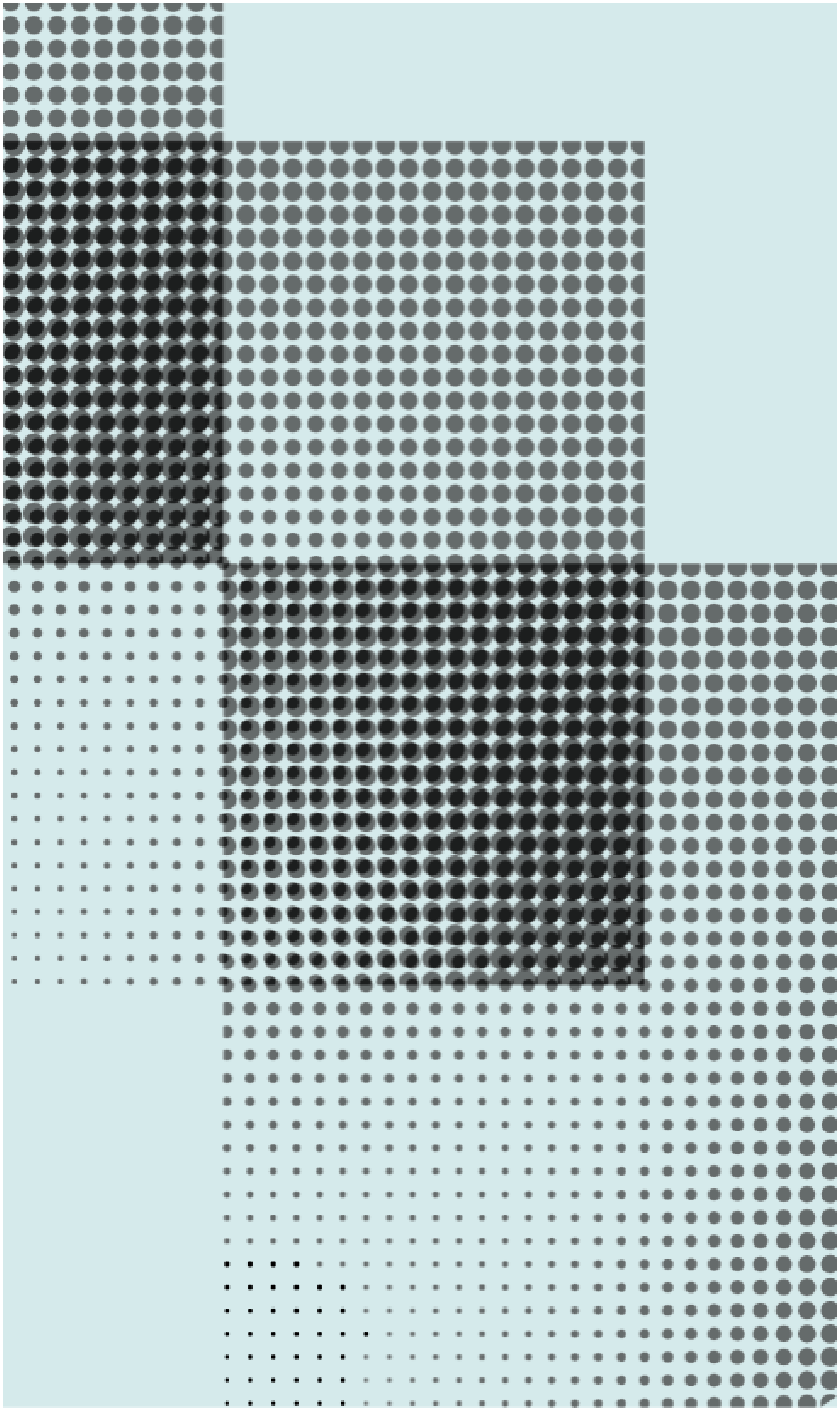
Whitepaper Sep 2022

Okta HIPAA Cell

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



Contents

Okta cell architecture

Okta created Identity-as-a-Service (IDaaS) and from the start has firmly believed in building a best-in-class enterprise-grade service. Infrastructure investments have been a priority at Okta from the beginning.

Today, Okta continues to invest in one of the most resilient, secure and “Always On” cloud architectures in the world. Overall, the Okta architecture uses a concept we call a “cell” as the largest unit of scale in the service. Each Okta “cell” encapsulates a full multi-tenant cloud service with extremely high availability. For more details on the architecture overall, see these papers:

An Insider Look: How Okta Builds and Runs Scalable Infrastructure

Scaling Okta to 10 Billion Users

Okta Security: Technical Whitepaper

HIPAA scoping

The most difficult component of operating in a regulated environment is the definition of the scope boundaries. Organizations want to ensure that only required systems are included in any regulatory audit, as the expansion of scope incurs additional setup, maintenance, and cost. This drives the selection of an Identity vendor that can operate as a Business Associate to the customer.

HIPAA scoping also includes determining if the data being protected by your Information System is classified as Protected Health Information (PHI). PHI can be defined as information that “relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, …and directly identifies the individual or there is a reasonable basis to believe …can be used to identify the individual.”[1]

[1] Paraphrased from HIPAA section 1171

Cell for HIPAA

To support the ability of Okta to sign a Business Associate Agreement (BAA) for customers, Okta has developed a solution that requires customers to sign a BAA prior to storing HIPAA-related information. The IDaaS Cell for HIPAA is available to customers, which includes the core Okta service, as well as products such as Workflows to automate identity tasks. There are two main aspects where the HIPAA solution differs from a standard Okta implementation.

Reporting requirements

HIPAA contains specific regulations regarding communication of data breaches, access to Protected Health Information, and financial reporting to the US Department of Health and Human Services. These regulations require Okta, upon request by any user, to provide a report of any time that a user's PHI was viewed by an Okta employee.

Trickle-down requirements

As a cloud service provider, Okta relies on external vendors to provide critical support for the Okta IDaaS product. This includes Amazon Web Services for Infrastructure, Splunk for log data management, Snowflake for log data retention and third-party US-based Customer Support providers. In order for Okta to handle PHI, we must also have agreements with our vendors who may be exposed to PHI as a result. These agreements typically come with additional costs or implementation requirements.

At an infrastructure level, within each cell, Okta uses strict internal traffic segmentation via Amazon Security Groups to ensure that data in motion between the different production services that make up our solutions cannot be viewed by unauthorized parties. This provides a high level of protection while maintaining fast network performance. Amazon’s interpretation of the HIPAA regulations requires us to add IPSEC encryption in between services as well. Okta has deployed this technology within our HIPAA cells. Okta uses multiple levels of encryption within our product to provide equal protection, however this trickle-down requirement adds additional cost and complexity.

Benefits of the Okta cell for HIPAA compliance

Okta has made significant special investments to provide a HIPAA-compliant environment for its customers who need to comply with HIPAA.

Okta makes available a BAA for its customers who purchase Okta services that operate within a HIPAA cell to enter into that a customer may choose to execute prior to storing any Protected Health Information (PHI) within Okta.

In addition to being able to sign a HIPAA BAA, Okta offers the following features in its product and organizational policies to every customer regardless of cell location:

- Data encryption in transit and at rest
- Restricted physical access to production servers
- Strict logical system access controls

Configurable administrative controls available to the customer to:

- Monitor access
- Reporting and audit trail of account activities on users and content
- Formally defined and tested breach notification policy
- Training of employees on security policies and controls
- Employee access to customer data files are highly restricted
- Mirrored, active-active data center facilities to mitigate disaster situations
- 99.99% uptime SLA
- Annual SOC 2 Type II Reports and 3rd party penetration testing
- ISO 27001, ISO 27017, and ISO 27018 certification

The main benefit to a customer of using Okta’s HIPAA cell infrastructure is that it enables a customer to take advantage of Okta’s additional safeguards to help them meet their HIPAA compliance needs. This is a unique capability that Okta offers to customers.

About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. To learn more, visit **okta.com**.