ERP TECH
SUMMIT 2024

Securing Your Cloud Applications

Jerry Hook
CTO

Agenda

Introduction

ICG's Approach & Value We Deliver

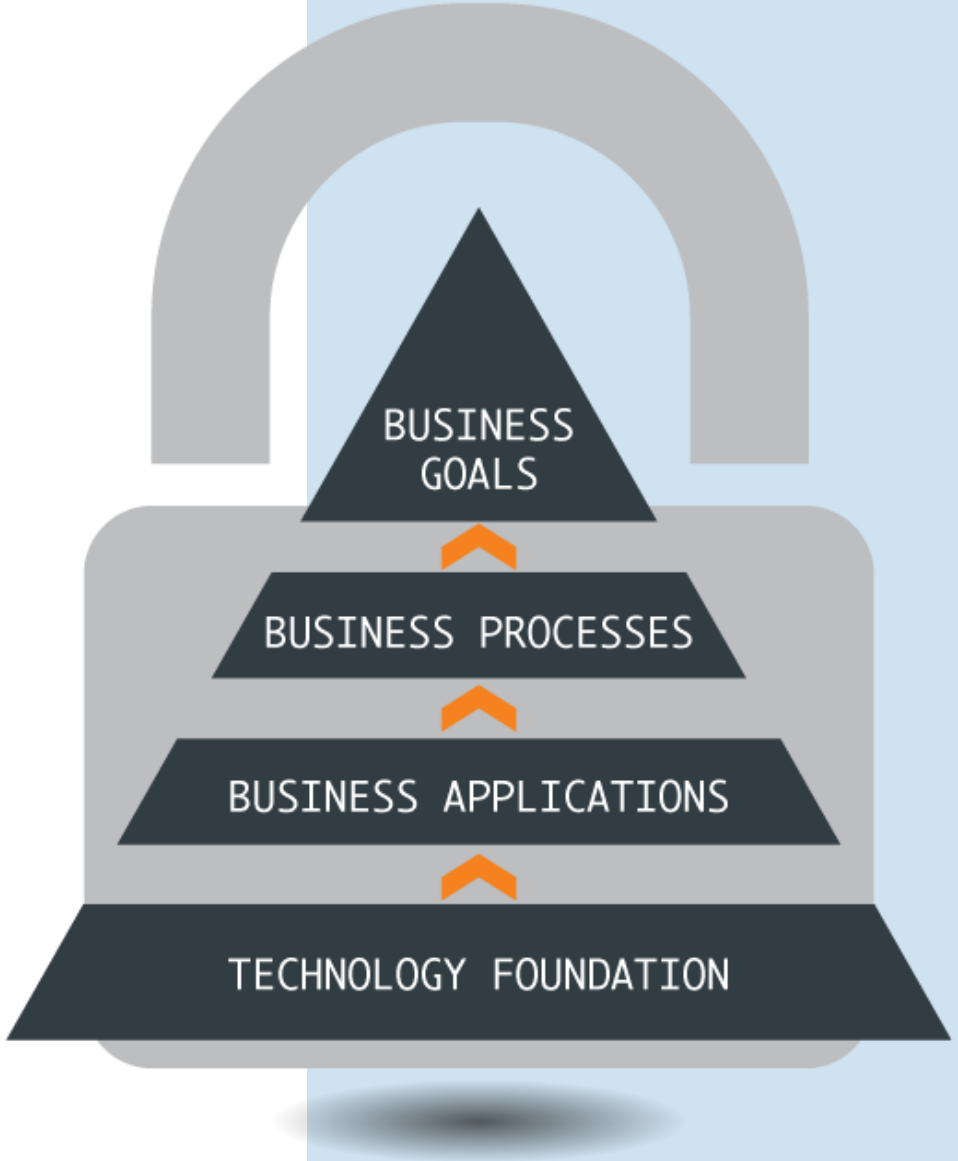
Securing Your Cloud Applications

Discussion & Next Steps

The ICG Approach

A solid **technology foundation** delivers your **business applications** when and where you need them. These two combined implement your unique **business processes**, allowing you to reach your **goals**.

ICG is a process-driven business technology company that ensures your IT platform securely delivers your applications and processes whenever and wherever you need them.



OUR MISSION:

Deliver innovative and reliable business and technology solutions that exceed our client's expectations, resulting in reduced cost, improved efficiency, and a guaranteed ROI.

OUR VISION:

Enable enterprises of all sizes to leverage technology for business growth and success.

Value We Deliver

ERP SOLUTIONS

One-Stop Shop for Fourth Shift, VISUAL, Acumatica

- Sell ERP
- Cloud Hosting
- Implementation
- Optimization
- ERP Upgrades
- Training
- Develop/Customization
- And More!

ICG is uniquely qualified with both IT and ERP under one roof!

IT SERVICES

We Architect & Implement Strategic IT Solutions:

- Managed Services
- Technical Support
- Cybersecurity
- Cloud Infrastructure
- Data Center Infrastructure
- Virtual Desktop Infrastructure
- TSR and Health Checks
- And More!

Aren't my Cloud Apps Secure Already?

ARE CLOUD APPLICATIONS SECURED BY VENDOR?

WHY YOU NEED TO LOOK AT CLOUD APPLICATION SECURITY

- **Myth:** The vendor is responsible for keeping my data secure!
- **Fact:** Most vendors are not responsible—it is documented in the EULA they have zero liability if your data is compromised.
- SaaS constitutes the fastest-growing cloud attack surface.
- Average Large Enterprise has over 200 SaaS applications in use.
- Maintaining user access and security is extremely difficult.
- Protecting data loss from external and internal sources is difficult.

Four Common SaaS Security Pitfalls

Visibility to Attack Surface

- SaaS applications typically do not give IT complete oversight on data and security
- IT is reliant on vendor for security protocols
- Another password for users to manage

Misconfiguration Risks

- Flexibility in SaaS applications increase chance of security misconfigurations
- Maintaining security across multiple SaaS applications leads to misconfiguration

Configuration Drift

- SaaS is highly customizable but also dynamic, changes by vendor (updates or upgrades) can affect security settings
- Adding new users and privileges changes with updates

Broader Attack Surface

- 3rd party app integrations broaden attack surface
- Create SaaS to SaaS connections enable unsanctioned 3rd party apps to access data, potentially gaining access to write or delete data

Systems to Help Protect SaaS Applications

Cloud Access Security Broker (CASB)

- Monitors and controls the use of cloud services
- Inspects network traffic and visibility into user access including DLP

Secure Access Service Edge (SASE)

- Primarily focus on network security connecting users to applications
- Allows companies to incorporate a secure VPN between sights managing from one location
- VPN for users is zero trust connecting to cloud VPN instead of internal networks

Secure Web Gateways (SWG)

- Also known as web proxies, they control traffic to SaaS applications and enforce compliance policies
- SWGs do not do well when users are outside corporate network and bypass SWG for access to SaaS applications

Must DO to Protect SaaS Applications

- Multi Factor Authentication: All SaaS applications must have MFA in place

- Password Management: Tools to help users maintain the multitude of passwords, SSO, Key pass, IT-Glue

- Identity and Access Management (IAM)
- Principal of least privileges as a rule for each applications
- Role Based Access (RBAC)

Must DO to Protect SaaS Applications

- Ensure Data Encryption is in place
- Employee Training: Human error is still single most significant factor in security breaches
- Data Backups and Recovery
- Special backup tools might be needed for cloud backups that traditional backups do not have access to

Discussion and Questions

www.ICGTechnology.com

Thank You!

www.ICGTechnology.com