KOFAX

SOLUTION OVERVIEW

Supplier Portal Security

A Dependable, Secure Infrastructure Built on Amazon Web Services

Kofax provides customers with a reliable, secure application to manage the procure-to-pay process from anywhere at any time. Kofax has partnered with Amazon Web Services to provide the hardware and infrastructure to support Kofax Supplier Portal solution.

Amazon AWS was launched in July 2002 and is now the most popular on demand infrastructure for commodity computing and virtual secure storage on the planet. More information about the service can be found on the website: http://www.amazon.com/aws.

Physical Security

Kofax contracts with Amazon.com to provide its physical hosting infrastructure using Amazon's EC2 service. Amazon enforces physical security through a variety of methods as covered in their security whitepaper. The buildings, servers, and infrastructure of Amazon's EC2 service is the same as their multi-billion dollar Amazon.com retail business, so Kofax customers can be assured that their application and data are secure.

Transport Security

Kofax encrypts all communications between customers and our data center using high-grade Encryption (DigiCert SHA256 CA·G3). Access to Kofax's on-demand applications and services is only available through secure sessions (https) and only available with an authenticated login and password. Passwords are never transmitted or stored in their original form, so they are never compromised by third parties.

Perimeter and Server Security

Kofax protects its application infrastructure by using state-of-the-art firewalls at the hypervisor, kernel, and application levels, as well as intrusion detection systems across all servers. Kofax's anomaly detection system instantly notifies operations staff, 24/7, if anything unusual is detected.

Key features

- Application hosted on Amazon Web Services – the same infrastructure that supports Amazon.com's multi-billion dollar business
- High-grade encryption of passwords and other data offers extra security during transport
- State of the art kernel firewalls and intrusion detection software provide continuous system monitoring
- Multi-layered architecture secures customer sessions and prevents unauthorized data access
- Best-in-class disaster recovery protocols eliminates data loss in the event of system failure

Key benefits

- Highly secure and reliable infrastructure ensures application up time and availability
- 24/7 monitoring and response protects application from unauthorized access
- No costly hardware or infrastructure to support or maintain
- Redundancies and other protections eliminate data loss
- Limited access and encryption provides complete data privacy and security

In addition, Kofax contracts with third party security firms and consultants to conduct vulnerability threat assessments including penetration tests.

All front-end servers are behind firewalls and only accessible via https protocol. Database servers inside the perimeter firewalls are protected using proprietary non-routable IP addressing schemes, network address translation and more.

Kofax enforces tight operating system-level security by maintaining a minimal number of access points to all

production servers. Operating system accounts are protected using secure public key authentication and only operations personnel has access to the servers. All operating systems are maintained at each vendors recommended patch levels for security and are hardened by disabling or removing any unnecessary users, open ports, and processes. Access to the databases is controlled through limited and separately access-controlled passwords.

Kofax employees do not have direct access to production equipment, databases or customer data, except where necessary for system management, maintenance, and backups. Access to customer data is further restricted to technical and customer support staff on a need-to-know basis. No parties outside Kofax have access to customer data unless required by law.

Application Security

No customer can see another customer's data. This is enforced on several layers of the architecture, including authenticated sessions, which are required for any page access. Sessions are stored in cookies that do not encode any customer identifiable information. Nor is any customer ID ever transmitted or stored during page access, thus preventing ID spoofing.

Reliability and Backup

In addition to the physical redundancy (network, power) that Amazon.com provides, Kofax has redundant configurations for each component of its infrastructure. All customer data is stored on redundant database servers with live failover. All customer data is placed on RAID class hardware, replicated in real time to a secondary environment in a different data center, then backed up daily onto the Amazon.com S3 service. The Amazon.com S3 service is then replicated throughout the Amazon.com data centers globally.

Disaster Recovery Program

Kofax is able to leverage the Amazon AWS cloud to provide a best-in-class disaster recovery program. Amazon AWS services for data storage eliminate the risk of customer data loss. In the event that the primary hardware for a customer fails, Kofax can immediately switch over to the secondary hardware, which is running concurrently with the primary. If there is a disaster that fails both the primary and secondary servers, Kofax has the ability to failover to any of a number of Amazon.com data centers in the United States and in Europe, in a matter of minutes.