GREAT VALLEY
ADVISOR GROUP
REGISTERED INVESTMENT ADVISOR

GVA SecureOffice

Powered by Align Managed Services

Align IT Suite – Managed IT Support

Management of all Client technology equipment including:

- Desktops & Mobile Devices
- Firewalls, Switches and WAPs
- Software Patch Management – Windows updates for workstations
- Virus, Anti-Spam and Web Filter Software
- Asset Management
- Monitoring of Desktop and Network Infrastructure
- Remote Support Service Desk – 24 x 7 x 365
- Microsoft Application Support

Office 365 Enterprise E3 + Security E3, Windows 10 Enterprise E3 and SharePoint

- Office 365 Advanced Threat Protection (ATP)

  ATP Safe Links - protects the organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents.

  ATP Safe Attachments – this feature checks to see if email attachments are malicious, and then takes action to protect your organization

Azure Active Directory (Azure AD)

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which allows users to sign into the Office 365 environment utilizing a single sign on experience.

- User password management is controlled through Azure AD, password policies are as follows:
  - Passwords are set to expire every 90 days
  - Complexity requirements
    - ◊ Previous five passwords cannot be reused
    - ◊ Must not contain username, or parts of it
    - ◊ Must contain three of the four categories: *Uppercase, lowercase, number, special character*

Azure AD Identity Protection protects against the following scenarios:

- Users with leaked credentials
- Sign-ins from anonymous IP addresses
- Impossible travel to atypical location
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from unfamiliar locations

Device-based Conditional Access

Utilizing Microsoft Intune and Azure Active Directory, only corporate managed and compliant devices can gain access to the organizations Office 365 environment.

Microsoft Authenticator

Microsoft Authenticator is a multifactor app for mobile devices that generates push notifications or time-based codes for two step verification into users Microsoft accounts.

- All users are required to enable Multi-Factor Authentication (MFA)
  - Users will be required to authenticate trusted devices every fourteen days.
  - If the device is not trusted (e.g. the user has never logged into the device), a request for authentication will be required.

MDM - Microsoft Intune

Intune is a cloud-based service that allows the organization to place a management profile on end-user's mobile devices and ensures users mobile devices (phones/tablets) are compliant with corporate security standards

- Screen lock set to 15 minutes or less
- Minimum password protections
- Block jailbroken devices

Remote wipe

- In the event a device is lost or stolen, corporate data can be remotely wiped.

DNS Blocking – Cisco Umbrella

- Cisco Umbrella is a cloud driven secure internet gateway that provides protection from internet-based threats no matter where workstations are located.
- Umbrella allows the organization to restrict access to websites that are potentially malicious or against corporate standards (e.g. pornography, social media, and personal email).

Data Protection

MS Data Loss Prevention (DLP)

- Allows client to implement controls to enforce their own data governance policies.

Encryption

- BitLocker Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.
- Data on a lost or stolen computer is vulnerable to unauthorized access, either by running a software-attack tool against it or by transferring the computer's hard disk to a different computer. BitLocker helps mitigate unauthorized data access by enhancing file and system protections. BitLocker also helps render data inaccessible when BitLocker-protected computers are decommissioned or recycled.

Align esEndpoint by eSentire and CarbonBlack

- Monitors endpoints on and off the network around the clock with a 24 x 7 x 365 Global Security Operations Center
- Assumes the suspicious is malicious sending all endpoint activity that has not been seen before to an elite team of threat hunters
- Protects your endpoints anywhere users and data reside–across cloud, mobile, virtual, and physical environments
- Accelerates forensic investigation, acting as a "black box" flight recorder that continuously records, centralizes, and retains vital endpoint activity
- Catches what prevention misses with proprietary machine learning layered with attack pattern and behavioral analytics
- Locks down and isolates threat actors on your behalf preventing lateral spread and potential business disruption.