

SECURITY COMPASS FRAMEWORK

Security at cloud-speed.

 **Microsoft**
Solutions Partner
Microsoft Cloud

 **Microsoft**
Solutions Partner
Security

Specialist
Cloud Security
Identity and Access
Management
Information Protection and
Governance
Threat Protection

 **REPLY**
VALOREM



ORGANIZATIONS HAVE THE OPPORTUNITY TO SIMPLIFY AND OPTIMIZE SECURITY TO MOVE AT CLOUD SPEED.

Embracing the path to a fully integrated enterprise security system empowers organizations to refine policies, streamline processes, and enhance skills, ultimately driving improved operations and potential long-term cost savings. Valorem Reply's **Security Compass Framework** is a holistic approach to Security vendor consolidation and solution replacement planning, implementation, and execution.

CHALLENGES

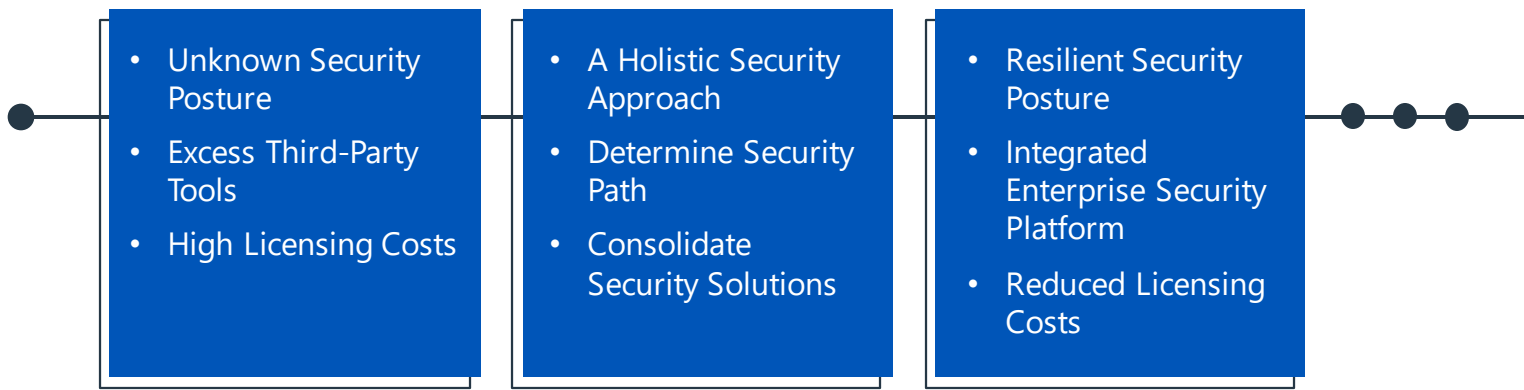
- Unknown Security Posture
- Excess Third-Party Tools
- High Licensing Costs

IDEAL SOLUTION

- A Holistic Security Approach
- Determine Security Path
- Consolidate Security Solutions

DESIRED OUTCOMES

- Resilient Security Posture
- Integrated Enterprise Security Platform
- Reduced Licensing Costs



SECURITY COMPASS FRAMEWORK

Valorem Reply's Security Compass Framework meets you where you are to ensure technical, operational, and skilling changes happen on-time and in-budget with minimal organizational disruption for your unique environment and needs.

1

SECURE IDENTITIES

4

AI GOVERNANCE & RISK MANAGEMENT

2

THREAT PROTECTION

5

COMPLIANCE & RISK MANAGEMENT

3

INFORMATION PROTECTION

6

AZURE SECURITY



WHY VALOREM REPLY'S SECURITY COMPASS FRAMEWORK?

With Valorem Reply's Security Compass Framework, organizations have the choice of where to begin their security journeys in order to meet their unique needs and goals, receiving expert guidance every step of the way.

Executive Briefing

Strategic Evaluation

Security Playbook

Deployment





EXECUTIVE BRIEFING



In an Executive Briefing, Valorem Reply's Security experts will help you understand your current security posture and goals.

- Current Licensing and Renewal Timelines
- What's Happening in Your Marketplace
- How to Do More with Less



STRATEGIC EVALUATION



A Strategic Evaluation is a data-driven analysis where we identify security gaps and priorities, explore new ways to protect and secure data, optimize existing security investments, and reduce 3rd party expenses. Choose between a variety of key modules:

- Zero Trust and Your Security Program
- Get Ready for AI: Governance and Risk Management
- Vendor Consolidation Opportunity Identification and Economics
- Recommendations and Next Steps



SECURITY PLAYBOOK

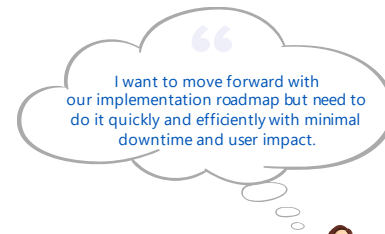


Receive a detailed Security Playbook outlining a roadmap to success in your areas of interest, including:

- Secure Identities
- Threat Protection
- Information Protection
- AI Governance & Risk Management
- Azure Security

Milestones Include:

1. Current Feature Level Deployment
2. Security Architecture / Integration
3. Detailed Implementation Roadmap
4. Business / Contractual Realities
5. Change Readiness Assessment
6. Security Solution Playbook



CAPABILITY DEPLOYMENT



Secure Identities

- SSO
- Directory Services
- Conditional Access
- Risk-Based Controls
- Privileged Identity Management
- MFA
- Identity Governance
- Identity Protection
- User Entity Behavior Analytics

Information Protection & Governance

- Sensitive Data Classification
- Sensitive Data Discovery
- Data Retention
- Information Governance
- Endpoint DLP
- O365 DLP for Emails and Files
- DLP for Microsoft Teams
- Encrypted Email
- Drive Encryption
- Backup & Recovery of M365 Data
- EDRM
- SIEM

Cloud Security

- CASB
- Cloud Workload Protection Platform
- Cloud Security Posture Management
- O365 Cloud Services Encryption

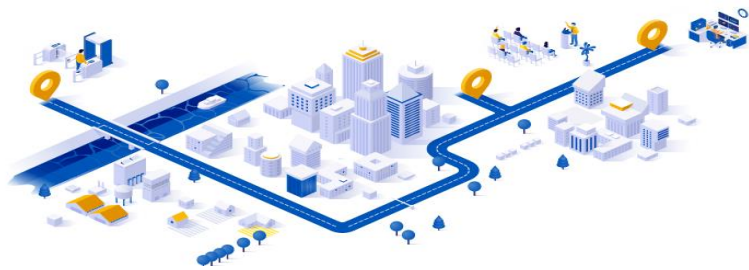
AI Governance & Risk Management

Compliance & Risk Management

- Insider Risk Management
- Communication Monitoring
- Code of Conduct
- Information Barriers
- Privileged Access Management
- Lockbox
- eDiscovery & Legal Hold
- eDiscovery Advanced Content Analysis
- Auditing
- Compliance Management

Threat Protection

- SOAR
- Investigate & Respond
- Biometric Security
- NTLM Hash Protection
- Prevent Infected Devices from Connecting
- Email URL Detonation
- Windows Kernel DMA Protection
- Firmware Protection/OS
- Targeted Browser Exploit
- Web Malware Protection
- Client Antivirus
- Host Firewall
- Endpoint Detection
- Email Filter/Antispam
- Secure Email Gateway
- Attachment Sandboxing
- Email Attack Simulation
- Email Investigation & Response
- Threat Intelligence
- Server EDR
- Advanced Threat Hunting



Find your place in Valorem Reply's
SECURITY COMPASS
FRAMEWORK

IAM MODERNIZATION FOR NONPROFIT EDUCATIONAL ORGANIZATION



PROBLEMS & OPPORTUNITIES

- Current third-party security tools becoming increasingly difficult to manage and costly.
- Complex security infrastructure creating friction among users and leaving a heavy burden on operational support.



STRATEGIC SOLUTIONS

- Strengthen the security posture around Identity and Access Management to prevent identities from being compromised.
- Replace Okta SSO and MFA with equivalent functionality with Microsoft Entra technologies.
- Implement Azure-based authentication for new and existing external facing applications.



BUSINESS IMPACT

- A modern Identity and Access Management environment capable of supporting the organization's security infrastructure in the long term.
- Simplified architecture leading to faster time to delivery for new solutions.
- Significant cost savings from reducing on-premises server costs, decreasing operational support burden, and minimizing insurance costs.
- Enhanced user experience with bring your own identity and multi-factor authentication, increasing participation and programmatic impact.



LEARN MORE ABOUT VALOREM REPLY'S **SECURITY** **COMPASS FRAMEWORK**

Learn more: <https://go.valorem.com/Security-Compass-Framework.html>

