



Cloud Defense

The Azure and Office 365 Battleground

Who Am I?

ID

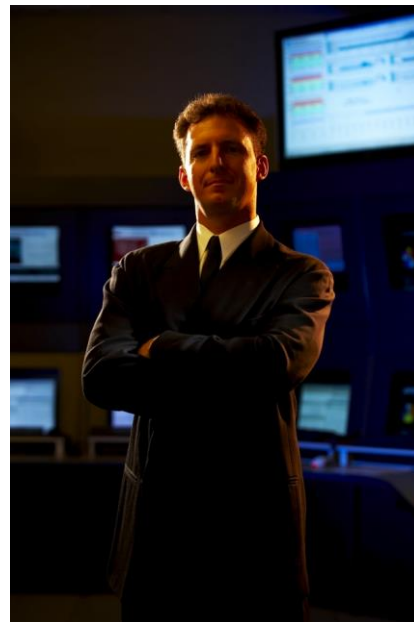
- Jeffrey T. Lemmermann
- Information Assurance Consultant – SynerComm
- January 2018

EXP

- 24 Years with CliftonLarsonAllen
- Risk Services Practice Manager
- IT Audit / IT Security Specialist
- 5+ Years as CIO/CFO – Manufacturing Industry

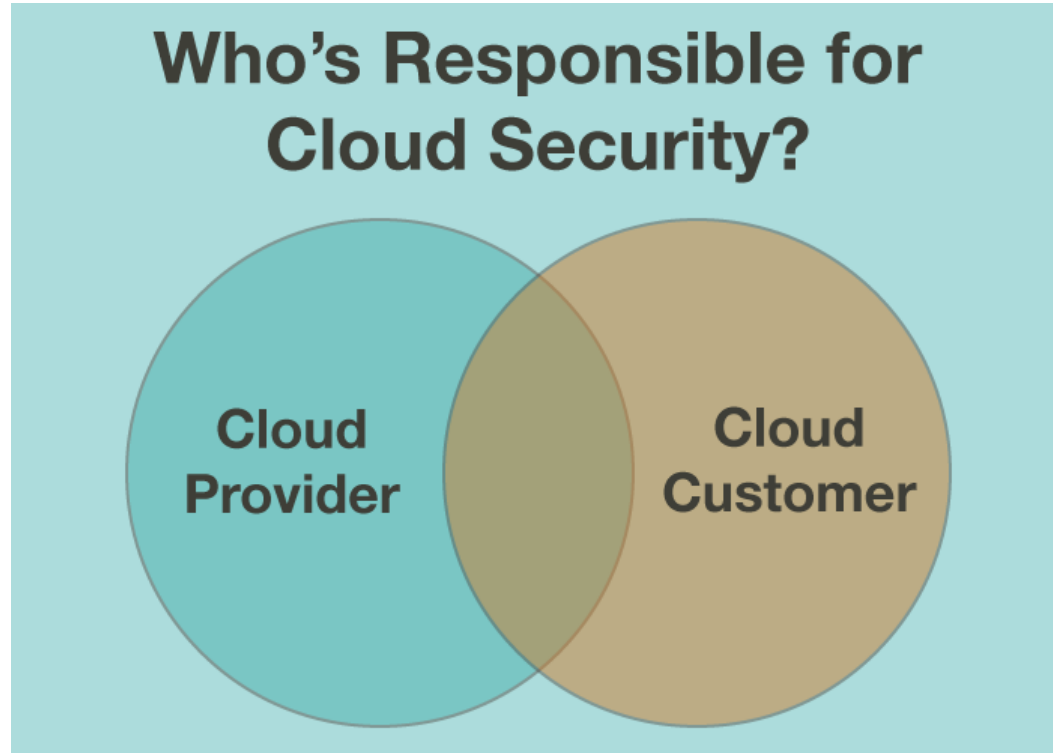
CERT

- CPA, CITP, CISA, CEH
- CITP – Wisconsin Champion (If you are a CPA 😊)

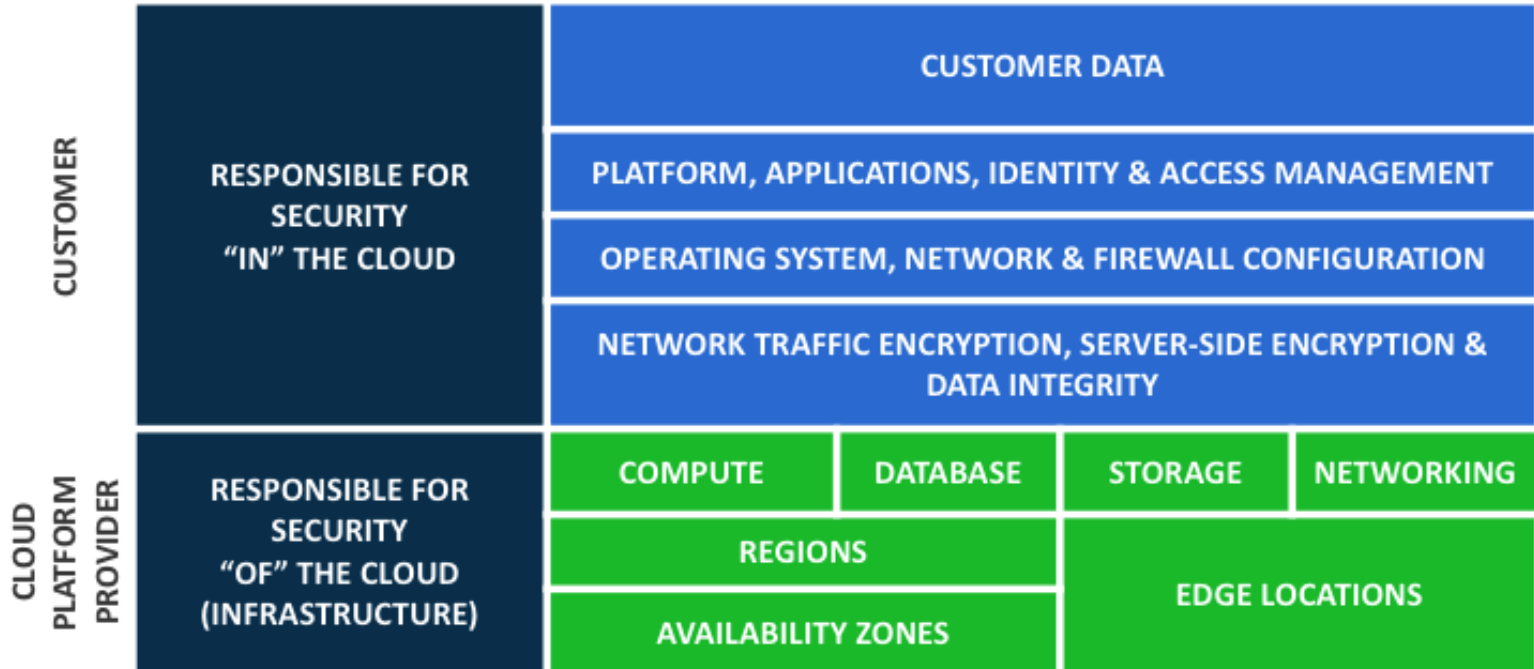


“Security Assessment & Consulting, IT Audit, Compliance with IT Frameworks (NIST, COBIT) and continuing an ongoing crusade to promote information security!”

Shared Responsibility Model





Shared Responsibility Model

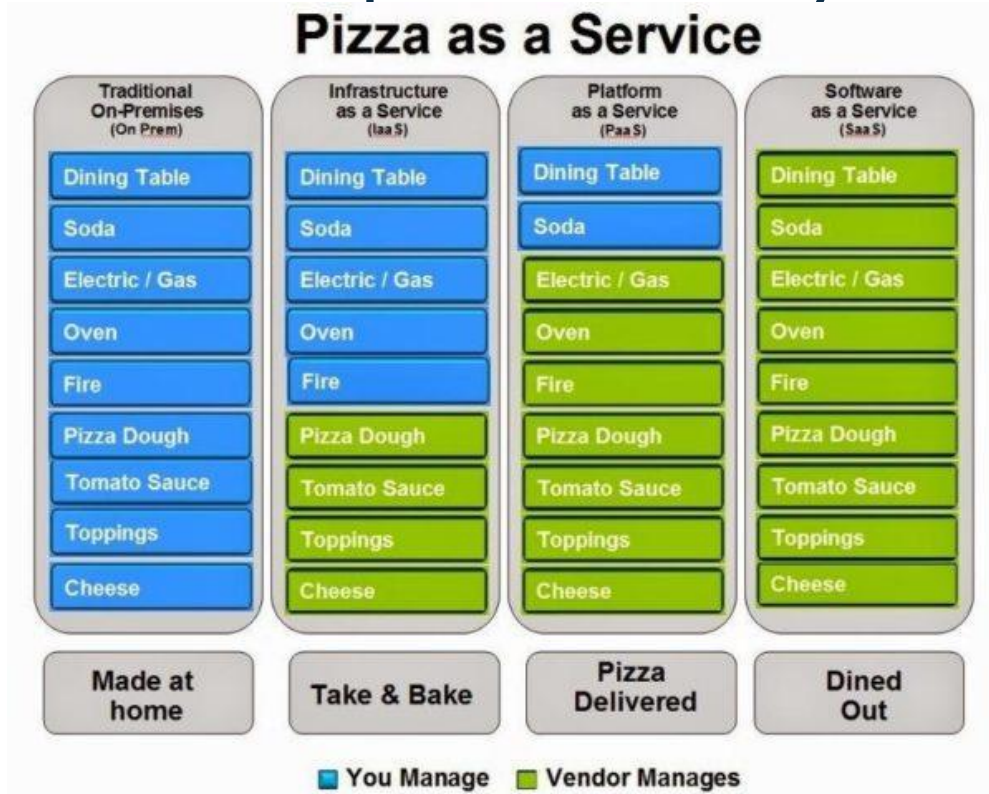


Azure's Shared Responsibility Model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend:  Cloud Customer  Cloud Provider

Shared Responsibility Model



Who is Responsible?

- “Security is Everyone’s Responsibility”



Re

I changed all my passwords to "incorrect".

hip

- Spons
 - Fina
 - Peo
- Tone a
 - Wri
 - Mak



Responsibility: Departments

- Help enforce policies and procedures within their areas.
- Partner with Security/Compliance
 - Evaluate risks versus return of new tools
 - SharePoint Sites
 - Mobile Document Collaboration

Responsibility: End Users

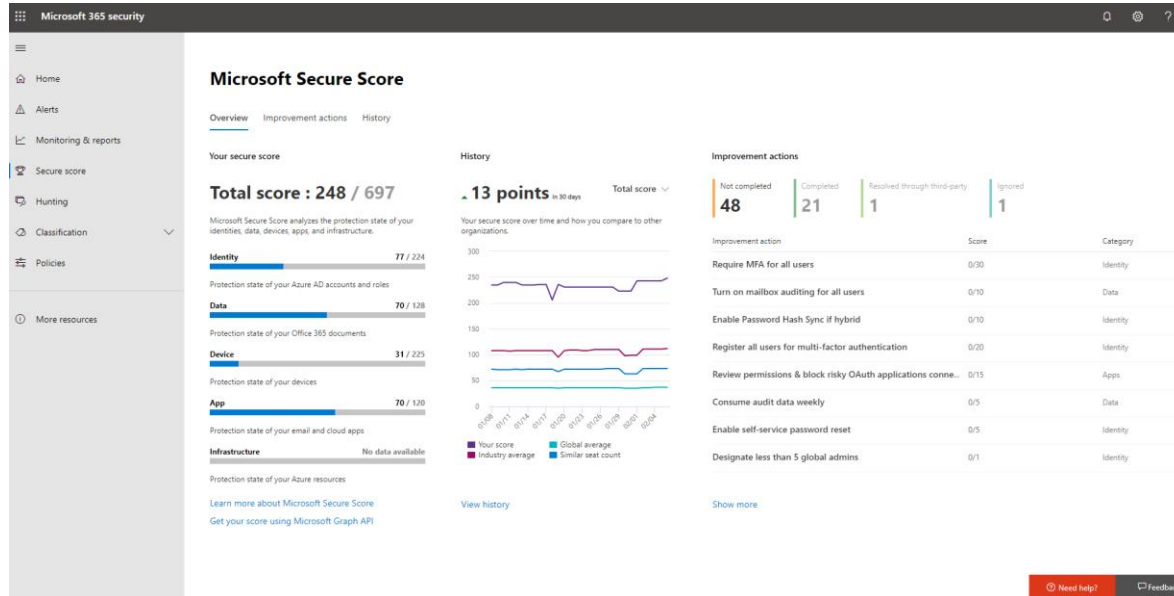
- Training on new tools
 - No longer just email and attachments
 - Exposure of data
 - Risk of new devices
- Ground defense of data

Responsibility: Security

- Review existing policy detail.
- Modify, create, and enforce policies that securely enable the cloud efforts.
- Develop procedures related to the policies.
 - Log distribution and review
 - User maintenance & licensing

Security Group Tools

Secure Score



What Does Secure Score Do?

“From a centralized dashboard you can monitor and improve the security for your Microsoft 365 identities, data, apps, devices, and infrastructure.”

Secure Score Positives

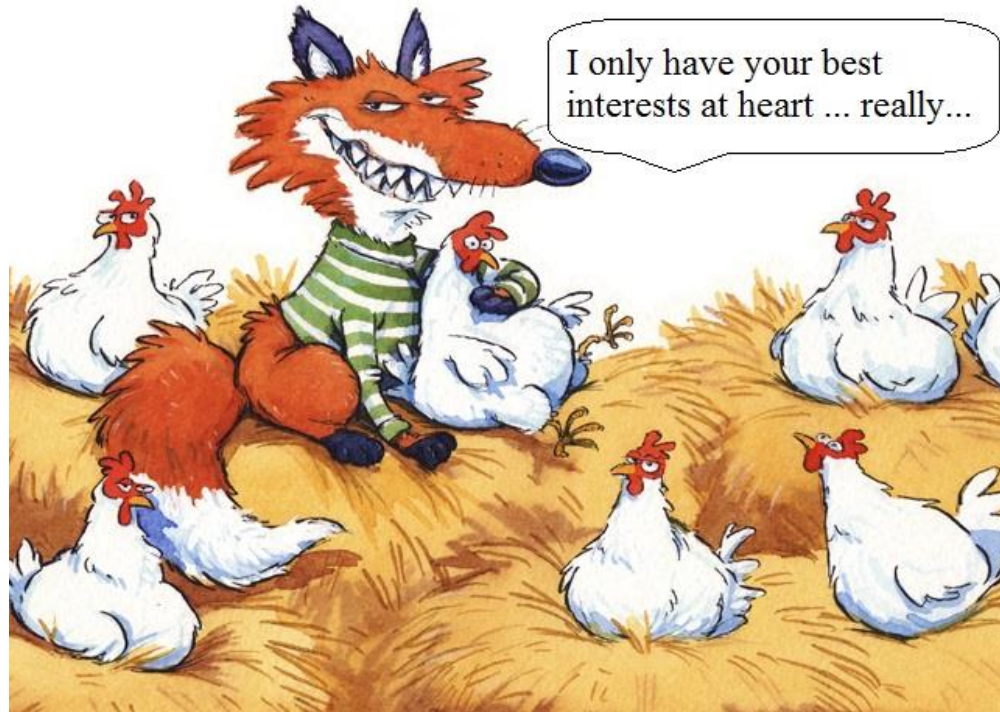
- Checks important settings
 - Trends over time
 - Comparison to other companies
- Feedback on changes
 - If I turn this item on/off, what happens?

Secure Score Shortcomings

It's not a bad thing, it just isn't everything!

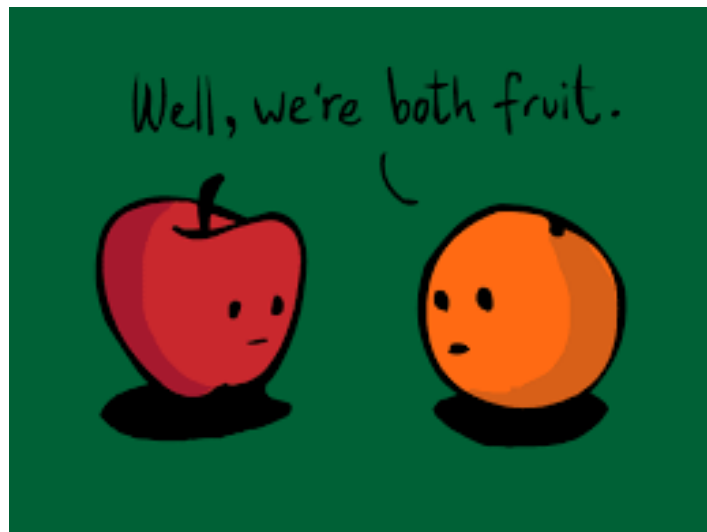
Fox Guarding the Hen House

More point
options at E5 vs.
E3.



It' Microsoft, not
NIST

Environments are Different



“Marking as resolved through third-party indicates that you have completed this action in a non-Microsoft app, and will give you the full point value of this action.”

90% Is not a finish line.

Once you ignore an improvement action, it will no longer count toward the total Secure score points you have available.



“In reality, any scoring shortage could represent a critical configuration issue that puts information assets at risk.”

Automated Security = False Security



“We hear stories all the time about breach activities that were being reported by automated logging systems, except no one was looking at the logs.”

Diversity of an organization:

- Governance, Risk, and Compliance
- Physical Security
- Network Security
- Application Security
- Data Security

These areas are all interdependent, yet all have their own unique traits and ways to be assessed and secured. No one measurement tool is enough.

Office 365 Example

On Premise to Cloud Migration:

- Hardware moves to Azure Cloud
 - Azure AD Connect On-Prem Active Directory
- Software becomes a per user subscription
- Data moves to the Azure Cloud
 - Still need backup services
- Client Access – Anywhere there is Internet

How Does Azure Fit?

- Azure for AD
- All Azure
- Hybrid

What does your environment look like?

SynerComm's Approach

- Leverage the CIS Hardening Guides
- Integrate Processes and Procedures
- 3rd Party App Assessments
- Device Configuration Assessments
- Password Analysis

Hardening Guides



Operating Systems

Server Software

Cloud Providers

Mobile Devices

Network Devices

Desktop Software

Currently showing Cloud Providers [Go back to showing ALL](#)

Cloud Providers

Amazon Web Services

Expand to see related content ↓

Download CIS Benchmark →

Cloud Providers

Google Cloud Computing Platform

Expand to see related content ↓

Download CIS Benchmark →

Cloud Providers

Microsoft Azure

Expand to see related content ↓

Download CIS Benchmark →

<https://www.cisecurity.org/cis-benchmarks/>

The SynerComm Blog

- www.synercomm.com/blog
 - AWS Metadata Endpoint
 - Understanding HIPAA
 - How to approach GDPR

Thank you!

- Questions, Comments, Stories to share?

Jeffrey T. Lemmermann, CPA, CITP, CISA, CEH
Information Assurance Consultant - SynerComm, Inc.
Jeffrey.Lemmermann@synercomm.com

The SynerComm Raffle

Good Luck and thank you to all our sponsors!

