident that our framework of integrated systems, tight controls, and monitoring technologies will help address and mitigate current and emerging risks. As leaders in developing enterprise software, Microsoft and SAP are collaborating closely to provide the preferred foundation for enabling a safe and trusted path to digital transformation for other enterprises.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Hello Azure: Unpacking how Microsoft moved its SAP workload to the cloud
Strategies for migrating SAP systems to Microsoft Azure
Optimizing SAP for Azure
Building an agile and trusted SAP environment on Microsoft Azure
Streamlining business processes with SAP connectors and Azure services
Azure Trust Center compliance offerings
Create your Azure free account today

© 2018 Microsoft Corporation. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.