CASE STUDY

NIST Compliance & Mac Security

tucu
managed IT services inc

Industry
Communications

Size
25 - 50 staff

Solutions

- Azure Active Directory & Apple Business Manager Security Controls
- NIST compliance
- Digital Loss Prevention
- Managed IT Services

Passing Client Security Screenings To Do Business

This communications company needed to pass a vendor security screening in order to retain Client X - a very important client. In the past, Client X only required business partners to complete a self assessed IT security questionnaire. Due to rising global cyber threats, Client X now requires all business partners to pass an IT security audit.

Audits are performed by approved third party auditors, selected by the client, and must be separate entities from the IT provider. Auditors verify that IT security controls, processes and policies are met to the client's satisfaction.

TUCU created IT systems based on NIST best practices, our client passed their audit, and retained Client X. TUCU provides ongoing IT management so that our client can focus on operations and growth.

The Challenge

Our client has an all Mac environment.

The average person is unaware that Mac's lack centralized administrative control capabilities.

Most IT security solutions are geared to PC's, since they dominate the business landscape.

As such, the tools used to manage most networks are built for PC's. They lack advanced functionality for Mac's.

This means they leave Mac environments with gaping security holes, and no way to meet compliance requirements, secure data, prevent digital loss, authenticate users or block suspicious activity.

In order to meet NIST best practices, all the above are required.

To help our client create a secure environment, we used Azure Active Directory as the framework for connecting users computers and cloud applications.

We paired it with Apple Business Manager to control devices, and extensive data loss prevention policies.

The result is a secure network and stringent company wide policies that can meet and exceed any compliance audit they may face.

Technical Summary

Azure Active Directory (AAD) is Microsoft's multi-tenant, cloud-based directory and identity management service.

Azure AD combines core directory services, advanced identity governance, and application access management.

Apple Business Manager connected to Azure AD and Microsoft InTune was used to bind Mac devices, applications, and managed Apple ID's. This enables to network administrators to grant or deny access to company data hosted in the cloud.

Advanced compliance controls were necessary to pass the clients audit. These included:

Mandatory encryption on computers and mobile devices.

Enforcement of data labelling policies to classify files that may contain sensitive information and apply security controls to those file (i.e. you can tag a file as confidential or Client X, which will encrypt it, water mark it, prevent it from being shared, prevent it from being forwarded, prevent it from being printed).

Retention labels were required to maintain specific time frames for automated deletion of Client X's files.

Extensive data logging was required for any activity against any service, on any device, that may access Client X's data.

Azure Sentinel is the repository for all log files generated from computers, network equipment and connected cloud services. Those log files must be kept for a specific length of time to investigate or reconstruct potential data breaches.

Microsoft Cloud App Security (CASBE) is used for anomalous activity detection for connected computers and cloud services. These log files are also stored in Azure Sentinel. CASBE generates security alerts and notifications with severity levels, which are reviewed and actioned by IT administrators.

Benefits

The above and additional security controls can help any business just like yours.

Not only can such IT systems help you meet compliance requirements, but will also enable you to:

- control your data
- limit your risk of data loss
- prevent intentional or accidental data exfiltration
- securely offboard team members and their computers
- protect against data loss due to device theft

The above solutions have excellent applications for **PIPEDA, PIA, HIPAA and GDPR.**

Any industry will benefit from these security controls, and especially those handling sensitive data such as medical, legal, financial.

TUCU Managed IT Services Inc is a local leader in small business IT solutions. We help you use technology to protect and grow your business.

Learn more at tucu.ca

Your Digital Transformation

People choose TUCU for responsive, reliable, support on a first name basis. Join our long list of happy clients and discover why we're voted #1 for small business IT Support.

Talk to us today about your digital transformation.

(416) 292-3300
info@tucu.ca

Grow With IT

Are you in compliance with your industry's data security requirements?

Even in industry's without requirements, SMB's are being asked to prove their cyber security posture by potential vendors, partners and clients.

Would you pass a Vendor Security Screening or Business Service Agreement for the chance to win new business?

Our clients meet pass screenings and grow their business with modern, secure IT systems we build and manage for them.

Outsourced IT Management with TUCU can help your business thrive and grow.

tucu
managed IT services inc