# Elevate Your Cybersecurity with Appalachia's Member-Exclusive Offers

In partnership with CCAP, Appalachia Technologies is pleased to offer these cybersecurity services at a discounted rate for Pennsylvania Counties.

## Active Directory Health Check

Appalachia's Active Directory (AD) Health Checks seek to ensure the health and functionality of your AD environment, particularly focusing on its synchronization with Office 365. AD serves as a critical component for user authentication, authorization, and access control, while Office 365 integration is vital for seamless user management and productivity.

This comprehensive health check includes:

1. Review Documentation
   - Collect and review documentation related to AD configuration, including forest and domain structure, trusts, replication settings, hybrid configurations with Azure AD, AD Auditing practices and AD security practices.
2. Check Domain and Forest Functional Levels
   - Ensure that domain and forest functional levels meet the requirements for county infrastructure and any integrations with Azure AD (Using DCDiag or other tools).
3. Verify Replication
   - Check AD replication health using tools like repadmin or Active Directory Replication Status Tool.
   - Ensure that replication is occurring without errors between domain controllers in both domains.
4. Monitor Event Logs
   - Review event logs on domain controllers for any critical errors or warnings. Pay special attention to the Directory Service and DNS Server logs.
5. Check FSMO Roles
   - Verify the placement of FSMO (Flexible Single Master Operations) roles. Use netdom or PowerShell to check the role holders.
6. DNS Configuration
   - Ensure DNS is properly configured on all domain controllers, using DNSCMD or other tools based on Microsoft best practices.
7. AD Users, Groups and Security Groups
   - Check the integrity of user and group objects in AD.
   - Verify group memberships and permissions.
8. GPOs (Group Policy Objects)
   - Review and analyze Group Policy settings.
   - Ensure that policies are applied correctly.
   - Align/compare to CIS Controls v8
9. Azure AD Connect

- For hybrid Azure environments, check the status of Azure AD Connect.
- Ensure synchronization is running smoothly, and no errors are reported.

10. Security and Authentication
    - Review security settings, including password policies, account lockout policies, and authentication protocols.
    - Ensure Kerberos, NTLM, and LDAP configurations are secure.
    - Ways to reduce the AD attack surface.
11. Audit Policy Settings
    - Review audit events against Audit Policy Best Practice by using auditpol or other tools.
12. Certificate Services
    - If Certificate Services are used, check the health of the Certificate Authority.
13. Azure AD Integration
    - Validate the integration between on-premises AD and Azure AD.
    - Check Azure AD for any synchronization issues.
14. Backup and Recovery
    - Confirm that regular AD backups are being performed.
    - Test the restoration process in a non-production environment.
15. Patch Management
    - Ensure that domain controllers and servers are up to date with the latest security patches.
16. Reporting / Documentation / Presentation
    - Consolidate findings / recommendations into final report and present to client.
    - Provide current state and future state based on industry best practices

| Project (Fixed Fee) | Project Fee |
|---|---|
| Single Active Directory Domain with 1 Tenant | $7,500 |
| Additional On-Premise Domain | $3,500 |
| Additional M365 Tenant | $3,500 |

## Managed Zero-Trust with Application Whitelisting

Ransomware continues to be a top cybersecurity threat for public sectors. Unlike antivirus or traditional EDR, Appalachia's Managed Zero-Trust Service provides total control of what software, scripts, executables, and libraries can run on your endpoints and servers. This approach stops not only malicious software in its tracks, but also stops other unapproved applications from running in your environment.

However, these tools can be complex to implement and time-consuming to manage. With Appalachia's fully-managed service, our in-house SOC analysts take the burden off your limited resources.

Our Managed Zero-Trust Service includes:

- Application Whitelisting (Allowlisting): Allow only approved files to execute and blocks everything else. Policy-driven management of what software is allowed to run, effectively blocking malicious software.
- Ringfencing: Granular control over what applications are allowed to do. Limit interaction between applications, their access to files, the registry, and the internet to protect against the weaponization of trusted applications while mitigating the risks posed by application vulnerabilities.
- Elevation Control: Provide just-in-time elevation on a temporary or per-application basis allows organizations to remove local admin permissions without stopping productivity. Selected applications can run as a local administrator without making users local administrators.

- Network Access Control: Lockdown endpoints and block both inbound and outbound network traffic. Protect endpoints and servers from untrusted devices on your LAN or the internet. With dynamic ACLs, you can automatically open ports based on a trusted device location.
- Storage Control: Provide Storage Control over all storage device access including USB devices, network shares, even individual files to help protect data, limit access to data by application, controls data exfiltration, and minimizes the damage caused by cyberattacks.
- Exceptions, access requests, and policy changes will be reviewed by the Appalachia SOC Team, with notification to the client designated contacts.
- Monitor critical security log events for potentially unauthorized access attempts, with notification to client designated contacts. Examples include failed admin logins, account lockouts, failed remote sessions etc.

| Managed Zero-Trust Pricing (Monthly Recurring) | Unit Price |
|---|---|
| Servers – per device | $8.00 |
| Workstations – per device | $12.00 |

## Cloud/M365 Security

Often, the first sign that one of your user's Office 365 accounts has been compromised comes too late to prevent damage to your organization's reputation and financial health. The goal of Appalachia's Managed M365 offering is to add a significant layer of protection against Business Email Compromise (BEC) and other similar attacks. These attacks attempt to gain control of your users' accounts to steal sensitive data or defraud your organization, as well as its partners.

To detect and prevent such attacks, Appalachia has partnered with Huntress to actively monitor and stop Microsoft 365 account compromises before they can cost your business both time and money. We use a wide variety of detection methods to monitor for suspicious activity, and if needed we can lock a user long enough for an incident to be investigated. We will use the following tools to provide the service:

- MDR for Microsoft 365 allows Appalachia to monitor your M365 tenant and all associated accounts for suspicious activity on a truly 24/7/365 basis. You will have not one, but two Security Operation Centers (SOCs) actively evaluating and protecting your environment (Appalachia and Huntress).
- MDR for Microsoft 365 monitors for Mail Forwarding and Inbox Rules configurations that might indicate Business Email Compromise (BEC). Appalachia and Huntress will investigate any findings, escalating them to you for verification when needed.
- MDR for Microsoft 365 will also monitor account login, access, and privilege activity to find patterns consistent with attackers attempting to compromise other accounts in your tenant. Appalachia and Huntress will investigate any findings, escalating them to you for verification when needed.
- When account compromise is strongly suspected, accounts will be locked and isolated to prevent further exploit attempts while detailed investigation can take place. This can stop the threat actor in their tracks and prevent further damage from occurring. All alarms of this nature are reviewed by humans before any locking action is taken.
- If an incident indicates that your Microsoft 365 security configuration should be changed or updated, Appalachia engineers will be available to assist on an hourly rate basis.

| M365 Security Pricing (Monthly Recurring) | Unit Price |
|---|---|
| Per Device License Fee | $3.25 |
| Tenant Fee | $150.00 |

## Tabletop Exercise

Appalachia Technologies, LLC leverages the steps outlined in the NIST Computer Security Incident Handling Guide (SP 800-61 Rev. 2) for Cybersecurity Incident Response. The tabletop exercise will use the client's Incident Response Plan (IRP), Disaster Recovery Plan (DRP), and Business Continuity Plan (BCP) as applicable. It will also supply focus on the following steps from the NIST document:

- Preparation
- Detection & Analysis
- Containment, Eradication & Recovery
- Post Incident Activity

**Option 1: Canned Scenario**
Creation and facilitation of cybersecurity breach tabletop exercise (TTX). The activity will include one canned vignette (scenarios) that are cyber breaches. Appalachia will aid in creating exercise material and function as the exercise facilitator.

**Option 2: Custom Scenario**
The creation of custom-tailored exercise focuses on the client's incident response and coordination with other involved entities during a potential Cybersecurity incident. The intent is to improve the cyber response posture and collective decision-making processes.

Appalachia designs tabletop exercises to encourage an exchange of ideas to help test, develop and expand the participants' existing knowledge of company policies and procedures within the framework of cyber incident response—the exercise emphasizes coordination, resource integration, and problem identification and resolution during the event.

| Project (Fixed Fee) | Project Fee |
|---|---|
| Option 1: Canned Scenario | $5,000.00 |
| Option 2: Custom Scenario | $10,000 - $15,000 |

## Contact Information

Chris Notarfrancesco
Sr. Account Executive
Phone: 717-579-9438
Email: chris.notar@appalachiatech.com