Security and Compliance in the Cloud

Security is a top concern for any customer considering the cloud. There are many advantages to storing data in the cloud, but that data must be stored securely and only be accessible by the customer.

A common misconception about the cloud is that it is not as secure as storing data on premises. When you host the systems yourself, the servers on premises are vulnerable to hackers, break-ins, and natural disasters.

Moving to the cloud provides the benefit of scale. Cloud hosting providers continuously update their servers to combat the newest cyber-threats, backup data to separate servers, and employ expert resources at a level that no single organization could reasonably commit to.

In this course we'll review

1) How Epicor leverages data backups and recovery to keep its customer's data secure

2) How Epicor guards against malware and system vulnerabilities

3) How Epicor protects its customers at login through identity services that verify a user is who they say they are

4) And lastly, we'll look at Compliance considerations

Select the right arrow icon to start the first topic, Data Backup and Recovery

Objectives

- Data Backup and Recovery
- Vulnerability Management
- Keeping Users Secure
- Compliance Considerations

Data Backup and Recovery

A common question many people have when they consider moving to the cloud is whether their data will be kept current and if it could be lost. Data backup, retention, and disaster recovery policies address this question.

Epicor backs up customer data at least daily and keeps these backups for 30 days. This means that at any time, a customer can recover data from the previous 30 days if necessary.

You also need to consider disaster recovery in case of a severe weather incident, loss of power, or other disaster where customer data is stored.

For those products in the Azure Public Cloud, Epicor leverages the Microsoft Azure Disaster Recovery strategy. This means that several copies of customer data are replicated in near real time across multiple highly secured datacenters.

In the unlikely event that one location goes down, the customer will not experience a complete shut-down of their business. The secondary location will be available, and access will be restored including data from the most recent backup.

This is much more difficult to do on-premises, because servers are stored at the business location and subject to potential disasters. These can have a significant impact or even cause a shut-down for hours or potentially days.

Select the right arrow icon to begin the Vulnerability Management and Anti-Malware topic.

Vulnerability Management

Bad actors are constantly trying to access customer data, whether it is stored on premises or in the cloud. Staying vigilant about identifying and assessing vulnerabilities and scanning for malware is a critical part of cloud security.

Many of Epicor's cloud products run on Microsoft Azure, which is widely recognized as one of the world's most secure cloud platforms. Its virtual and physical security policies are constantly evolving with technology advances, so you can be confident that its datacenters are secure.

Epicor leverages many encryption services including Microsoft Azure's Storage Service Encryption to protect data stored in the environment. This means that customer data is encrypted at all times, including when that data is transmitted between datacenters.

Anti-malware software is a critical component of any security strategy, and Epicor has anti-malware software installed in all environments at risk. We push updates at least daily, so that customers can be confident that we are staying on top of bad actors trying to gain entry to the systems.

Our experts are constantly monitoring and analyzing the latest cyber threats. Intrusion Detection is in place at key network points and alerts are analyzed by our Security Operations Center. Escalated alerts are also analyzed by our Cloud Reliability Center as necessary.

At Epicor we take cloud security very seriously, conducting penetration testing regularly and remaining SOC 1 and SOC 2 compliant through annual independent assessments. Reports are available by request.

Select the right arrow icon to move onto the Keeping Users Secure topic.

Keeping Users Secure

The ability to access your data from anywhere is a big advantage to being in the cloud, but it is critical that you know who is logging in. Hackers may try to impersonate your employees.

Requiring that employees have a username and password to gain access has been common practice for many years. Unfortunately, this may not be enough to be secure.

Bad actors may try to gain access to your systems by pretending to be a valid user. They may use software that guesses passwords, or usernames and passwords may be included in a data breach.

An identity provider that verifies that your users are who they say they are is an important layer of security. Epicor Identity Provider (IdP) provides multifactor authentication, requiring that users login with an email and password and use a second method of authentication to prove they are who they say they are.

Multifactor authentication is widely viewed as significantly more secure than the use of only a username and password, guarding against bad actors accessing your systems.

IdP also allows you to manage password policies like character requirements or mandatory password resets after a specific number of days, so that you can be confident that users are who they say they are and that your data is secure.

Select the right arrow icon to continue to the last topic: Compliance Considerations.

Compliance Considerations

Many of Epicor's customers work in industries that are subject to government regulation. a move to the cloud cannot jeopardize their compliance.

Compliance considerations can be different depending on the regulatory body, for example the FDA may have different concerns than the Department of State. This means that any business that is subject to regulation should investigate their specific compliance needs.

Depending on the regulation, customers may have specific requirements for storage of customer data or financial data. They may also have requirements in other areas like privacy, data archiving, system requirements, testing and approval of new functionality, and more.

If a business that is subject to regulation does not remain compliant they may face large fines, lawsuits, or even risk having to shut down their business, so it is critical that they do not put their compliance at risk.

Epicor's public cloud is compliant with a number of regulations including GDPR, CCPA, ITAR, FDA, and CMMC depending on the product and industry. Reach out to an Epicor expert to have an in-depth compliance conversation.

Microsoft Azure is widely known as a leader in this area, with technologies that allow for compliance with a wide variety of regulations in the U.S. and internationally. As Epicor's strategic partner this means that Epicor's public cloud could become compliant with more regulations in the future.

Select the right arrow icon to view a recap of the topics and complete the course.

Recap

Good work completing the Security and Compliance in the Cloud course.

In this course you reviewed

1. How Epicor leverages data backups and recovery to keep its customer's data secure
2. How Epicor guards against malware and system vulnerabilities
3. How Epicor protects its customers at login through identity services that verify a user is who they say they are
4. And lastly, you learned about some Compliance considerations Epicor's customers face.

The contents of this document are for informational purposes only and are subject to change without notice. Epicor Software Corporation makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims, to the full extent of the law, any applicable implied warranties, such as fitness for a particular purpose, merchantability, satisfactory quality or reasonable skill and care. This document and its contents, including the viewpoints, dates and functional content expressed herein are believed to be accurate as of its date of publication. The usage of any Epicor software shall be pursuant to the applicable end user license agreement and the performance of any consulting services by Epicor personnel shall be pursuant to applicable standard services terms and conditions. Usage of the solution(s) described in this document with other Epicor software or third party products may require the purchase of licenses for such other products. Epicor, the Epicor logo, and are trademarks of Epicor Software Corporation, registered in the United States and other countries. All other marks are owned by their respective owners. Copyright © 2021 Epicor Software Corporation. All rights reserved.

About Epicor

Epicor Software Corporation drives business growth. We provide flexible, industry-specific software that is designed around the needs of our manufacturing, distribution, retail, and service industry customers. More than 40 years of experience with our customers' unique business processes and operational requirements is built into every solution—in the cloud, hosted, or on premises. With a deep understanding of your industry, Epicor solutions spur growth while managing complexity. The result is powerful solutions that free your resources so you can grow your business. For more information, connect with Epicor or visit www.epicor.com.

Corporate Office
804 Las Cimas Parkway
Austin, TX 78746
USA
Toll Free: +1.888.448.2636
Direct: +1.512.328.2300
Fax: +1.512.278.5590

Latin America and Caribbean
Blvd. Antonio L. Rodriguez #1882 Int. 104
Plaza Central, Col. Santa Maria
Monterrey, Nuevo Leon, CP 64650
Mexico
Phone: +52.81.1551.7100
Fax: +52.81.1551.7117

Europe, Middle East and Africa
No. 1 The Arena
Downshire Way
Bracknell, Berkshire RG12 1PU
United Kingdom
Phone: +44.1344.468468
Fax: +44.1344.468010

Asia
238A Thomson Road #23-06
Novena Square Tower A
Singapore 307684
Singapore
Phone: +65.6333.8121
Fax: +65.6333.8131

Australia and New Zealand
Suite 2 Level 8,
100 Pacific Highway
North Sydney, NSW 2060
Australia
Phone: +61.2.9927.6200
Fax: +61.2.9927.6298