MASTERING POWER PLATFORM SECURITY

Sep 19, 2025

Stalin Ponnusamy

protiviti®
Global Business Consulting

Stalin Ponnusamy

Associate Director, Protiviti
Enterprise Architect
Power Platform & D365 CE Lead

Enterprise Technical Architect
Practice Lead

IT Consultant Veteran of 21 years

Power Platform Enthusiast | Customer Experience MVP | D365 CE Specialist
Learntoilluminate.com (Learn To Illuminate)

linkedin.com/in/stalinponnusamy

@stalinponnusamy

LEARN to ILLUMINATE

protiviti

M365 TWIN CITIES

Please thank our sponsors

SECURE ITnet

DEVICIE

highmonkey

sdg

AvePoint

MYTECH PARTNERS

SkyNorth SOFTWARE

RBA

tiviti

Submit session feedback

M365 TWIN CITIES

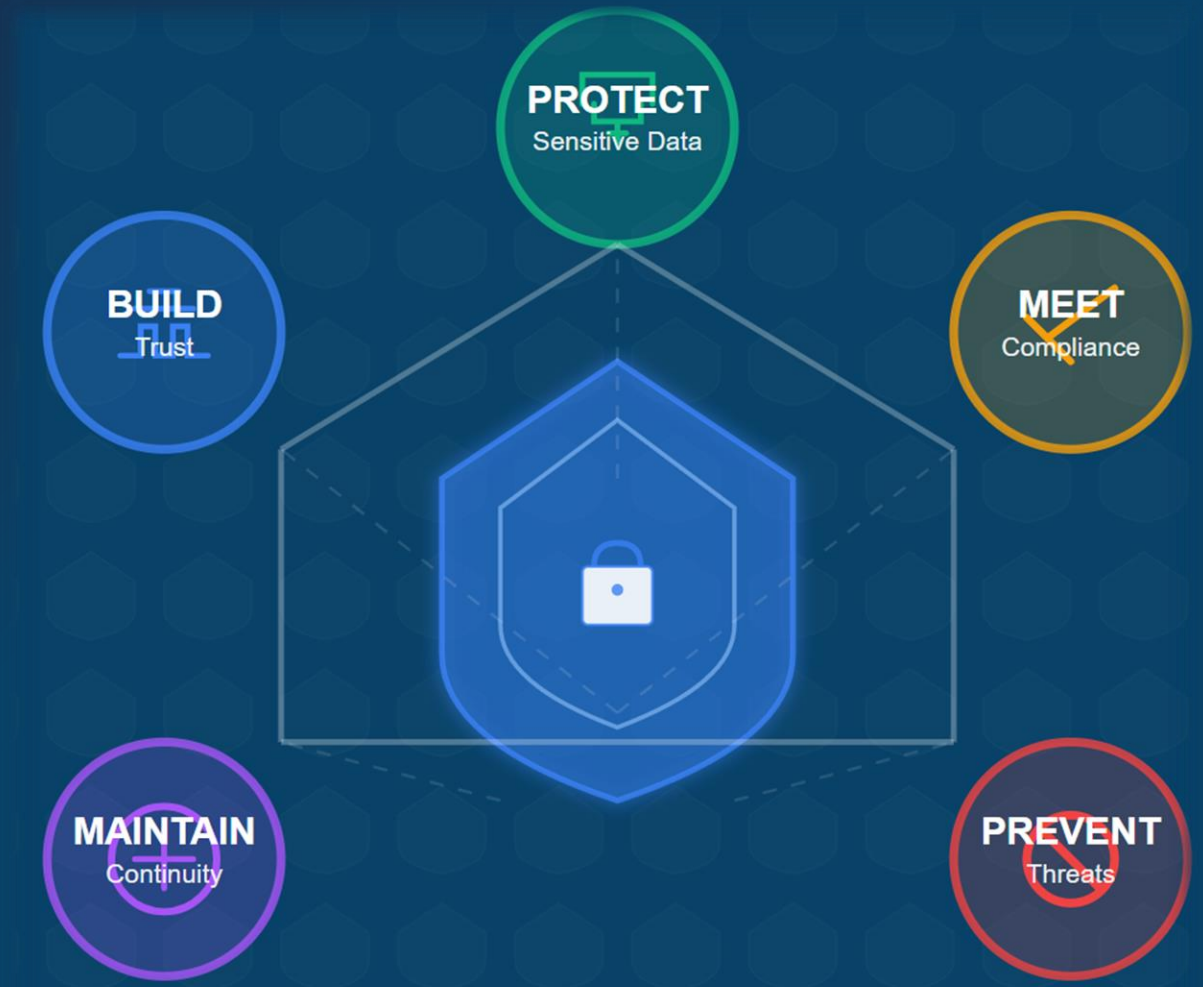
Overview

- Security Layers
- Environment Security
- Best Practices
- Monitoring & Compliance
- Key Takeaways
- Q&A

Security

protiviti®

Why Security Matters



protiviti®

Why Security Matters

2024 IBM Cost of a Data Breach Report - https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

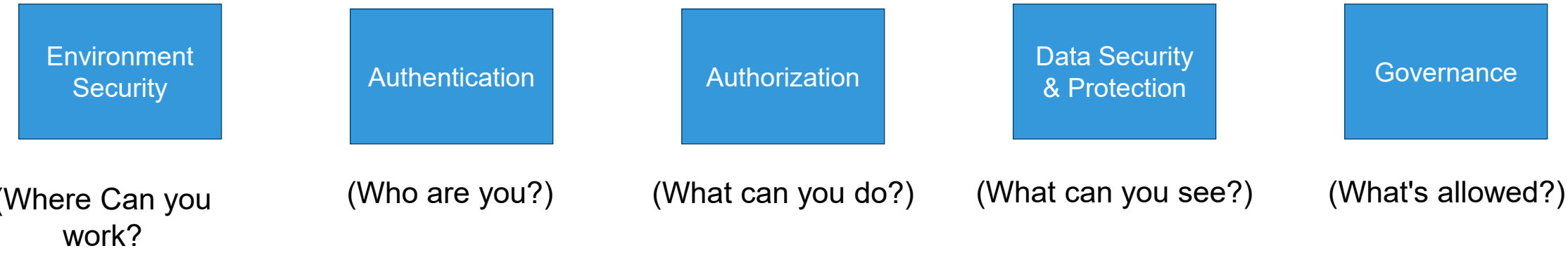
Industry-Specific Costs

- Healthcare: $9.77 million
- Financial services: $6.08 million
- US organizations: $9.36 million

Average global data breach costs $4.88M

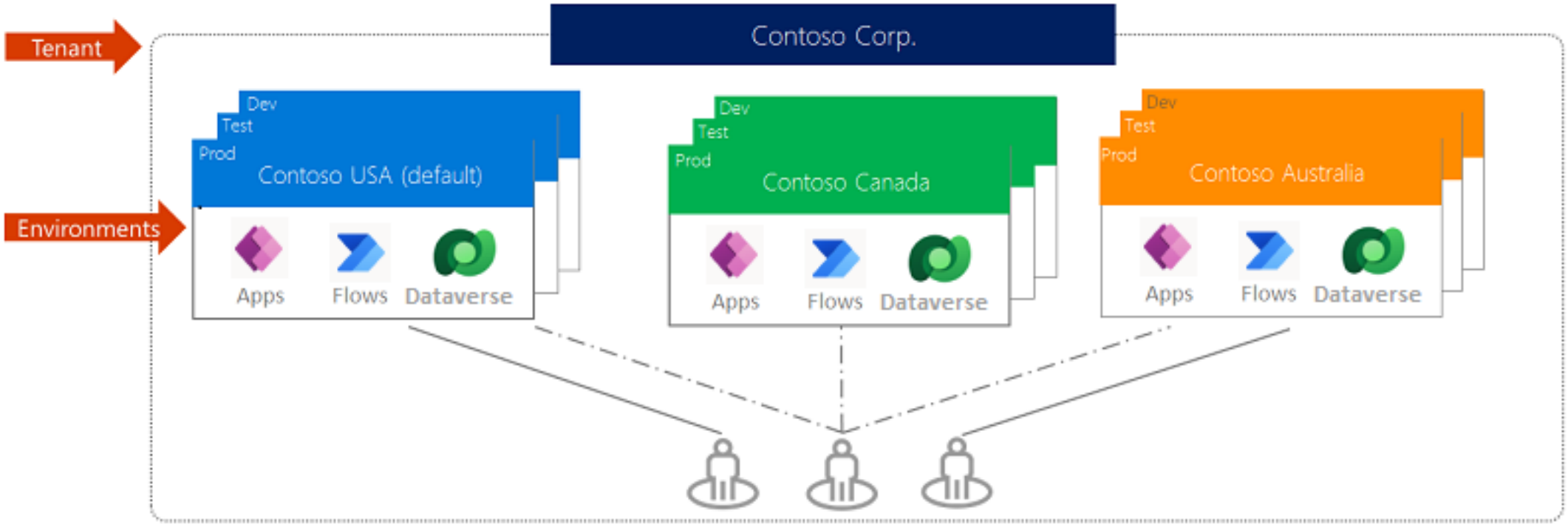
protiviti®

Security Layers Overview



protiviti

Environments



Environment Level Security Group

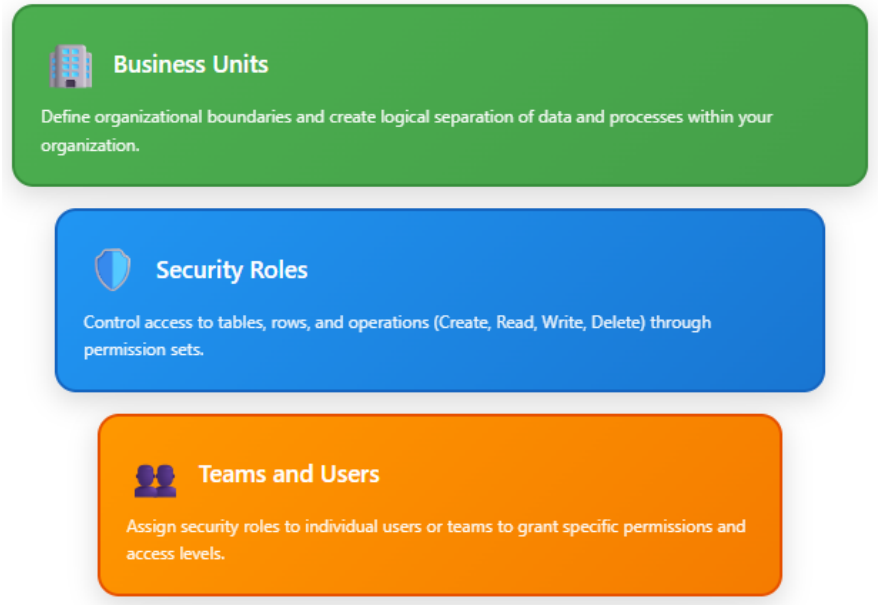
protiviti

Authentication

- ❑ Azure AD / Entra ID integration
- ❑ Multi-Factor Authentication (MFA)
- ❑ Conditional Access policies
- ❑ Single Sign-On (SSO)

Example: MFA when logging in from unknown device

Authorization



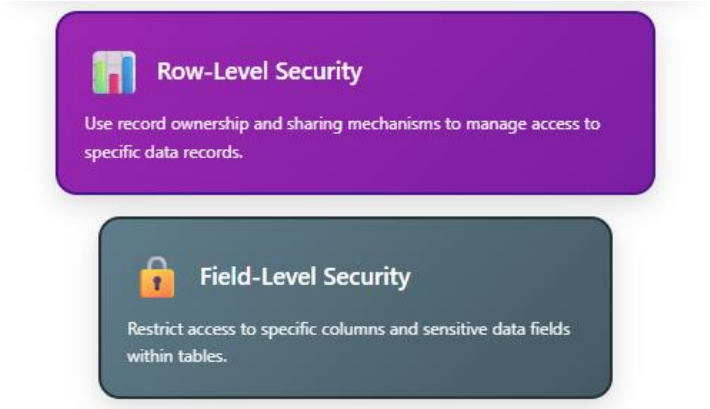
Company's divisions, departments, or geographical locations

Define what actions users can perform on different types of data

Organize users into teams for easier management. Teams can own records and have security roles assigned

protiviti

Data Security & Protection



Control which specific records users can access based on ownership

Secure sensitive information by restricting access to specific columns

protiviti

Security Model

Company's divisions, departments, or geographical locations

Define what actions users can perform on different types of data

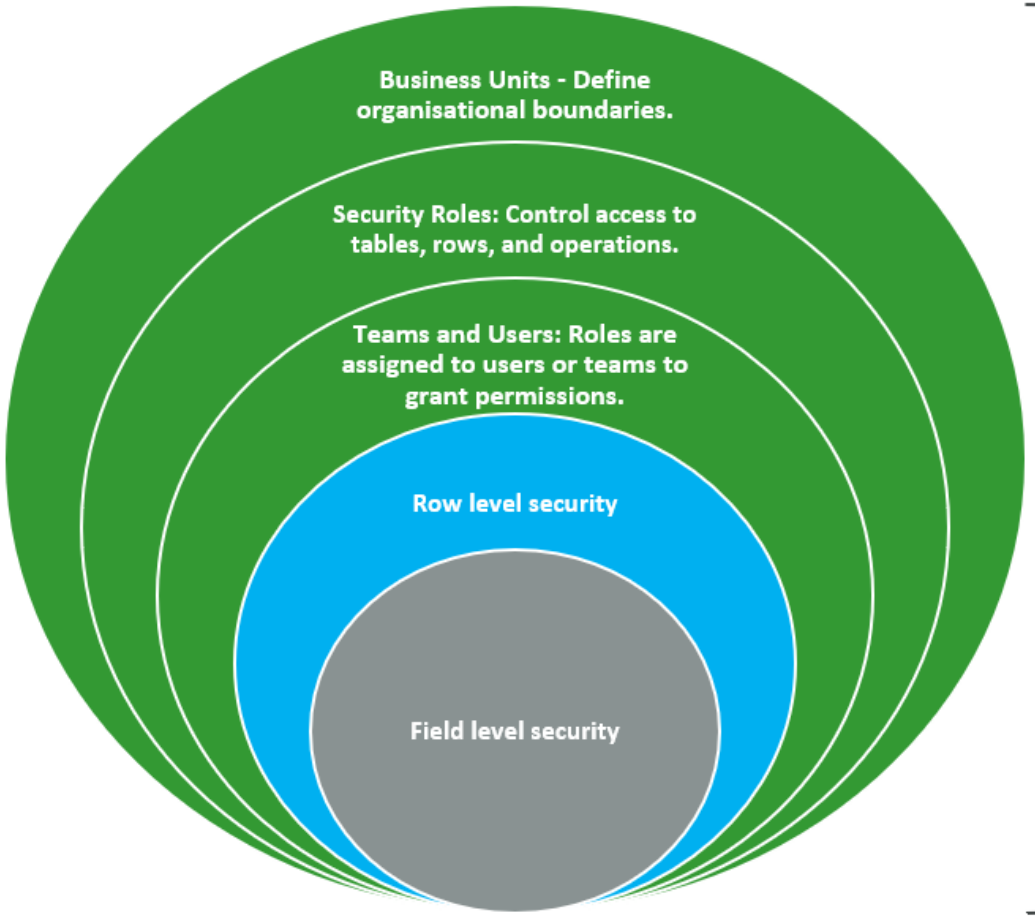
Organize users into teams for easier management. Teams can own records and have security roles assigned

Control which specific records users can access based on ownership

Secure sensitive information by restricting access to specific columns

protiviti

Security Model



- **Business Units**: Define organizational boundaries.
- **Security Roles**: Control access to tables, rows, and operations (read, write, delete).
- **Teams and Users**: Roles are assigned to users or teams to grant permissions.
- **Row-Level Security**: Uses record ownership and sharing to manage access.
- **Field-Level Security**: Restricts access to specific columns in a table.

protiviti

Owner Team

Purpose: Own records, inherit security roles, and can be assigned as record owners.

Membership: Users + can be linked to Azure AD Security Groups.

Scope: Full role-based access + can own & manage records.

Use Case: Departmental ownership (e.g., Sales Team, Customer Support).

Access Team

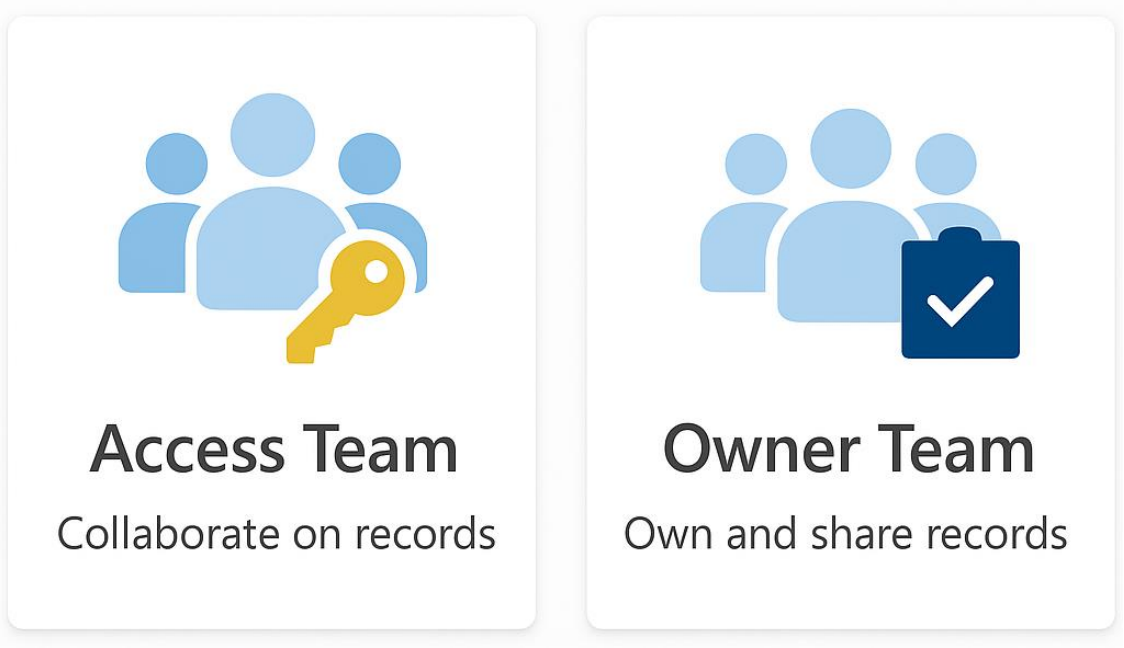
Purpose: Provide ad-hoc, flexible access to individual records.

Membership: Users are manually added (no security roles by default).

Scope: Record-specific access (Read, Write, Append, etc.).

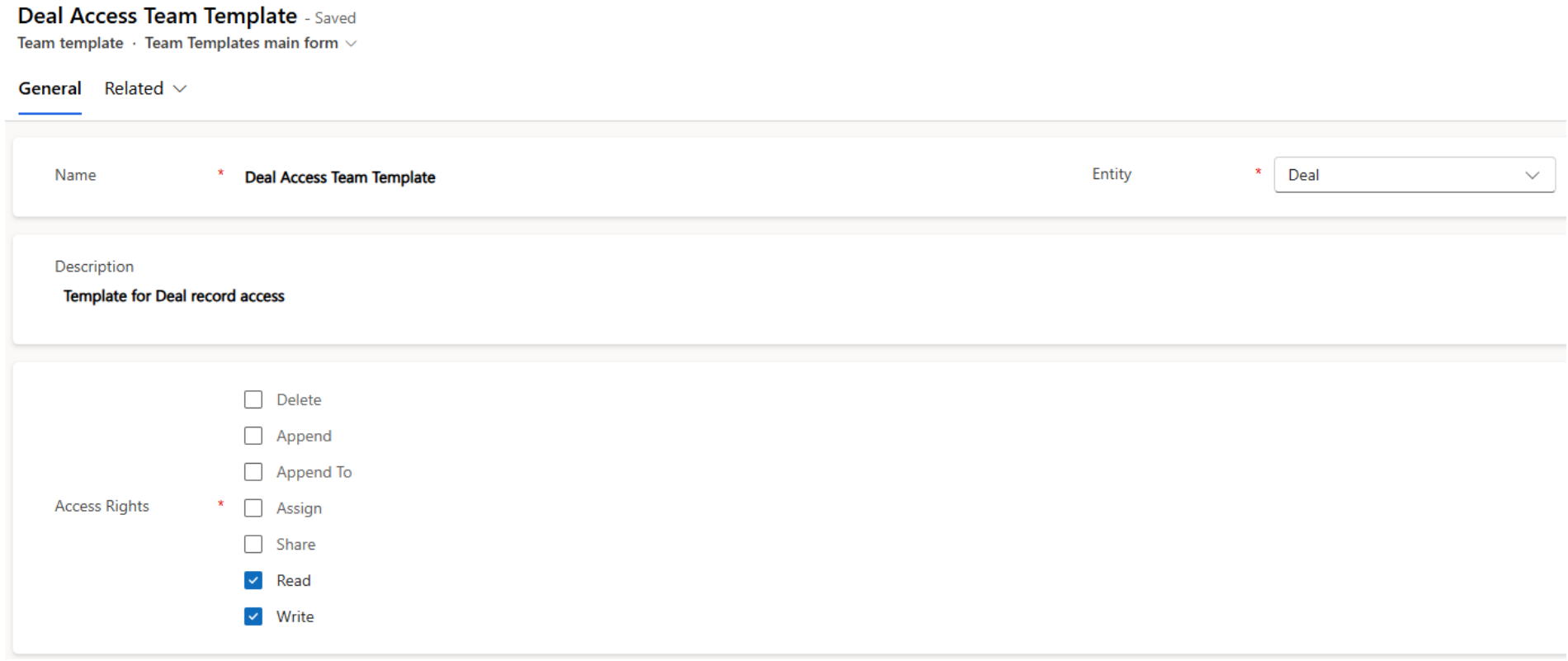
Use Case: Share a single opportunity, case, or deal with a group of users for collaboration.

Comparison : Access Team vs Owner Team



protiviti

Access Team Template



protiviti

Record-Level Security

- Record Owner
- Sharing models: Manual, Team, Cascade

Use Case : Record-Level Security Example

Status	Who Can View	Owner (Team)	Access Team/Grant Access
Draft	• Only to DC (DC Team) and Read & Write access	DC Team	None
Submitted For Approval	• Only tagged Lead PM	DC Team	Tagged Lead PM (Only One PM)
Approved	• Lead PDM can Archive • All SPARK Users - Read Only	Finance BU Team	Tagged Lead PM

User/Team	Access Level
DC Team	Read and Write access to all records
Finance BU Team	Read only Access for All records
Tagged Lead PM	Write access to Deal and related tables

Sharing

Definition: Directly granting a user or team access to a specific record.

Scope: Record-level only (Read, Write, Append, etc.).

Flexibility: Very granular but can become hard to manage if many users need access.

Ownership: Does not change record ownership.

Best For: Quickly granting access to 1–2 users without creating a team.

Limitation: If multiple records or multiple users are involved, administration becomes complex.

Comparison : Sharing vs Access Team

Feature	Sharing	Access Team
Type of Access	Record-level	Record-level (via template)
Ownership	❌ Does not own records	❌ Does not own records
Scope	Individual record	Individual record
Management	Harder if many users	Easier (group-based)
Security Role Support	❌	❌ (template-based permissions)
Best For	1–2 users ad-hoc	Multi-user collaboration

Field-Level Security

- Restrict access to sensitive fields (salary, SSN)
- Controlled via Field Security Profiles
- Example: HR can see salary, Sales cannot

HR User View	Sales User View
Name: John Doe Dept: Sales Salary: $75,000 Phone: 555-1234	Name: John Doe Dept: Sales Salary: ******** Phone: 555-1234

Tenant Level Security

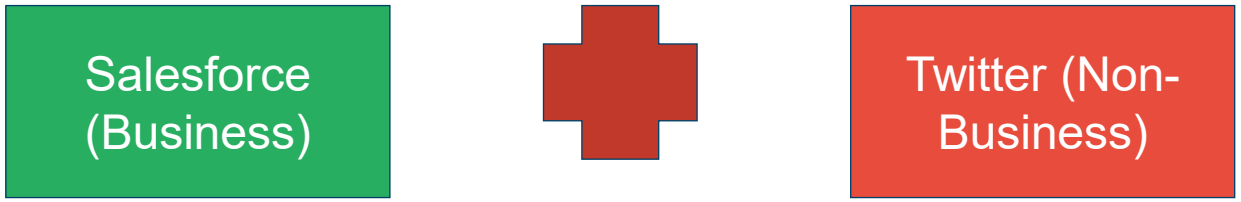
- Environment Security Group
- Customer Managed Encryption Key (CMK)
- Data Policy
- Azure Virtual Network Policies
- IP Firewall
- Tenant Isolation

Tenant Level Security - Compliance

- Auditing
- Temp Access to MS Engineer for Troubleshoot

DLP Policies

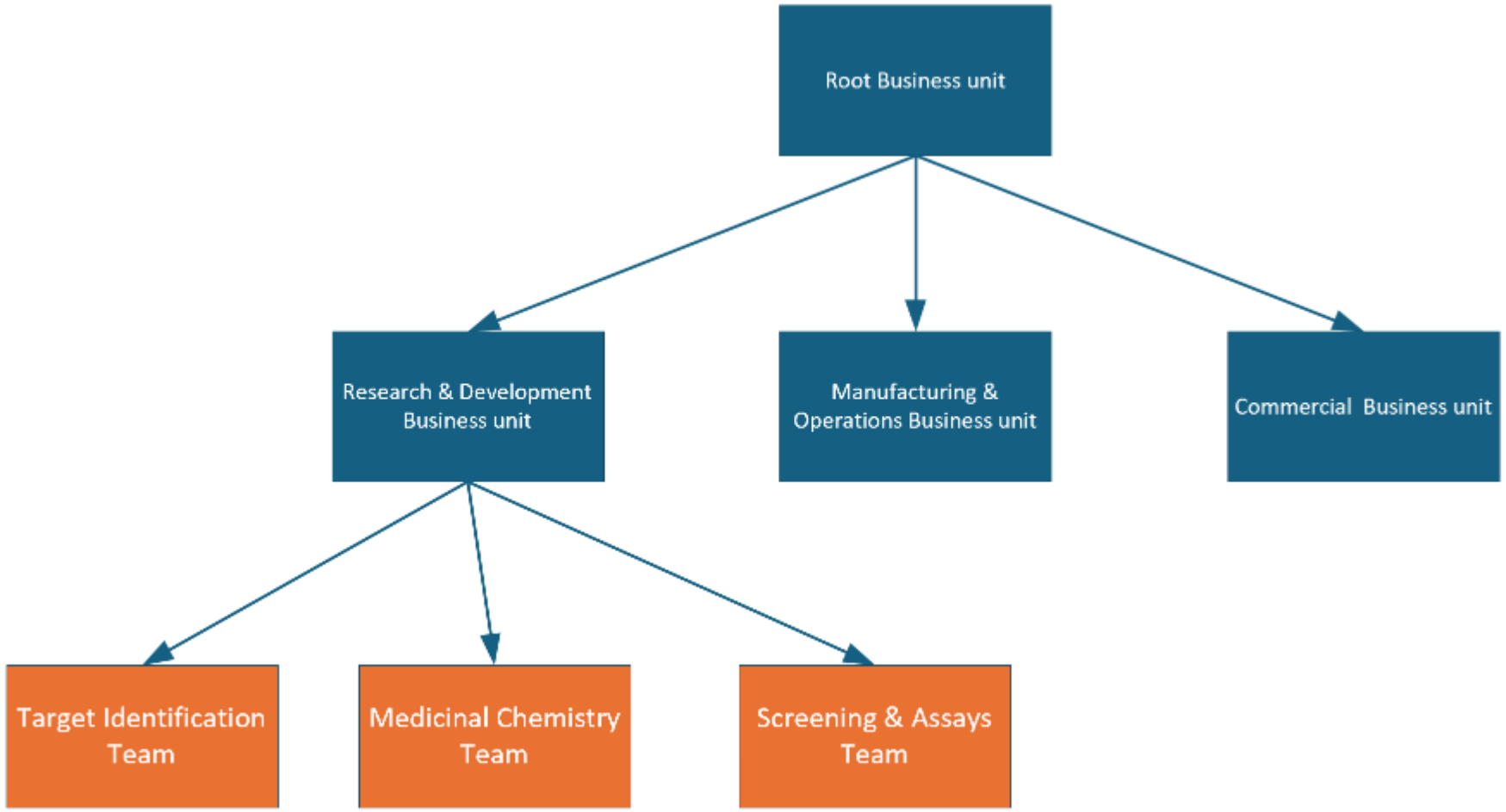
- Separate Business vs Non-Business connectors
- Example: Allow Salesforce + Block Twitter



Example

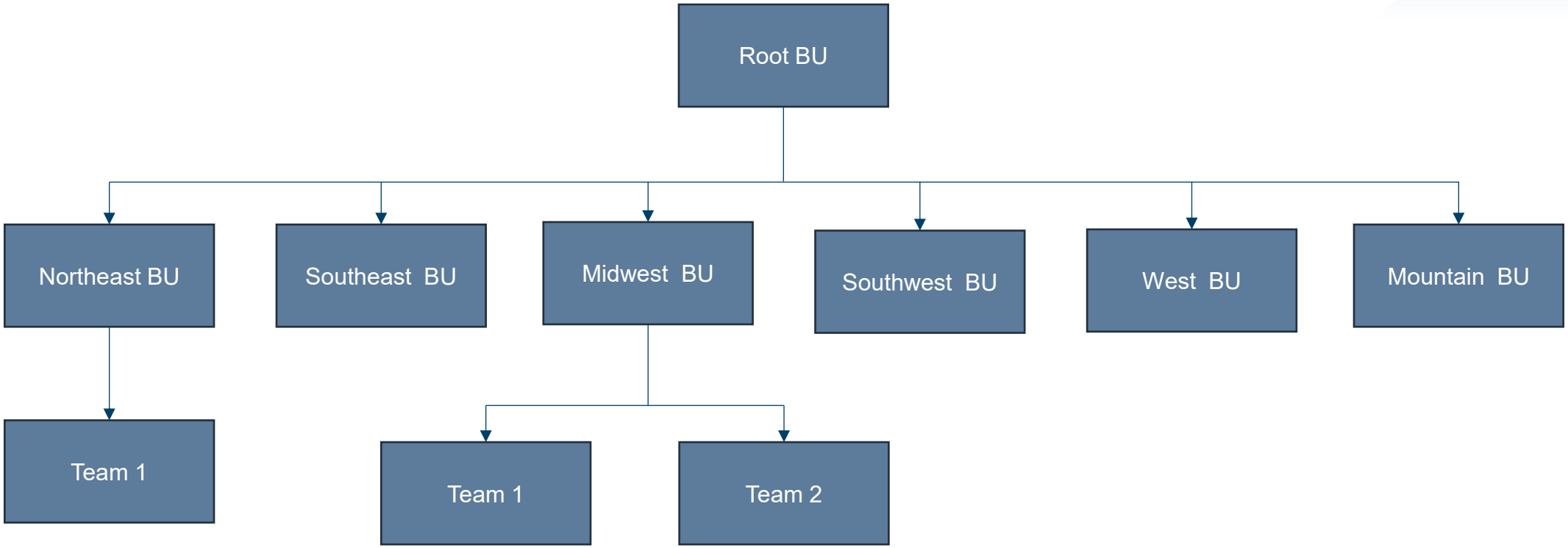
protiviti®

Example 1

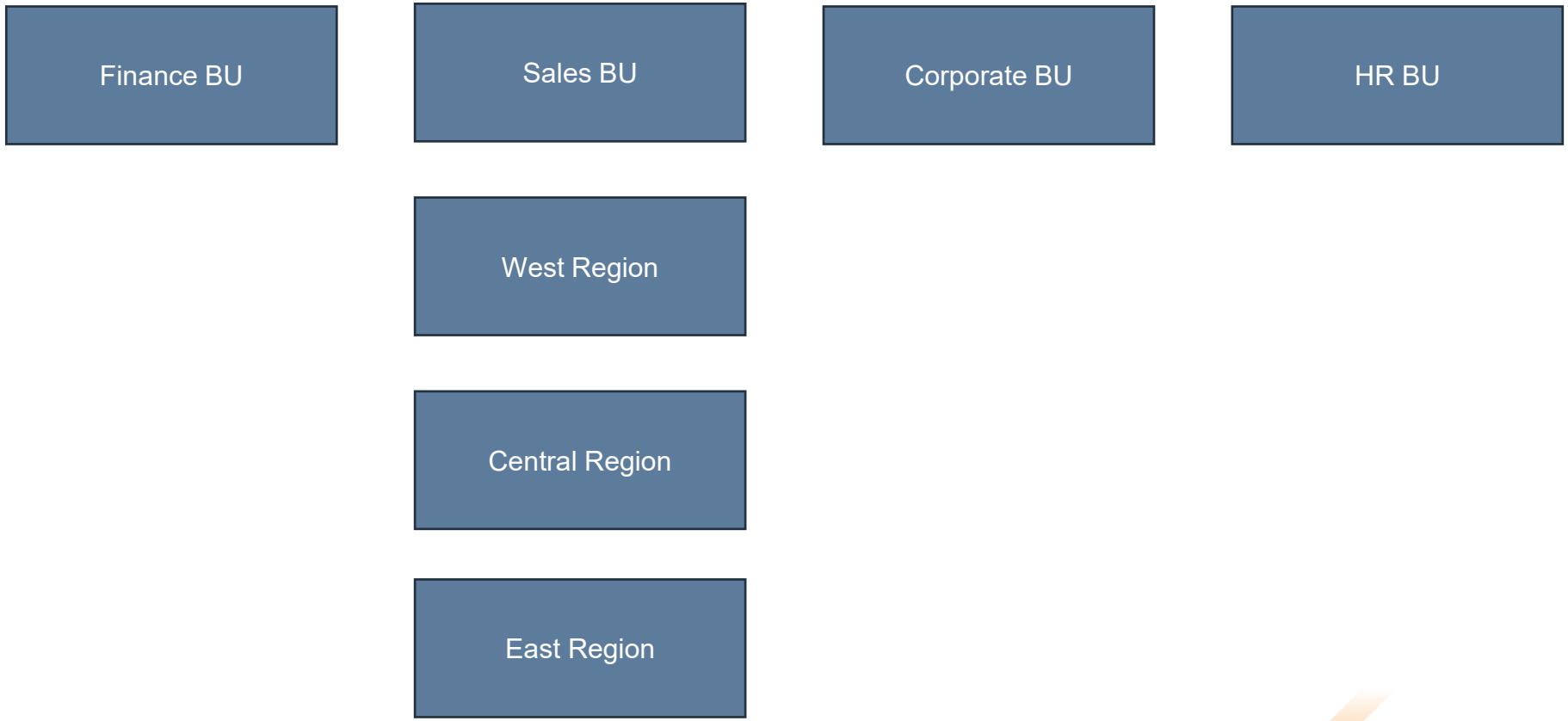


protiviti

Example 2

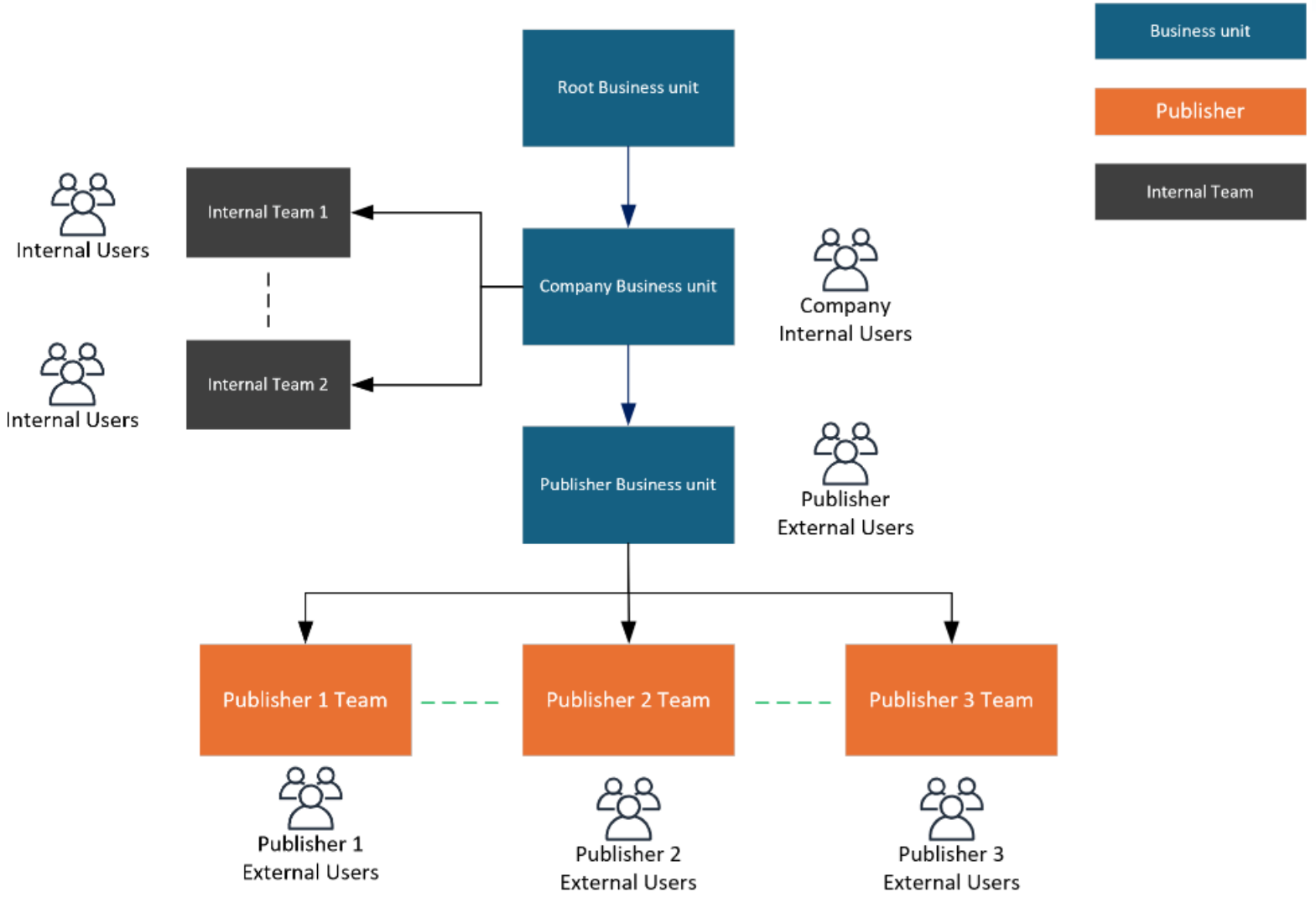


Example 3



protiviti

Example 4



protiviti

More Security

protiviti®

Best Practices

- ❑ Assign roles to Teams (not individuals)
- ❑ Map to Azure AD groups
- ❑ Follow least privilege principle
- ❑ Monitor via audit logs
- ❑ Conduct regular reviews

Common Mistakes

- ❑ Giving System Admin role broadly
- ❑ Skipping Business Unit design
- ❑ Ignoring DLP policies
- ❑ Not using field-level security
- ❑ Poor documentation of security model

Monitoring & Compliance

- ❑ M365 Security & Compliance Center
- ❑ Activity logging, retention, reporting
- ❑ Monitor: failed logins, data exports, privilege escalations

Troubleshooting Common Issues

- ❑ User can’t see records → Check BU + role
- ❑ Field hidden → Verify FLS profile
- ❑ Flow blocked → Review DLP policies
- ❑ Access denied → Validate entity permissions

Key Takeaways

- ❑ Authentication = Who are you?
- ❑ Authorization = What can you do?
- ❑ Data = What can you see?
- ❑ Governance = What's allowed?
- ❑ Security requires ongoing monitoring & improvement

Q&A

Think Security First when building apps

protiviti®

Thank You

Stalin Ponnusamy

Associate Director, Protiviti US

linkedin.com/in/stalinponnusamy

@stalinponnusamy

LEARN to ILLUMINATE

Submit session feedback

M365 TWIN CITIES

protiviti

Face the Future with Confidence®

protiviti®
Global Business Consulting