AUBRANT DIGITAL
Creating Digital Businesses

Aubrant Digital Security Overview

Executive Summary

Aubrant Digital leverages a modern, cloud-first technology stack anchored in Microsoft 365 and Azure. This document outlines the detailed technical architecture, security framework, compliance measures, and operational procedures that support our global operations. Aubrant is committed to a Zero Trust security model, continuous monitoring, and best-in-class governance, ensuring a secure and scalable environment for our team and clients across geographies.

Security Framework

Aubrant Digital follows a Zero Trust security model as the foundation of its cybersecurity strategy. This model operates on the principle of "never trust, always verify." Every access request is fully authenticated, authorized, and encrypted before granting access—regardless of whether it originates from inside or outside the corporate network.

Identity is the core control plane in our Zero Trust model. Entra ID enables strong identity assurance with MFA and Conditional Access policies. Access decisions are based on a continuous evaluation of user, device, and session risk. Devices must meet security standards such as endpoint protection, encryption, and policy compliance before gaining access to resources.

Network segmentation is enforced using Azure Virtual Networks, Private Endpoints, and Just-In-Time VM access. Application security is enhanced by controlling traffic flow via NSGs, Azure Firewall, and WAF. Data access is tightly controlled with granular permissions, classification, and labeling enforced through Microsoft Purview and Azure RBAC.

Furthermore, CIS (Center for Internet Security) Benchmarks — both Level 1 and Level 2 — are implemented across all endpoints, Azure services, and Microsoft 365 configurations. Level 1 ensures essential security hygiene, while Level 2 applies stricter hardening policies for organizations that require higher assurance.

User Provisioning

Once an employee or contractor is hired and marked as an active team member in our Human Resource Information System (HRIS), their user account is automatically provisioned in Microsoft Entra ID through a secure integration. Access is granted based on the principle of least privilege, with role-based controls enforced directly from the HRIS. Each user's role within the HRIS governs their minimum necessary access to systems, applications, and data in Entra ID. Upon termination or role change, the integration immediately revokes or adjusts access accordingly, ensuring timely and consistent access lifecycle management and reducing the risk of orphaned accounts or unauthorized access.

Device Provisioning and Management

Aubrant uses physical Windows and Mac devices along with Windows 365 Cloud PCs (for team members outside of Costa Rica, India or the US only) to deliver secure desktops to team members, regardless of location. Both the physical and virtual environments provide a consistent OS experience with centralized policy enforcement and seamless integration with our Microsoft ecosystem.

Devices are provisioned and managed using Microsoft Intune a cloud-based service that mobile device management (MDM) and mobile application management (MAM).

All devices are provisioned and managed via Microsoft Intune and Endpoint Manager, allowing centralized deployment, update management, and security policy application. Conditional Access policies ensure that only compliant and trusted users can connect, with rules that account for device health, location, and risk score.

Provisioning is automated based on predefined job roles and geographic context. This allows us to deliver customized desktop environments efficiently while maintaining a consistent security and compliance posture.

Endpoint Protection and Device Compliance

Endpoint protection begins with Microsoft Intune, which manages device compliance policies across all user devices, including Cloud PCs. Devices must meet security baselines for antivirus, disk encryption, and OS versioning. Non-compliant devices are automatically quarantined using Conditional Access until remediated.

All devices are enrolled in Microsoft Defender for Endpoint, which provides behavioral-based detection, attack surface reduction rules, and integration with Microsoft Threat Intelligence. BitLocker is enforced on all devices to ensure full-disk encryption, while app whitelisting and exploit protection are used to prevent malicious code execution.

Endpoint analytics are continuously monitored to identify performance or compliance issues. Devices are automatically patched through Intune's Update Rings or Windows Update for Business, minimizing vulnerability windows.

Employee Productivity Applications

Aubrant's Microsoft 365 environment serves as the central foundation for productivity, communication, and collaboration. Our implementation includes Exchange Online for secure and reliable email, SharePoint Online and OneDrive for Business for centralized document storage and sharing, and Microsoft Teams for persistent chat, meetings, and team collaboration. All identity and access controls across Microsoft 365 services are managed through Entra ID (formerly Azure Active Directory), ensuring secure single sign-on and centralized policy enforcement.

Administrative control is streamlined through the Microsoft 365 Admin Center, which provides visibility and configuration tools for services across our global footprint. Microsoft Purview is used extensively for governance, compliance, and information protection, helping to safeguard sensitive information and enforce regulatory requirements. Defender for Office 365 adds another layer of protection by detecting and neutralizing threats such as phishing, malware, and business email compromise.

Networking

Aubrant leverages a 100% cloud infrastructure. This enables us not to have any physical network. Within our Azure environment, we use Azure Virtual Networks (VNets) to form the backbone of our secure networking model. Network Security Groups (NSGs), route tables, and private endpoints control traffic flow and restrict public exposure. Azure Firewall and Application Gateway with Web Application Firewall (WAF) provide perimeter protection and traffic inspection.

To further enhance global secure connectivity, Aubrant Digital leverages Microsoft Global Secure Access, to ensure secure, policy-driven connectivity for our global workforce. Built on Zero Trust principles, Global Secure Access enforces continuous verification of user identity, device health, and contextual risk before granting access to any internal or external resource. Traffic is routed through Microsoft's distributed network with advanced threat protection, inline inspection, and network segmentation, helping to prevent lateral movement and data exfiltration. Integrated with Microsoft Defender and Entra Conditional Access, this solution ensures encrypted, least-privilege access to private and SaaS applications—while maintaining full visibility, governance, and compliance across all sessions.

Cloud Infrastructure

Aubrant's Azure cloud environment is structured using the Azure Landing Zones architecture. This enables clear segmentation of production, development, testing, and staging environments while aligning with regulatory and operational boundaries across regions. Each landing zone includes foundational components such as governance, networking, identity, and monitoring tools that adhere to security baselines.

The cloud services are tightly integrated with EntraID, Microsoft Defender for Cloud, and Microsoft Purview to ensure compliance and security.

Defender for Cloud extends these capabilities to Azure workloads, offering Secure Score recommendations, threat detection, and compliance tracking. Defender for Office 365 secures communication channels by detecting phishing, malware, spoofing, and zero-day attacks within Microsoft Teams, SharePoint, and Exchange Online.

Identity and Access Management (IAM)

Entra ID

Entra ID, formerly known as Azure Active Directory, is a comprehensive identity and access management service that helps secure access to your applications and services. Entra ID provides single sign-on (SSO), multifactor authentication, and conditional access to protect users and data.

Aubrant uses Entra ID to manage user identities and control access to internal and external resources. All employees authenticate through Entra ID using Single Sign-On (SSO), streamlining user access and reducing the risks associated with credential reuse.

Conditional Access policies dynamically assess and restrict access based on factors such as device state, user role, geographic location, and real-time risk signals from Microsoft's security graph. This context-aware approach allows us to balance user productivity with tight access controls.

Multi-Factor Authentication (MFA) is enforced across the organization and is mandatory for all privileged roles. These users are further governed through Privileged Identity Management (PIM), which allows for time-limited access elevation, approval workflows, and full auditing of administrative actions.

Role-Based Access Controls (RBAC)

We implement Role-Based Access Control (RBAC) across Microsoft 365, Azure, and other platforms to ensure the principle of least privilege is enforced. Roles are mapped to job functions and regularly reviewed through automated and manual access review processes. This helps prevent privilege creep and ensures that users only have access to the resources necessary for their work.

Custom roles are used when out-of-the-box RBAC definitions do not fit our operational or compliance needs. These roles are defined, tested, and reviewed in collaboration with our security and operations teams.

Identity Segmentation and External Access

Identity segmentation extends beyond internal users. We onboard partners, contractors, and external collaborators via Azure B2B, enabling them to use their own organizational credentials. Access is scoped to specific resources and time-bound, with automated lifecycle management ensuring timely deprovisioning.

Guest users are subject to the same Conditional Access and compliance policies as internal users, including MFA and endpoint verification. Access reviews are scheduled regularly to identify and clean up stale or unused external accounts, reducing the attack surface and maintaining a secure identity perimeter.

Compliance and Data Governance

Regulatory Compliance Framework

Aubrant Digital is compliant with industry-leading frameworks including **SOC 2 Type 2** and **ISO 27001**. Our compliance strategy involves continuous monitoring of our control environment, with third-party audits performed annually to validate our adherence to security, availability, and confidentiality principles. These frameworks guide our practices in access control, data security, vendor risk management, and incident response. Microsoft compliance tools, including Compliance Manager and Secure Score, are used to track progress and automate evidence collection for audit readiness.

Microsoft Purview for Data Protection

Microsoft Purview provides governance, risk, and compliance solutions designed to help you manage and protect your data across your environment. It offers data discovery, classification, and reporting to ensure compliance with regulations.

Microsoft Purview is used extensively to enforce data classification, labeling, and protection. Information types are auto-discovered and classified using sensitivity labels. These labels control encryption, watermarking, content restrictions, and user permissions across Microsoft 365 and Azure storage. Purview Data Loss Prevention (DLP) policies protect sensitive information such as PII, PHI, and financial data from accidental or unauthorized sharing. Policies apply to email, Teams chat, SharePoint documents, and device-based actions. Retention policies and litigation holds are configured to ensure data is preserved in accordance with legal and operational requirements. The Purview Compliance Portal provides centralized visibility into data risk, insider threats, and regulatory posture.

Auditing, Logging, and Access Reviews

All administrative and user activity is logged across Microsoft 365, Azure, and endpoint environments. Logs are ingested into Microsoft Sentinel, where they are correlated, analyzed, and retained according to our data governance policy. Regular access reviews are conducted using Entra ID to validate entitlements for users, groups, and applications. Privileged accounts are subject to stricter review cadences, and orphaned or unused roles are automatically flagged for deactivation. Audit trails are preserved to support internal investigations, regulatory requests, and incident response. These logs include changes to security configurations, role assignments, data exports, and anomalous user behavior.

Monitoring and Incident Response

Centralized Monitoring and Telemetry

Aubrant has implemented a centralized monitoring strategy using Azure Monitor, Log Analytics, and Microsoft Sentinel. All operational data from Azure resources, Cloud PCs, Microsoft 365, and endpoints is collected and analyzed in near real-time. This provides visibility into system health, performance metrics, and potential threats. Custom workbooks and dashboards provide security, compliance, and operations teams with visualized insights. Alert rules are configured for key indicators such as failed login attempts, resource changes, policy violations, and security events.

Threat Detection and Response Automation

Microsoft Sentinel acts as our primary SIEM and SOAR platform. It integrates with Defender, Entra ID, Intune, and third-party sources to detect and correlate security events. Machine learning models and threat intelligence help identify attacks such as credential theft, ransomware, and lateral movement. Automated response playbooks are triggered for critical events. These include account lockouts, device isolation, and ticket creation for further triage. Logic Apps are used to coordinate actions across Defender, Entra ID, and ticketing systems such as ServiceNow. Playbooks are reviewed and tested regularly to ensure that incident response remains agile and effective.

Incident Management and Business Continuity

A formal incident response plan is in place to address cybersecurity events, including data breaches, malware infections, insider threats, and service outages. The plan defines severity tiers, escalation paths, communication procedures, and root cause analysis workflows. The IT operations team conducts periodic tabletop exercises to simulate incidents and validate readiness. Lessons learned are documented, and controls are adjusted to prevent recurrence. Business Continuity and Disaster Recovery (BCDR) plans are developed for each critical system. Azure Backup and Azure Site Recovery are used to ensure data availability and workload continuity in the event of regional outages or cyber incidents. Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are defined based on system criticality.

Let’s Build Better, Together

We’re not just another delivery partner—we’re your strategic co-pilot. Let’s connect to design outcomes that move the needle.

🌐 www.aubrant.com

✉ info@aubrant.com