ZERO TRUST FOUNDATION

Digital Workplace

REPLY
VALOREM

MODERN DIGITAL WORKPLACE

Outcomes of a Modern Digital Workplace

- Attract/Retain the Best Talent
- Gain/Maintain Competitive Advantage
- Build/Keep Deep Customer Connections
- Get/Stay Secure and Compliant
- Lower operational IT costs
- A Platform for Continuous Innovation (Evergreen)
- A Great User Experience

Maturity Cycle

1 Standardize
2 Modernize
3 Transform
4 Innovate

Mobile Work/Customers/Partners/Vendors/3rd Party SaaS Providers

Modern Protection

| Identity | Security | Compliance | Privacy |

Enterprise Mobility & Security

Modern Workplace

| Modern Intranet "Who We Are" | Modern Apps "What We Do" | Modern Collab "How We Do It" |

PowerApps · Power BI · Microsoft Dynamics 365

Office 365

Modern Device

| Windows | Mac | Tablet | Phone |

Windows Enterprise + Office 365 Pro Plus + O365 Mobile Apps

VALOREM REPLY ENTERPRISE SECURITY FOCUS AREAS

THREAT
Protect, Detect, Respond

CLOUD
Security Strategy & Tactics

SIMPLIFY
Security for All Users

CLOUD SECURITY ENGAGEMENT TYPES

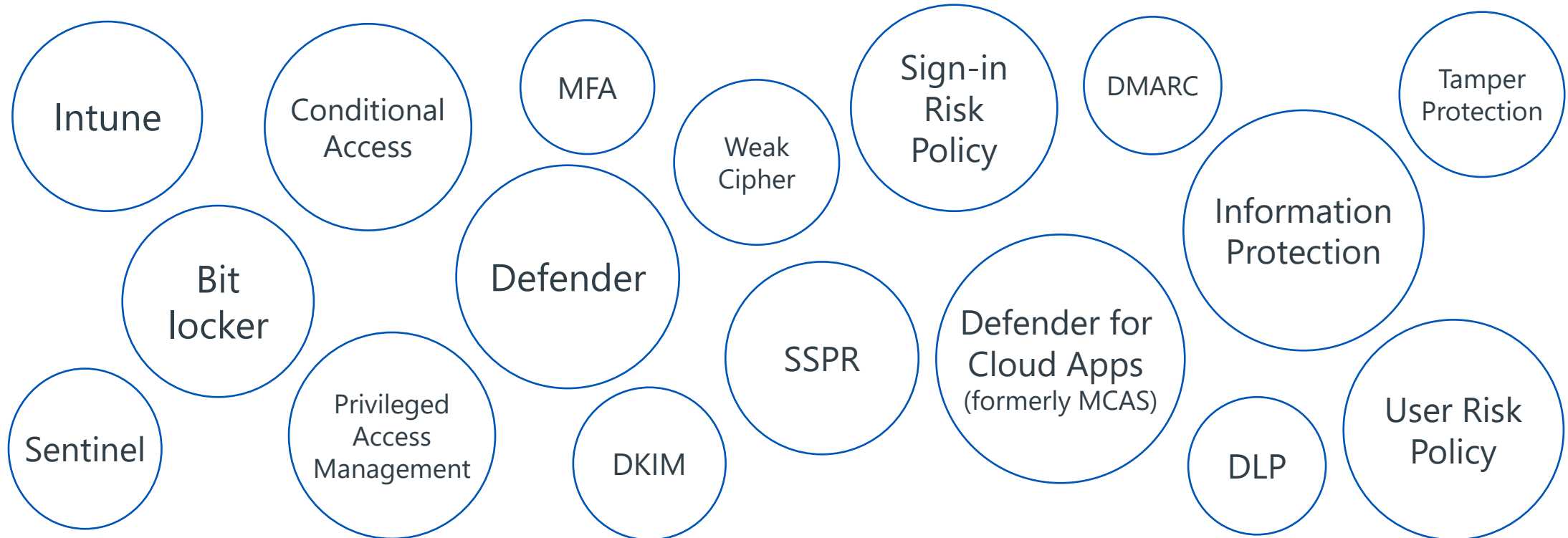| Workshop	Inform, Demo, ADS	The Challenge	The Possibilities	Critical Controls	Best Practices
Immersion	Roundtable	Strategy	HANDS-ON IMMERSION	Threat Protection	PDR
Assessment	Cloud Cybersecurity Posture	Identify Gaps & Needs	Create a Strategic Roadmap		
POC	Experience capabilities in your environment	Identify how the solution aligns to your unique needs	Explore opportunities for integration		
Deploy	Production Pilot	Full Deployment of tactical solution	M365 SSAGA (Strategy, Security, Architecture, Governance & Adoption)		
Operate	MDR	Virtual DPO			

OUR PHILOSOPHY

Security is part of everything we do

Whether it is helping our clients harden their security on Microsoft 365, Azure, data platforms or applications, we take an integrated and wholistic approach to protecting digital assets.
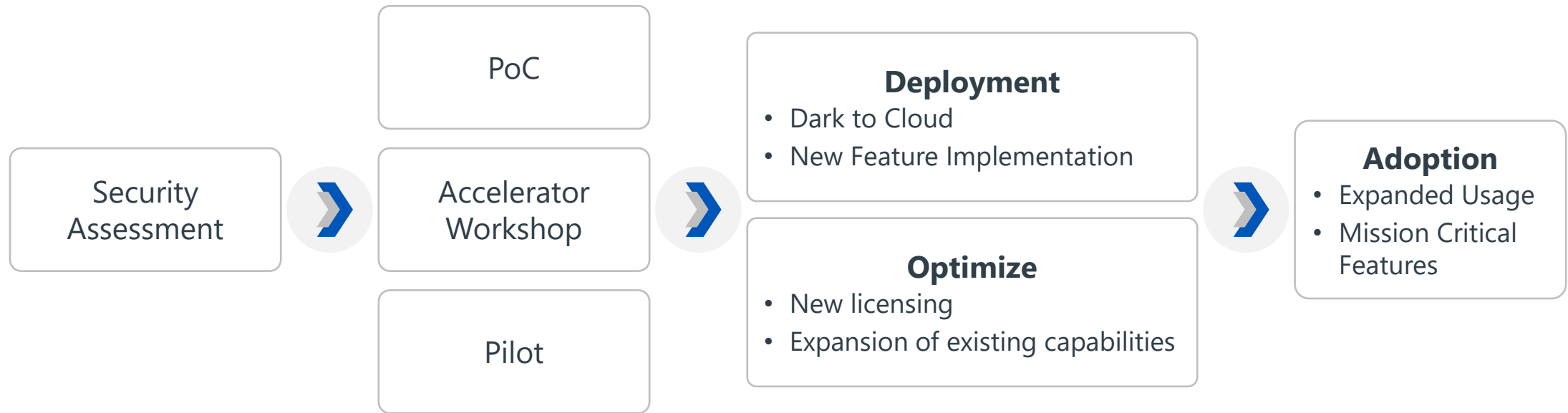
Intune

Conditional Access

MFA

Weak Cipher

Sign-in Risk Policy

DMARC

Tamper Protection

Bit locker

Defender

Information Protection

Sentinel

Privileged Access Management

DKIM

SSPR

Defender for Cloud Apps (formerly MCAS)

User Risk Policy

DLP

OUR APPROACH

Enable and Empower our Clients

With a detailed analysis, clear recommendations, and a strategic roadmap, we help our clients solve complex security challenges and prepare to face ever-evolving threats, starting with our assessments.

Security Assessment

PoC

Accelerator Workshop

Pilot

Deployment
- Dark to Cloud
- New Feature Implementation

Optimize
- New licensing
- Expansion of existing capabilities

Adoption
- Expanded Usage
- Mission Critical Features

Training, Enablement and Adoption

THE PROCESS

A Summary of our Steps

1 **UNDERSTAND**

Learn about the current state and where the client is on their security and zero trust journey.

2 **ANALYZE**

Develop insights and identify opportunities to make improvements.

3 **RECOMMEND**

Prioritize remediation items and longer-term implementation goals within the context of business goals.

4 **DO**

Follow through on remediation tasks, and implement new security features, eliminating third party tools where possible.

OUR SECURITY OFFERINGS

Beyond the Assessment

- **Cloud Security Solution Accelerator**
  Rapidly adopt the latest Microsoft security technologies using trial licenses to leverage read data in your actual environment. Leverage Microsoft funded accelerator programs to supplement/kick start modern security solutioning.

- **Security Assessment**
  Evaluate security readiness, identify potential risks, and make recommendations for hardening security. This includes product and licensing recommendations (e.g., **E5, Defender for Cloud Apps, Microsoft Endpoint Management**, etc.). Types of assessments include Microsoft 365, Compliance, Cybersecurity, and Secure Collaboration.

- **Protect Sensitive Data**
  Evaluate sensitive data policies, encryption, usage and user policy understanding. Build a roadmap for **Microsoft Information Protection** implementation. Execute and support deployment and training.

- **Manage and Investigate Risk**
  Support implementation of SOC and threat management tools like **Defender** and **Sentinel**.

- **Modernize Security and Establish a Zero Trust Foundation**
  Build a modern security and identity infrastructure that creates a foundation for zero trust. This includes migrating to Azure **Active Directory**, Implementation of **Privileged Identity and Access Management**, and **Conditional Access**.

MICROSOFT 365 CLOUD SECURITY ACCELERATOR

Summary

A completely customized security solution designed for security leaders with Microsoft 365 E3 or E5 licensing who want to reduce information security risk in their environment, cut 3rd party security costs, and progress their journey to a modern zero trust strategy.

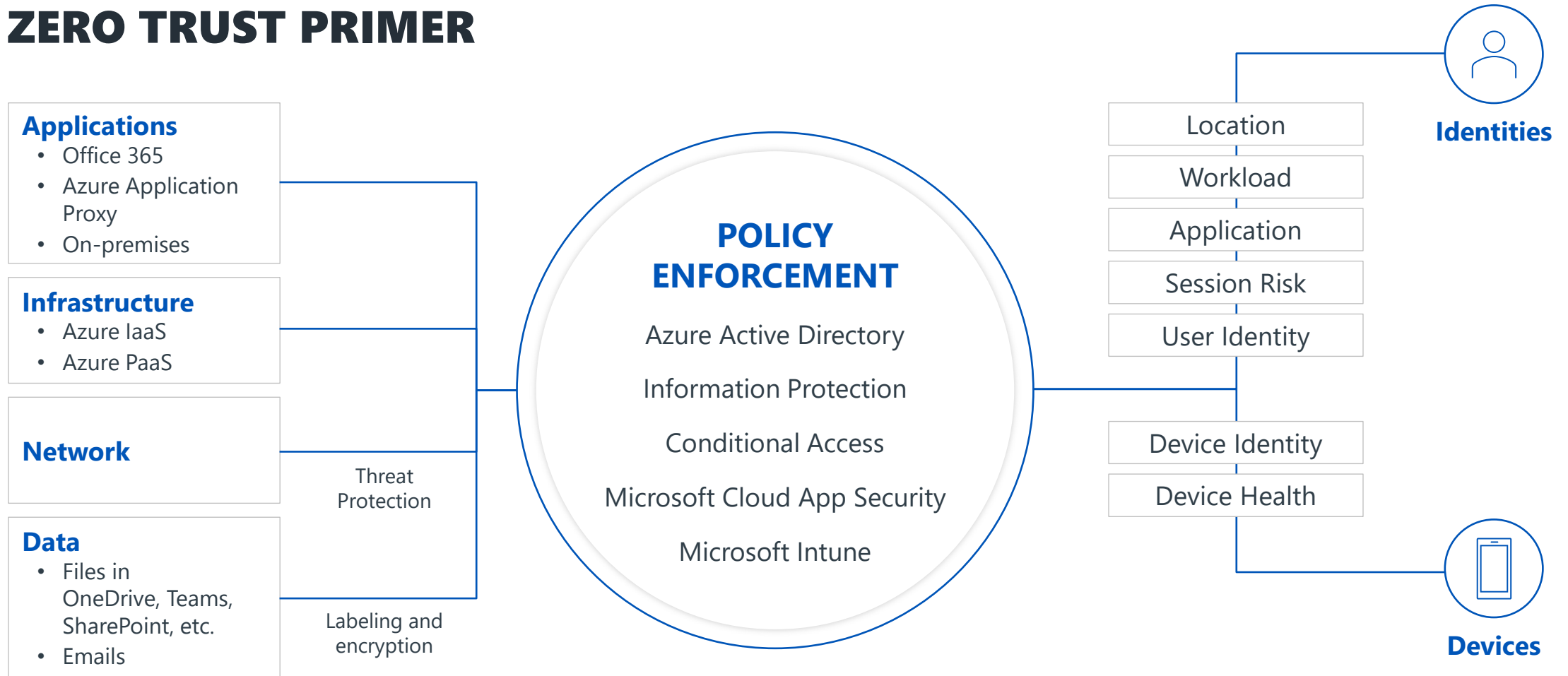|		
Duration	🕐	6 – 8 Weeks
Investment	💲	$50,000 - $75,000
Deliverables	↗	• Summary of the initial requirements. • Requirements and solution design tailored to your specific needs to advance their zero trust capabilities and security posture. • Custom solution design document. • Implemented solution.
Outcomes	📈	• Reduced information security risk. • Accelerated progress down the zero trust journey. • Better threat management.

ZERO TRUST PRIMER
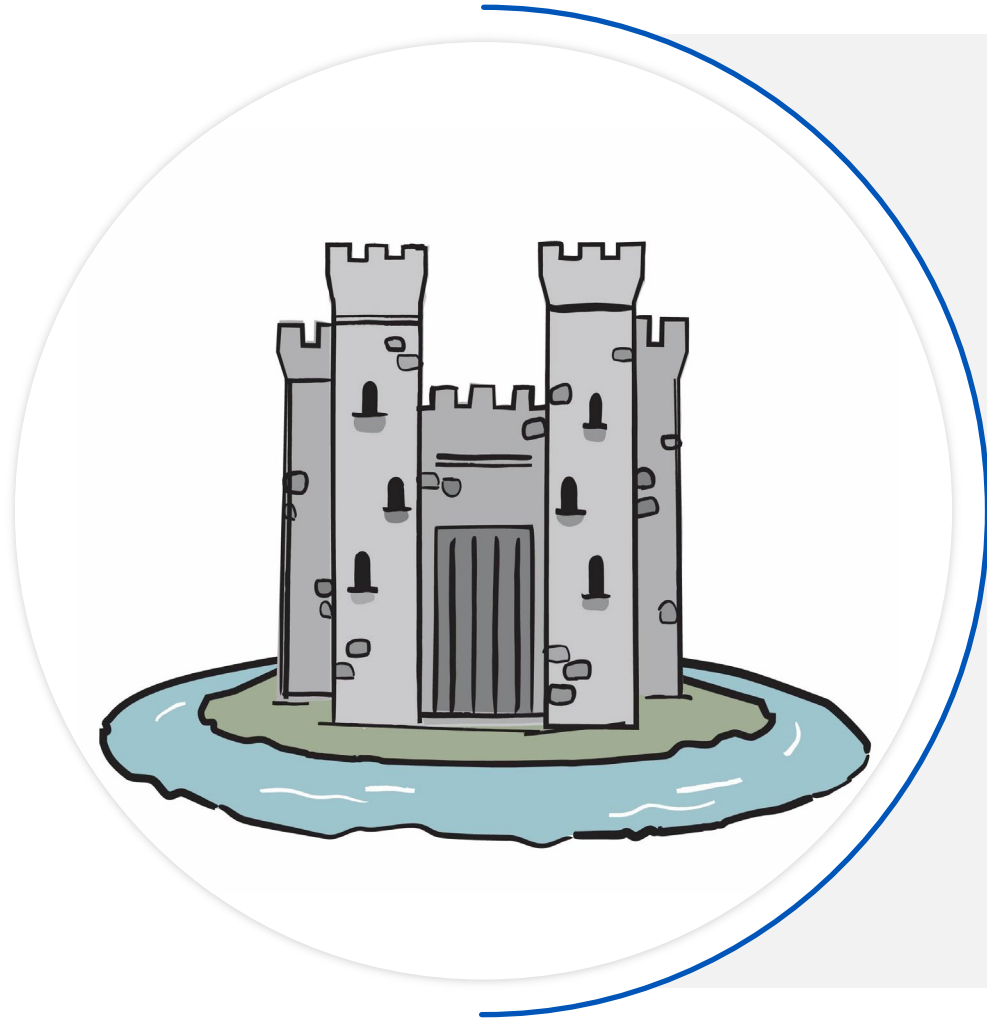
CASTLE AND MOAT

This is where most organizations generally sit today if they haven't started their Zero Trust journey:

- On-premises identity with static rules and some SSO.

- Limited visibility is available into device compliance, cloud environments, and logins.

- Flat network infrastructure results in broad risk exposure.

ZERO TRUST PRIMER

Applications
- Office 365
- Azure Application Proxy
- On-premises

Infrastructure
- Azure IaaS
- Azure PaaS

Network

Data
- Files in OneDrive, Teams, SharePoint, etc.
- Emails

Threat Protection

Labeling and encryption

POLICY ENFORCEMENT

Azure Active Directory

Information Protection

Conditional Access

Microsoft Cloud App Security

Microsoft Intune

Identities

Location

Workload

Application

Session Risk

User Identity

Device Identity

Device Health

Devices

GUIDING PRINCIPLES OF ZERO TRUST

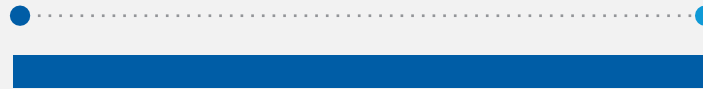**1** Verify explicitly.

2 Use least privileged access.

3 Assume breach.

ZERO TRUST FOUNDATION

Whether just starting our or advanced, Valorem's completely customized solution can accelerate your unique zero trust journey to reduce information security risk and better manage threats.

Phase 1

Assess & Plan
Assess your current security posture to identify the most impactful next step on your zero trust journey.
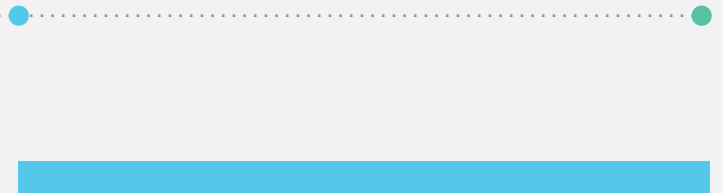
Phase 2

Build
Valorem Security Architects will gather requirements and design the highest value solution for your environment.

Phase 3

Deploy
Ensure protection services are configured according to planned architecture/design and deploy your custom zero trust solution.

THANK YOU

DOUG HEMMINGER

Director, Digital Workplace

dhemminger@valorem.com

+1 (816) 406-1566