

SYNERGITA DATA SECURITY

TECHNICAL WHITE PAPER



Synergita

Synergita is a cloud based Employee Performance Management software product. We deliver performance management solutions to various industries. Our clientele spread across companies of varied sizes. Here is our high level feature set.

Synergita - Product Overview



Technology Stack

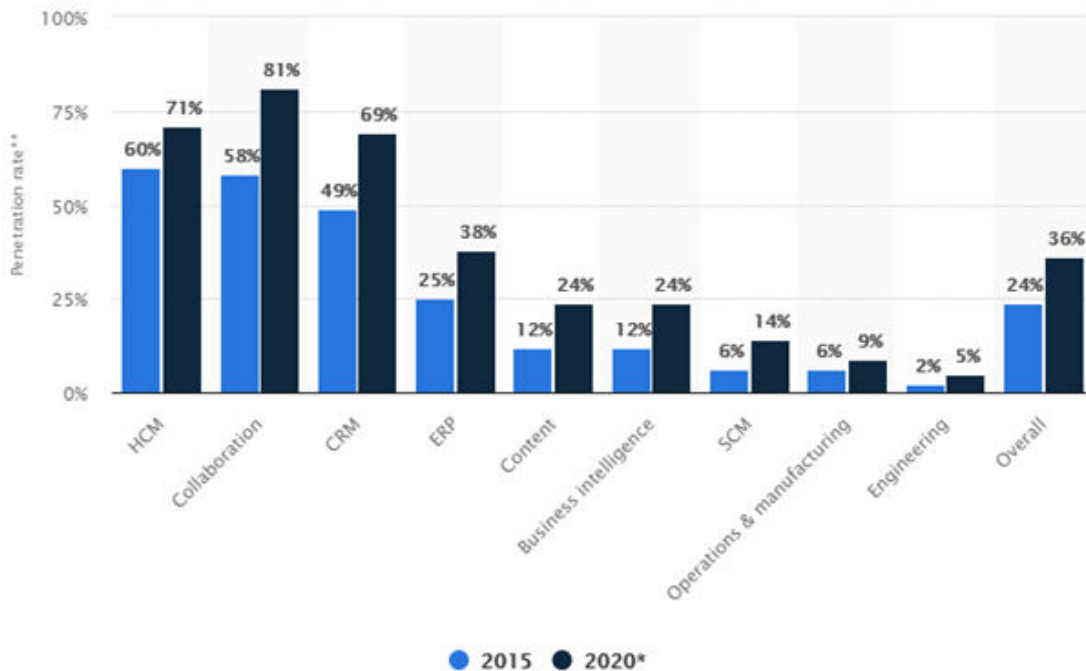
Synergita is built on Microsoft DotNet platform. Here is the technology stack of the product.



Penetration of SAAS products

Statistics shows the penetration of SAAS products industry wise in 2015 & 2020. In 2020, around 71% of the HCM products will be delivered via software as a Service. And the other industries as well adapting to cloud at a very good pace.

Rate of public cloud application services/software as a service (SaaS) penetration worldwide in 2015 and 2020, by application type



Benefits of SAAS Cloud Deployments

SAAS is typically “on-demand software”. SAAS apps are subscription based and hosted in cloud environment. Businesses don’t have to install and maintain these apps. Cloud vendors take the larger responsibility of managing the infrastructure, security, etc. So companies, which are looking for IT infrastructure can benefit from this model.

Customers have to pay only for what they use; so it becomes easy to scale down and up on the usage front as business demands.

Security

While reaping the benefits of cloud deployments, it's also very critical to consider all the threats and safeguard the customer data. This whitepaper describes the various security measures, which are put in place by Synergita to secure the data.

Cloud Security

Synergita is hosted on AWS cloud environment separately for US & Asia Pacific customers.

Amazon Web Services (AWS)

Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability. AWS provisions a variety of basic computing resources such as processing and storage. The AWS infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. As an AWS customer, we are assured that we are building web architectures on top of some of the most secure computing infrastructure in the world.

The IT infrastructure that AWS provides to us is designed and managed in alignment with best security practices and a variety of IT security standards, including:



- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 27001
- ITAR
- FIPS 140-2

The audit reports are published for all AWS customers.

Physical & Environmental security is taken care and this includes Fire Detection and Suppression, Power, Climate and Temperature, Management, Storage Device Decommissioning, etc.

The AWS network provides significant protection against traditional network security issues:

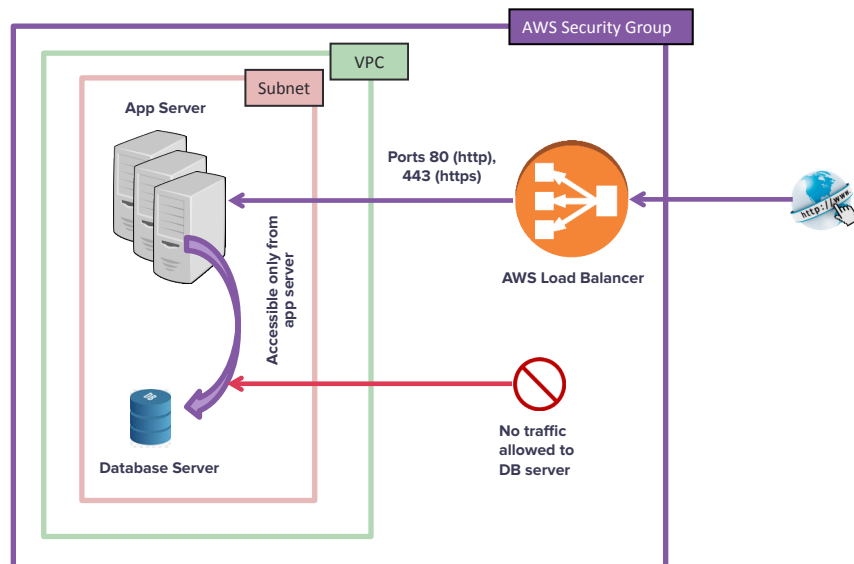
- Distributed Denial Of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants

Multiple user accounts with required level of access are created using AWS Identity and Access Management (AWS IAM). We have implemented the best practices such as least privilege and resources required for the users to perform their jobs.

Network Security

Synergita cloud architecture is built on top of AWS and designed to deliver high level of security & resiliency.

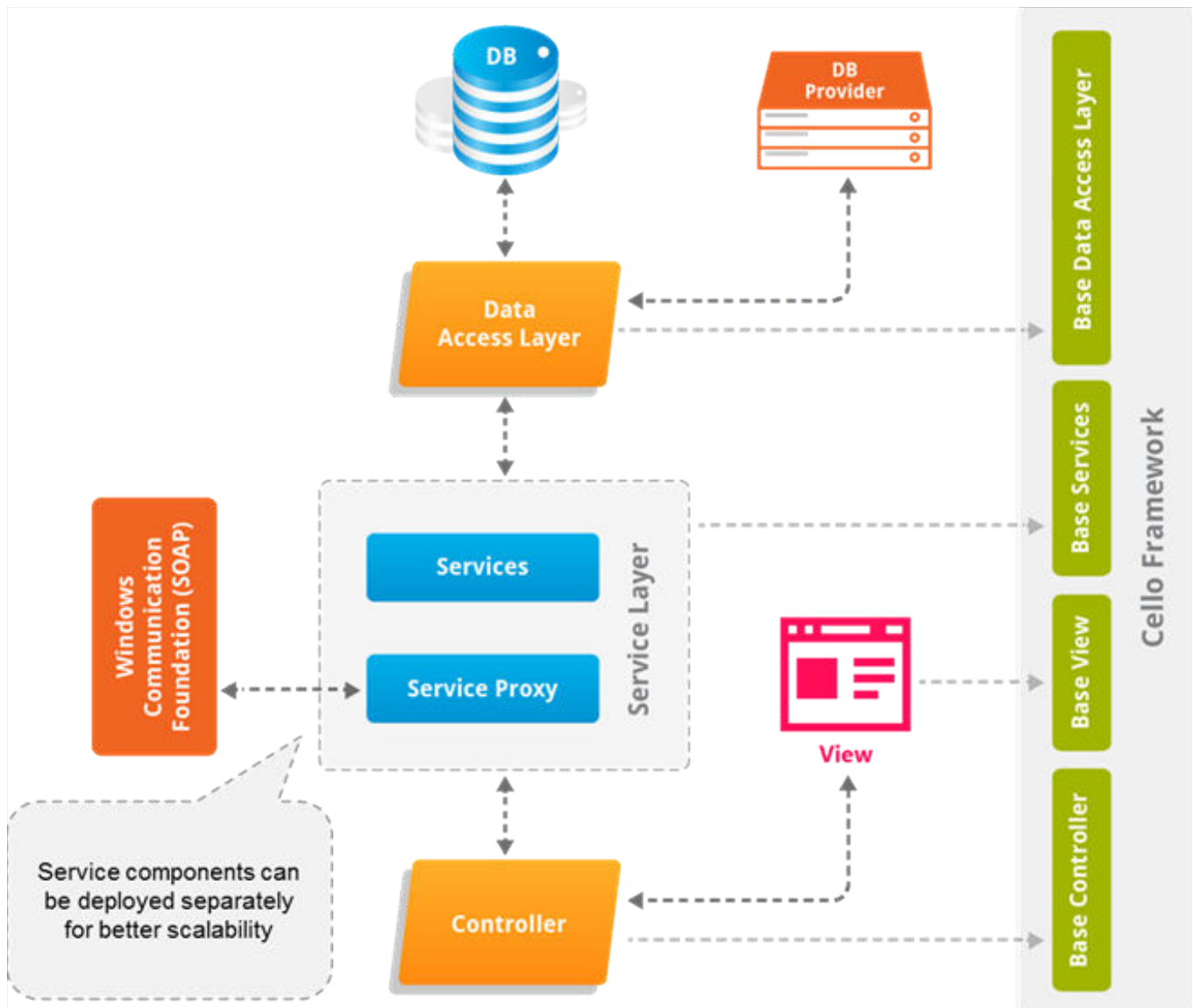
Security Groups – A security group acts as a virtual firewall that controls the traffic to each of our server. We have allowed only the required traffic to our servers opening the required set of ports. For example, database server is kept inside the subnet where the application server resides and accessible only for from application server. So we ensure that our servers are protected from intruders.



Application Security

Architecture

Synergita's architecture is built on top of Techcello (<https://www.techcello.com/>), an award winning framework for SAAS products. The multi-tenant architecture enables hosting the product in cloud environment. The architecture is designed keeping security as the top most consideration. Here is the snapshot of the architecture.



Tenant Data Isolation

Synergita uses shared schema model. The architecture takes care of tenant data isolation; the data of tenants will be accessible only for the privileged users of the respective tenants. This check is implemented in all the layers of the architecture to ensure tenant data isolation completely.

SAAS - How single DB Instance hold data from multiple customers?

Database Design


Tenants Table

Tenant ID	Name
10001	Customer 1
10002	Customer 2
10003	Customer 3

Tenant ID	Workflow
10001	WF1
10001	WF2
10001	WF3

Users Table

User ID	Tenant ID	Name
9001	10001	Anandhi
9002	10001	John
9003	10001	Ramesh
9004	10002	Sridhar
9005	10002	Umesh
9006	10003	Anand
9007	10003	Jab
9008	10003	Karthik

 Foreign Key Referenced Columns

All customer data are linked with the tenant id and there by making it possible to serve multiple customers with single DB and app instance as it is done in any SASS product

Roles & Privileges

Using access control lists (ACLs) to determine who can access data in the application and what they can do with it. (For example, Employee Salary information will be visible only for few people in the organization – employee self, manager, HR manager and whoever is provided relevant access, e.g. CEO).

All the features are controlled by role based privileges and for each privilege, scope of data under consideration can also be configured. (For example, Department head can view the salaries of employees from his department only & not from other departments)

Engineering Practices

Our development and QA teams are trained regularly on the web application security threats and the ways to avoid the same in software.

Security Testing with 3rd Party Vendor

We are tied up with IndusFace (<https://www.indusface.com/>) for security testing the product. This platform is being used for several banking companies in India and it one of trusted platforms across the world.

Here is the scope covered in the security testing.

- **Continuous Application Scanning** - Daily or on-demand web application scanning to detect vulnerabilities
- **Business Logic Vulnerability Checks** - Extensive manual penetration testing checks to discover application specific business logical vulnerabilities
- **OWASP Top 10 Detection** - Efficiently detect most common application vulnerabilities validated by OWASP

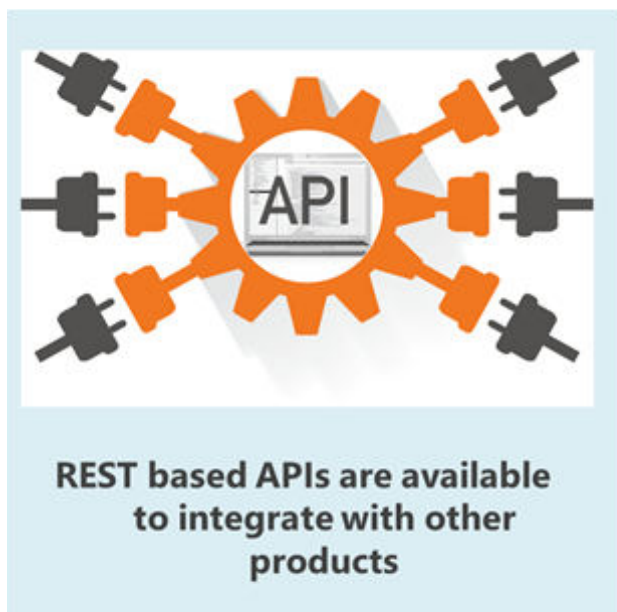
The product is security tested before every major release and the identified issues are fixed before release.

Integrations with Other Systems

Synergita supports multiple secured approaches for integrating with other products such HRIS or Payroll products.

API based integrations

REST based APIs are used for integrating with other products. We support both way data transfer. In most cases, the employee data comes from HRIS into Synergita and Synergita can also share the employee performance ratings to other systems such as Payroll or Compensation



REST API Authentication

All the API calls must be authenticated & authorized before accessing the data. This ensures that the data is accessible for authorized personnel. The authorization parameter has to be passed in the header of each request. A unique authorization key will be generated for each tenant/customer to access the APIs.

Security of Data

All the API end points are secured with TLS 1.2v certificate. This ensures that the data in transit is encrypted and secured.

Data Backup Strategy

Here are the SLAs committed to our customers.

Recovery time objective (RTO) - The time it takes after a disruption to restore the software application to its accepted service level.

Synergita offers an RTO of 8 business hours to all customers.

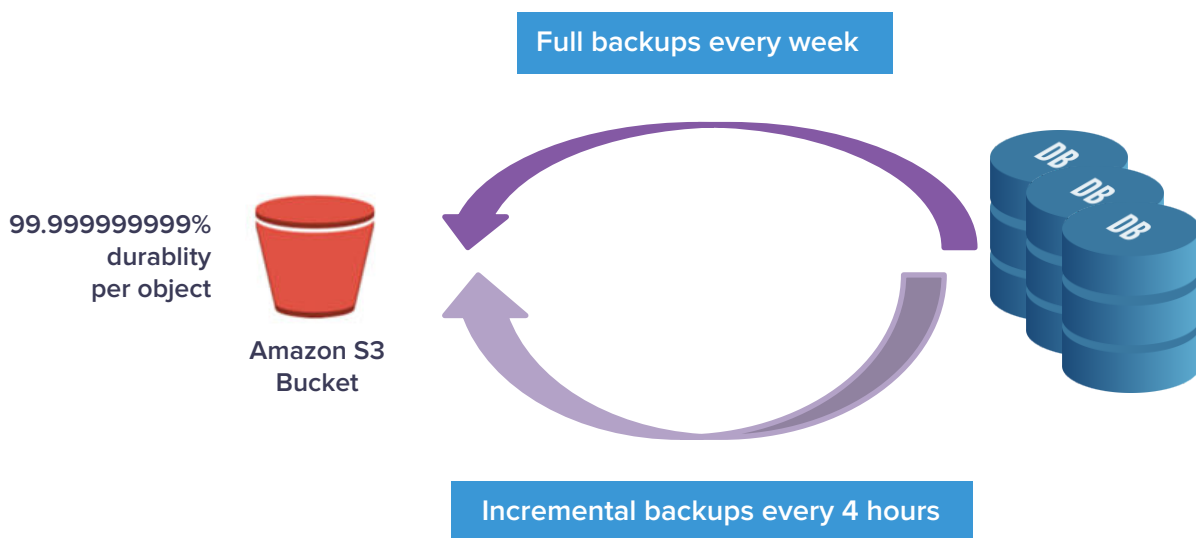
For example, if a disaster occurs at 12:00 PM (noon), the application will be restored to the acceptable service level by 8:00 PM.

Recovery point objective (RPO) - The acceptable amount of data loss measured in time.

Synergita offers an RPO of 4 business hours to all customers.

For example, if a disaster occurs at 12:00 PM (noon), all the data that was in the system before 8:00 AM shall be recovered

Backup process for SQL Server databases



We are taking full backups on Weekly basis and Transactional Log Backups for every 4 hours.

Full Backups: @ 2AM Every Saturday.

Incremental Log Backups: Every 4 hours (6 Logs for Database per Day).

AWS S3 Backups

The database backs are stored in AWS S3. These backups can be retrieved easily from S3 and restored into database.

Amazon Simple Storage Service (Amazon S3) is a simple storage service that offers software developers a highly-scalable, reliable, and low-latency data storage infrastructure. You can write, read, and delete objects containing from 1 byte to 5 terabytes of data each. The number of objects you can store in an Amazon S3 bucket is virtually unlimited. Amazon S3 is also highly secure, supporting encryption at rest, and providing multiple mechanisms to provide fine-grained control of access to Amazon S3 resources.

Amazon S3 is designed to sustain the concurrent loss of data in two facilities, making it very well-suited to serve as the primary data storage for mission-critical data. In fact, Amazon S3 is designed for 99.999999999% (11 nines) durability per object and 99.99% availability over a one-year period. In addition to its built-in redundancy, Amazon S3 data can also be protected from application failures and unintended deletions through the use of Amazon S3 versioning.

About Synergita

Synergita is the leading, enterprise-ready, cloud-based continuous employee performance management and engagement software.

With Synergita, organizations effectively track goals & progress, engage employees with continuous conversation, complete performance review on-time and gain business intelligence with few clicks. Synergita provides extensive support and helps achieve performance-driven growth. Powerful integration with SAP and single sign-on (ADFS) makes Synergita the go-to software for business enterprises as well as SMBs.

THANK YOU
