Using App Service Environment v3 in Compliance-Oriented Industries
Using App Service Environment v3 in Compliance-Oriented Industries

Table of Contents

1  Summary
2  The Challenge: How Can Regulated Organizations Leverage Cloud-Based Platforms?
3  What is an Azure App Service Environment?
4  Key Criteria for App Service Environment v3 in Compliance-Oriented Organizations
5  Use Cases And Scenarios
6  Delivery Considerations
7  Impact on Stakeholders of App Service Environment Adoption
8  Conclusion: Start With KPIs and the End in Mind
9  About Michael Delzer
10 About GigaOm
11 Copyright
1. Summary

Today's organizations are looking to cloud-based platforms to deliver on their goals of digital-first customer experiences, technology-based innovation, scalability and operational efficiency. However, regulated industries such as finance, insurance, and healthcare have found themselves between a rock and a hard place. Historically, cloud-based environments have lacked the compliance-oriented capabilities they need, unless they were architected and orchestrated from scratch. As a result, compliance-oriented organizations are stuck with technically inferior, inflexible, yet compliant on-premises solutions.

The latest iteration of Microsoft's Azure App Service Environment (v3), includes capabilities that make it worth considering for such scenarios. App Service Environment (ASE) follows a Platform as a Service (PaaS) approach, offering comprehensive application and service frameworks upon which engineers can build application business logic. Unlike multi-tenant implementations of PaaS, App Service Environment consists of a single tenant instance through which customer traffic and cloud management traffic operate on separate virtual networks, with compute instances dedicated to customers.

This approach is particularly compelling for regulated industries. With App Service Environment v3, organizations can operate cloud-based services within a protected, policy-based environment. In addition, it offers a managed application ecosystem that separates operation and lifecycle management from application traffic. Consequently, cloud-based services can be operated and managed in the same way as in-house applications running behind the corporate firewall.

ASE v3 allows compliance-oriented verticals to fully leverage cloud-based services. They can deploy and manage applications at lower cost and with less technical know-how, unleashing the potential of cloud-based applications and opening the door to digital transformation. Outside of regulated industries, any business with large-scale corporate policies also can gain the agility and scalability of cloud-based services without losing control or risking non-compliance.

In this report, prepared for CIOs, CTOs, CISOs, chief architects and VPs of Engineering, we consider what Microsoft's App Service Environment offering looks like in practice. We outline the key needs of compliance-oriented scenarios, looking at how the platform’s capabilities map onto these needs. Based on these scenarios, along with end-user research, we map out lessons and strategies for making the most of App Service Environment v3 in the compliance context.

In conclusion, we determine that App Service Environment v3 does indeed offer a way forward for
regulated organizations as they look to embrace the digital transformation benefits that the cloud can bring.
2. The Challenge: How Can Regulated Organizations Leverage Cloud-Based Platforms?

Ever since virtualization was introduced into the data center, issues of workload isolation, security and regulatory compliance have created tension between IT staff building technical solutions and auditors ensuring that both the letter and the spirit of regulations is being followed. Zooming in on data privacy as an example, challenges often come from aligning policies and practices where different systems connect to each other, requiring that data is protected, available and used appropriately across both the systems and their interconnect.

Understandably, compliance-centric and risk-averse organizations have chosen to minimize such interfaces, keeping as much data and processing as possible within the protected walls of the organization. Today, it is still commonplace to run Tier 1 and regulatory applications in virtualized environments in data centers, and the idea of using third-party-hosted, cloud-based solutions has been too much of a hurdle to overcome. Consequently, compliance-based organizations have not taken advantage of cloud-based models or the agility benefits they bring.

Over recent years, we have seen Hyperscalers and cloud ecosystem players aiming to address such concerns. Examples such as geographical zoning, micro segmented networking, and row-level encryption all serve to deliver components of a solution, but what has been lacking is a single platform that offers such capabilities “out of the box.” As a result, the bar has remained too high: organizations faced with the costs of building a cloud-based solution versus the costs of sticking with an existing application have not found sufficiently compelling reasons to change.

**App Service Environment** v3 addresses this need by offering a highly scalable, yet isolated platform in a dedicated environment. Such environments enable organizations to benefit from cloud-based application services just as a cloud-native organization would, and yet still maintain a compliant, risk-managed profile without the operational overheads of implementing a custom solution. In later sections, we look at how App Service Environment v3 addresses these needs, but first we describe what the platform is and what it delivers.
3. What is an Azure App Service Environment?

App Service Environment fits in the overall category of cloud-based, managed PaaS hosting, which is a rapidly maturing cloud infrastructure category. Microsoft offers two versions of its PaaS offering:

- Azure App Service is a multi-tenant PaaS environment for building, deploying, and scaling web apps and APIs.
- Azure App Service Environment is the premium, single-tenant variation of Azure App Service, on which to deploy enterprise applications for compliance-oriented organizations.

App Service Environment v3 offers an application-agnostic, curated development experience. While we break out elements that are different from earlier versions below, we can summarize them by stating that App Service Environment v3 encapsulates all network traffic and services within an isolated environment unit (Figure 1).

![Figure 1. Differences Between ASE v3 and ASE v2](source | link)

Other key improvements in App Service v3 relative to previous versions include:
In the context of more general migration of applications to the cloud, we can consider the following features of App Service Environment v3 to be **Table Stakes**:

### Common Application and Infrastructure Services
Common services like web services, networking/load balancing, and cloud administration allow each enterprise to leverage the many features of Azure for its applications while enabling operational management, application observability, and situational awareness. The platform supports multiple application types and runtimes across Java, .NET, NodeJS, Python and PHP. Note that other PaaS offerings (for example, those based on Cloud Foundry) have a narrower offering of programming and supported applications.

### Support for Virtualization and Containerization
App Service Environment v3 supports both Windows and Linux, on both virtualized and container-based architectures. Support for virtualization and containerization give engineering teams a migration path from on-premises installations towards cloud-native application architectures. Similarly, Azure Functions and Azure Logic Apps, which can be leveraged also in cloud-native app patterns, are supported as well.

### De Facto Security Capabilities
Common security services like intrusion detection, instruction prevention, authentication, authorization, and auditing are incorporated in the Azure and Azure App Service platform, and these can be extended to offer more comprehensive functionality.

### Integrated and Transparent Networking
Past iterations of PaaS (including previous versions of App Service Environment) have required underlying networks to be configured and managed. With App Service Environment v3, infrastructure
maintenance traffic has been moved out of the customer’s network, so network configurations do not need to be coordinated between the client and Azure.

Overall, App Service Environment v3 provides a lower operational cost than hosting on-premises without the capital costs or need to pre-stage capacity for peak loads. It enables customers to focus on application functionality without worrying about monitoring, patch management, or version management of operating systems and application languages. There’s also a clear separation of duties that frees developers and operations (DevOps) staff to focus on their business application needs.
4. Key Criteria for App Service Environment v3 in Compliance-Oriented Organizations

Azure App Service Environment v3 brings some specific features for compliance-oriented organizations. Key criteria include:

- Compliance-oriented functionality and architecture.
- Compliance-oriented build and migrate.
- Compliance-oriented operations.

Compliance-Oriented Functionality and Architecture

- **Single-tenant model:** App Service Environment v3 (as well as previous versions) operates in a single-tenant model in which each customer’s workloads are run in isolation from others. Management and networking (customer traffic) are kept separate also. This includes the ability to scale on demand and release capacity safely.

- **Separation of management concerns:** App Service Environment provides a management plane used by Azure to maintain its PaaS features, with a separate application plane where only application traffic and control/compliance rules specific to the business application are applied. Management traffic is isolated as well, meaning that App Service Environment mitigates the risk of a “day zero” vulnerability being used to hop between tenants.

- **More advanced security features:** The App Service Environment operates as a black box, enabling security by making traffic inaccessible to monitoring or access by humans. Beyond this protection, the platform also offers custom settings to further configure security parameters, such as:
  - Enable end-to-end encryption of data.
  - Manage TLS settings by application, or disable all inbound TLS 1.0 and TLS 1.1 traffic.
  - Control and limit encryption ciphers, for example, to limit the encryption protocols in use by SSL.

- **Integrate other services:** Beyond basic security metrics and features, teams can upscale to more comprehensive security metrics and services without having to make any changes to deployed
applications. App Service Environment integrates with Microsoft services such as Azure Active Directory and Microsoft Defender, as well as with third-party security identity and access control services.

Compliance-Oriented Build and Migrate

- **Isolated pipeline support**: As a design paradigm, App Service Environment provides a stable and secure location for integration with CI/CD pipelines and the applications they support. This support can include cloud-provided tools or customer-provided CI/CD tools. Alternatively, it can enable those tools located elsewhere to deploy and maintain application code in the App Service Environment.

- **Declarative Services**: App Service Environment supports a fully API-driven declarative approach to requesting and releasing services. This means that service definitions, requests, and dependencies can be defined and assessed for compliance up front, rather than being buried within application code.

- **Geographic deployment**: App Service Environment incorporates the ability to deliver applications to multiple locations around the world, offering Availability Zones with geographical locations, based on specific criteria and policies.

Compliance-Oriented Operations

- **Policy-based operations**: Organizations can operate cloud-based services within a protected and policy-based environment. This means that cloud-based services can be operated and managed as if they were in-house applications running behind the corporate firewall.

- **Operational isolation**: A managed application ecosystem separates operation and lifecycle management from application traffic. This reduces the time and costs to maintain the security and DNS configurations needed for regulatory compliance and high-security standards.

- **Risk-aware Operations**: Management of networking, scaling, and support for availability zones are simplified—making response to systems failure or security breaches, business continuity, and disaster recovery easier.

- **Audit-compliant reporting**: Companies can enable the creation of audit-compliant reports on demand or on a schedule.
Overall, App Service Environment not only incorporates the features required to support compliance-based workloads, but it also makes the tasks of migrating, building, operating, and maintaining applications more straightforward for engineers working in compliance-oriented organizations. The platform makes it easier for Azure customers to sidestep routine labor, testing/patching, interoperability, and compliance practices that keep an environment sound. In addition, by creating a secure, single-tenant experience that is fully integrated with other Azure features, customers can leverage a secure and stable managed PaaS environment for compliance-oriented workloads while still being able to host other parts of their IT needs elsewhere in Azure.

Further, because the platform supports a range of deployment types and frameworks, companies can relocate a broader set of security-sensitive workloads to a single-tenant PaaS solution. The arrangement provides build-your-own software stacks while allowing customers to subscribe to one of the many supported stacks supported by Azure.
5. Use Cases And Scenarios

What are the typical scenarios that will compel an organization to migrate to App Service Environment v3? From conversations with end-user organizations, we can consider security, IT transitions, and workload management as the main scenarios. Note that it is not currently likely that an organization might migrate an application to the cloud for compliance reasons alone, although this may become the case as platforms such as App Service Environment v3 are adopted. Given that App Service Environment v3 can host applications in a way that is as (or more) secure than applications hosted on-premises, this may justify the effort of migrating on-premises workloads to a single-tenant PaaS like App Service Environment.

Security
Common use cases for App Service Environment deployment arise when security requirements, content sensitivity, or other compliance needs justify using a single-tenant offering over the multi-tenant Azure App Service. For many companies, five-year, fully burdened costs of maintaining a secure hosting environment, with fully tested and supported software components, will be lower using App Service Environment v3 than hosting on-premises.

As visibility increases for financial aspects of cloud use (as explored in current thinking around FinOps and Value Stream Management (VSM)), the value of using App Service Environment v3 becomes a straightforward option for business needs with high governance, or regulatory and compliance requirements. As a relevant KPI, you can look to measure audit report coverage for all regulator audit controls. The TCO of compliance reporting should be lower when using the App Service Environments v3 than for v2 or for on-premises, with a target savings of 20%.

IT Transitions
App Service Environment v3 provides a neutral place to host applications while offloading operations workloads to Azure. This makes it applicable wherever a secure, neutral environment may be beneficial, for example when multiple business units, or whole companies, need to work jointly on a project on a temporary or permanent basis. For example, consider cases in which highly sensitive applications need to be developed with minimal disruption to existing business units, development of a PoC in partnership with a third party is called for, or corporate M&A activities are launched. As shown in Figure 2, ASE v3 enables both companies to leverage the same independent, secure environment: this can exist only for as long as it is needed, with no lasting impacts on IT operations for either side. The KPI for this is again audit, plus contractual coverage. Typically, TCO is significantly lower because space and up-front costs are removed: workspace costs are dictated by on-demand usage for longer-term, transient or ephemeral secure workspaces. M&A tasks present a very good...
use case because clean environments can be created without risks of errors in network or security traffic controls exposing either company’s networks.

**Figure 2. Application Service Environment v3 enables merging companies to share information in a secure environment**

**Workload Management**
Many businesses may find that IT staff are overloaded and cannot take on the extra workload to support the software stack in secure and stable operations. In those instances, when the governance mandates and audit compliance are not fully known and the risk of re-deploying an application to a new on-premises secure environment is not acceptable to the business, the cost of the App Service Environment may be lower than the customer’s fully burdened costs to host applications. This typically occurs in greenfield applications where regulatory requirements may not yet be fully documented, but the need to deliver fast justifies the cost of using App Service Environment as a risk mitigation option. The KPI for this is again audit compliance and ease of reporting. The total cost of ownership (TCO) of creating and bursting into App Service Environments v3 is lower because the startup costs and CapEx purchases reduce to zero, as do risks of over- or under-funding the initial build-out. In addition, decommissioning costs become nominal, and are linked mostly to clerical and project management activity.
6. Delivery Considerations

What do organizations need to plan for, when considering a move to App Service Environment v3? The skill threshold is lower than on-premises applications, though effort is required around security, operations, audit metrics, alerts, and reports. Even here, however, the standardized method of delivery makes integration with enterprise tooling easier and more stable than it is for the custom-built solutions typically used on-premises.

Components in App Service Environment v3 are already monitored, tested, and audit compliant, so the business can focus on the business application and its code. This reduces the communication and integration aspects of project management and on-going operations. Moving forward, a business can address the following considerations, as a deployment progresses through its phases.

Moving an application from on-premises to App Service Environment v3 will require the following:

- Cleanup by IT and compliance staff to update systems of record and reporting once the project is complete. This technical debt is independent of the use of App Service Environment v3 but will have to be completed at the end of the migration.

- If the application uses components already supported by App Service Environment v3, developers see a change only in the configuration of the continuous deployment pipeline. If an application is currently running on unsupported platforms with known security vulnerabilities, an upgrade process can be tested using App Service Environment v3 to minimize change to the legacy production environment.

- The staff that needs some level of access to the App Service Environment will need to be configured with the correct access settings.

While waiting for App Service Environment subscription terms to be finalized between Azure and the customer’s legal and vendor management teams, and connectivity to be established between existing and on-premises systems (e.g. via VPNs), plan on the following:

- A company can make a short list of quick wins, whereby smaller applications currently using PaaS-supported components and versions are identified, and business units can be engaged about the value of the effort to ensure the initial projects are well supported.

- IT systems are often the first candidates to move over, with IT as the business unit. This is a good
point at which to work out change management and other internal process issues before engaging with another business unit.

Once a subscription is in place and connectivity established, a company can do the following in the next 30 days:

- Start to onboard the short list identified above and capture lessons learned to be applied to future projects
- The architects and IT leaders who identify the short list should now evaluate the next group of applications to move forward while keeping extra work on security and operations staff low so as not to cause a bottleneck or awareness risk
- As these applications do not require anything more than minor DNS and security or network routing changes, they can be moved over quickly and completed within 30 days.

For regulated organizations considering a Proof of Concept (PoC), the single-tenant aspect of App Service Environment v3 comes into play, minimizing the risk of data leakage or compromise that can occur in development environments that typically host PoCs. For regulatory or sensitive data, the cost to create a secure environment for a temporary PoC use is often unacceptable to the business. Since App Service Environments can be created and deleted easily, organizations can build temporary PoC environments using App Service Environment v3, then tear these environments down when they’re no longer needed. Once a PoC is completed, a hosted production pilot environment that will evolve in capability over time can be created.

The next 30 days should involve moving the next group of applications. Recognize that over time, easy applications will be completed and more complex or older applications can be tackled. These generally require more time and testing because software version updates may require code changes.

When the organization does not yet have 60 days of experience in moving applications, early lessons learned can serve as a guide to identifying the easiest applications to move next. The amount of time needed to upgrade them to compliant and fully patched software may dictate iterative deployments.

In various situations, a temporary ASE may be required, for example:

- To mock up a **safe testing environment** for these applications that require more work to get the
application using only fully patched and supported software products.

- For destructive testing in which data recovery processes can be tested and automated. The ability to use cloud services may speed up or change the process for data protection and recovery.

- As a clean way to conduct performance testing so the applications being tested don’t become noisy neighbors to other applications in the production App Service Environment location.

As use of App Service Environment v3 expands, an organization can grow its environment while still working within a single-tenant experience and with a level of control and the isolation that the tenant expects. App Service Environment is a single tenant environment on a public cloud ecosystem, so customers have greater control over traffic to third parties than traditional on-premises networking would allow, enabling scale without sacrificing compliance.

Imagine, for example, a new product order pipeline, which can start with one set of vendors and customers in a pilot and grow as the project matures. Increases in network traffic are addressed easily by the public cloud provider. This automatic scaling up removes the need to obtain the kinds of dedicated circuits or VPN tunnels that might be required for on-premises projects.
7. Impact on Stakeholders of App Service Environment Adoption

Like all PaaS solutions, App Service Environment simplifies the process of deploying applications by removing tedious and labor-intensive tasks that impair application delivery speed and have a negative impact on application uptime. It helps to understand the value that various stakeholder groups in the organization stand to gain from a deployment, both in compliance-related areas and the broader organization.

**Business Units Requiring Secure Hosting**
App Service Environment provides an environment that supports the regulatory and governance compliance needs of business units at a lower price point than on-premises models and with known and predictable costs that can be easily linked back to business value delivered. This new transparency removes the black hole of costs that can’t be traced to business requirements of value delivered. The process provides businesses with a secure, stable, and audit-compliant environment they can trust when requesting funding and setting up budgets.

**Risk Management and Governance Team**
The platform is designed to support compliance needs and quickly generate on-demand or scheduled compliance reports that auditors require. Further, it eliminates the risk of PaaS-supported components being out of compliance and creates a design pattern that can support disaster recovery testing and the ability to automate fail-over when the authorized request is made (typically, an officer of a company must authorize a disaster recovery process).

**Developer and DevOps Team**
The result of this support for compliance, reporting, and recovery is a consistent working environment that can be programmatically created, providing high value to cloud environments. Customers benefit from the certainty of knowing that all components used in App Service Environment v3 are the current and most secure versions of code and that all integration between PaaS components has been resolved by the Azure platform. This certainty allows DevOps teams to focus on business code and functionality.

**Operations Team**
App Service Environment v3 provides a known and trusted feed of operational metrics at a lower price point than can be achieved on-premises. These metrics can be used to create application observability solutions that reflect an accurate view of an application even years after its initial
development, and despite two-week release cycles that steadily add to application complexity.

**Security or (Dev)SecOps Team**

This audit-compliant, single-tenant, and well-instrumented hosting environment exceeds what many companies can achieve with on premises solutions and does it with a faster time to market using an OpEx payment model.
8. Conclusion: Start With KPIs and the End in Mind

Together with the multi-tenant Azure App Service, App Service Environment v3 can be seen as the latest generation of Azure’s PaaS offering, reducing overheads of building and managing the services required by modern, digital-first applications. We have learned how the platform extends these principles to applications in compliance-oriented organizations. The benefit is the same: reduced operational overheads, meaning application teams can get on with solving business problems, rather than dealing with infrastructure complexity. In regulated scenarios, this time savings offers distinct advantages to those who choose to embrace it.

Such a shift requires careful strategy, planning and execution. It is important to set out expectations and measurable benefits up front: we would propose adopting measurable Key Performance Indicators (KPIs) such as the following:

- **Performance**: What is your level of performance today and how are you measuring it? After moving to the cloud, this should be equal or greater than you have today, unless you had over-provisioned on-premises capacity, in which case you may see savings by right-sizing the environment to meet the business needs without excessive capacity.

- **Total Cost of Ownership (TCO)**: What are your fully burdened costs, and what costs are you not able to calculate or map to specific business requirements? After moving to the cloud, TCO should be equal or lower for the same level of performance and security. Note: if software or security issues were not addressed on-premises, correcting them and using supported products may be more expensive. However, you will have addressed audit compliance issues that may not have been exposed before.

- **Time to Market**: How long does it take for a regulatory or highly sensitive application to be deployed for the first time without infrastructure security vulnerabilities? How much time does it take to get a set of VMs created and added to security and audit systems to prove PCI compliance? Post migration, this time should be measured in less than a day, assuming the application is allowed to be fully automated once change control releases the request.

- **Time to Scale Capacity**: While some on-premises environments can easily add a few VMs, large increases in capacity typically require CapEx or changes to hardware or software contracts. In contrast, App Service Environment v3 leverages the cloud and can scale easily, while addressing management/maintenance requirements for capacity.

While acknowledging the financial implications of moving to cloud-based models, IT and business unit
leaders should agree on the need to move to an OpEx hosting approach that does not compromise security or performance guarantees. Over a five-year period, TCO will be consistent and predictable. In highly mature IT environments, these costs may turn out to be lower. However, most companies are likely to find the fully burdened cost to host even non-secure or highly regulated applications to be lower using App Service Environment.

Customers should view this offering as a strategic element of the hosted environment, unlocking the ability to migrate all legacy applications – both tightly regulated and less so – to the cloud. Acceptance of this strategy goes hand in hand with a commitment to migrate all legacy applications over time: only in this way can organizations, regulated and otherwise, derive the benefits from cloud-based models they are looking for. Anything else inevitably results in a compromise in which costs are duplicated across old and new models, creating overheads that are as untenable as they are unnecessary.
9. About Michael Delzer

Michael Delzer is a global leader with extensive and varied experience in technology. He spent 15 years as American Airlines’ Chief Infrastructure Architecture Engineer, and delivers competitive advantages to companies ranging from start-ups to Fortune 100 corporations by leveraging market insights and accurate trend projections. He excels in identifying technology trends and providing holistic solutions, which results in passionate support of vision objectives by business stakeholders and IT staff. Michael has received a gold medal from the American Institute of Architects.

Michael has deep industry experience and wide-ranging knowledge of what’s needed to build IT solutions that optimize for value and speed while enabling innovation. He has been building and operating data centers for over 20 years, and completed audits in over 1,000 data centers in North America and Europe. He currently advises startups in green data center technologies.
10. About GigaOm

GigaOm provides technical, operational, and business advice for IT’s strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm’s advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm’s perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.
11. Copyright

© Knowingly, Inc. 2022 "Using App Service Environment v3 in Compliance-Oriented Industries" is a trademark of Knowingly, Inc. For permission to reproduce this report, please contact sales@gigaom.com.