CORVUS

BY TRAVELERS

GUIDE

Common Security Controls

We've gathered the top security controls demonstrably proven to reduce cyber risk. Not only will they make your organization less likely to experience an incident, they'll also make obtaining cyber insurance easier.

You may see these common security controls referenced in subjectivities as part of your cyber insurance quote. These are steps that the underwriter has required to be completed before the policy can be bound or issued.

The goal of this guide is to help you work through these security controls and understand what resources Corvus has available to help you implement them at your organization.

Table of Contents

Multi-Factor Authentication (MFA)

What is MFA?

Multi-factor authentication (MFA) is an authentication method that requires a user to provide two or more verification methods in order to gain access to a resource or system. MFA requires a combination of: something you know (a password or PIN), something you have (a code or token generated by a cell phone app or other hardware), and/or something you are (a fingerprint or face scan). Modern MFA does not include static authentication methods such as; certificates or pre- shared keys (PSK). Using certificates or pre-shared keys in conjunction with a set of credentials **does not satisfy MFA requirements as underlined by National Institute of Standards and Technology (NIST).** Certificates and pre-shared keys are both forms of the same factor. MFA requires the use of multiple factors categories - not more of the same one.

Where are policyholders required to implement MFA?

MFA is required for:

- ✓ **Email Access:** on-premise email servers or cloud hosted email servers.
- ✓ **Remote Access:** anything that allows access into your internal environment or access to SaaS-based applications that store PII, PHI, or any critical information.
- ✓ **Administrator Access:** accounts that give full access to a system like local administrator accounts and domain administrator accounts (privileged user account access).

- Internal usage of **privileged accounts,** such as local administrators or domain administrators, should also be secured with MFA where possible — or be protected by compensating controls such as the use of a privileged account management (PAM) solution that stores privileged account credentials and unique local administrators' credentials, and can rotate them after use.
- For services accounts where MFA will not be applicable, we recommend using other cybersecurity best practices, such as a Privileged Account Management (PAM) solution to manage those, and all, privileged accounts.

Put simply, companies should look to **secure any remote access points to their systems or data with MFA.**

Why are policyholders required to implement MFA?

MFA helps protect against a large number of unauthorized access events, including data breaches and password-based cyberattacks. Fortunately, MFA is an affordable option to further protect your organization. Notably, through Microsoft 365 and Google Workspace, MFA is available for free at all license levels, making them great solutions for smaller organizations. For larger organizations, enterprise solutions such as DUO or Okta typically integrate with most systems already in use and provide additional security and monitoring features.

What resources are available to help policyholders implement MFA?

For email and cloud, major cloud email providers like Microsoft 365 and Google Gmail or Workspace have a free MFA solution, regardless of the subscription level purchased. Many cloud software comes with free MFA solutions that just need to be turned on, especially software that is used to store sensitive data (such as Electronic Medical Records software and HR software).

- **Official Microsoft documentation**
- **For GSuite Customers**

For remote access, policyholders should check whether the VPN or other remote access tool that they use has MFA as a free option. If not, they will need to identify an MFA tool that integrates with their software or hardware, such as Duo or Okta.

For administrator accounts, policyholders should determine if there are any free MFA solutions available for the admin credentials. This however is less likely, especially if they are a hybrid on-premise and cloud environment, and they may need to identify an MFA solution such as Duo or Okta.

For more information on MFA, visit:

- **Corvus tips on implementing MFA (PDF)**
- **Our knowledge base article on MFA**

Endpoint Detection + Response (EDR)

What is EDR?

Endpoint detection and response (EDR) is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

The core functions of an acceptable EDR solution include:

- Monitoring and collecting activity data from endpoints that could indicate a threat
- Analyzing the data to identify threat patterns
- Automatically responding to identified threats to remove or contain them, and notify security personnel
- Access to forensics and analysis tools to research identified threats and search for suspicious activities

When evaluating an EDR solution, a keen eye is needed to cut through the marketing messaging. Antivirus products may appear to have many bells and whistles, but ultimately lack some of the key functions listed above. And some of the EDR software vendors offer multiple levels of their product, the basic version of which may not have EDR features and is effectively just antivirus (AV) software. When in doubt, send your Corvus Underwriter the full name of the product that you're using or considering, and we can let you know if it's a true EDR solution.

Why are policyholders required to implement an EDR tool?

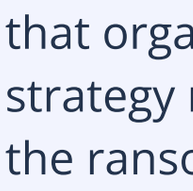
EDR provides something that traditional antivirus or even more advanced "next-gen AV" cannot: "Flight Recorder" technology that tracks activity on the system before and after an alert to clearly identify what malicious activity occurred on the system. EDR can provide insight into data from all of your systems, allowing for quicker investigations and reducing the time to get up and running following an incident. Additionally, EDR carries unmatched capabilities to protect your network's endpoints. If there's a threat detected, EDR can isolate the potentially impacted system from the rest of the network until an investigator can review the system.

For more on the differences between EDR, AV, and Next-Gen AV, **please read our article covering EDR on the knowledge base.**

What resources are available to help policyholders implement EDR?

Contact SentinelOne through Corvus's Partner Link and receive a 30% discount with a 60 day free trial. SentinelOne works across Windows, Mac and Linux OS and is very easy to implement.

- **https://www.sentinelone.com/lp/corvus-partner-page/**



Backup Strategy and Process

What is required regarding backups?

Corvus will ask if the policyholder has formal processes for regularly backing up, archiving, restoring, and segregating sensitive data. Policyholders may also be asked if they are storing three (3) copies of data in two (2) different media, one (1) of which is offsite ("3-2-1 backups"). If a system goes down, the organization is only as good as their backups and the most effective security measures typically involve a layered approach.

Why are policyholders required to have solid backup strategies?

Most companies we work with during ransomware incidents have some form of backup solution or process, but all too often the backups fail due to poor security controls. Having a great backup strategy (like the 3-2-1 strategy) will help ensure that organizations don't experience complete data loss. Not only can a great backup strategy mitigate against ransomware attacks (quicker recovery, less likely to pay the ransom, etc.), it can also reduce the impact of human error, be leveraged in the event of a natural disaster, and help organizations stay compliant.

What resources are available to help policyholders strengthen their backups?

Whether by human error or cyber attack, if your system goes down, you are only as good as your backups. Below are some resources related to backup solutions and best practices.

- Learn more about the **ABCs of 3-2-1 Backups** on our blog and check out our **detailed article here.**

Read helpful backup solutions **reviews sorted by revenue size.**

Email Security Filtering Tools

What are email security filtering tools?

An email security filtering tool, known by security professionals as a Secure Email Gateway (SEG), is software used to monitor inbound and outbound emails to protect businesses from spam, phishing, or malicious emails containing viruses and malware. The gateway works by scanning URLs and attachments in emails for any malicious content.

With email compromise used as a common attack vector for hackers to get access to an organization network, an email security gateway can serve as a first line of defense. Not only can a SEG block and protect businesses from email threats — organizations can also utilize their email security filtering tool to meet compliance needs, thanks to email archiving and encryption features, and to potentially avoid business interruption (since some SEG providers can give users access to cloud email services should their network go down.)

The Data Science team at Corvus analyzed the rates of phishing incidents among policyholders based on the email provider/email security tool the organizations used. Policyholders using a below-average rated email security service were 2x more likely to experience a cyber claim when compared to the group using above-average email security tools.

What resources are available to help policyholders implement email security filtering tools?

Well-known vendors in this space include:

- ✓ Proofpoint
- ✓ Mimecast
- ✓ Cisco Ironport
- ✓ AppRiver
- ✓ SonicWALL

If you are using cloud-based email platforms like Microsoft 365 or Gmail, you can consider services that are in-line operation, meaning mail flows directly through the email monitoring service and it monitors traffic without having to redirect mail flow. Products like Agari offer this service. To research and find the right solution for your organization, see **Gartner's peer reviews of different solutions.**

If the policyholder is using Microsoft 365, then consider turning on Microsoft Defender for Office 365 to meet the requirement. Microsoft Defender for Office 365 is standard in Microsoft 365 E5 or higher but can be added to other Exchange and Microsoft Office 365 subscriptions for an additional cost.

Corvus Finding

The Data Science team at Corvus analyzed the rates of phishing incidents among policyholders based on the email provider/email security tool the organizations used. Policyholders using a below-average rated email security service were 2x more likely to experience a cyber claim when compared to the group using above-average email security tools.

Protection of Admin Accounts

What are admin accounts?

Admin accounts, or administrative accounts, are special user accounts within an IT environment that have elevated privileges compared to regular user accounts. Examples include local administrator accounts or domain administrator accounts. These privileges allow legitimate IT administrators to install software, make configuration changes, manage user permissions, and perform other operational tasks related to managing an IT environment. Admin accounts are crucial for maintaining and managing IT systems, both in the cloud and in on-premise environments. However, their elevated privileges make them prime targets for hackers.

Why are policyholders required to protect admin accounts?

- **High Privilege = High Risk:** Admin accounts have extensive access and control over IT systems. If compromised, attackers can use these accounts to disable security measures, steal sensitive data, or move laterally within an environment to compromise additional systems which can disrupt business operations.

- **Business Continuity:** Compromised admin accounts can lead to significant operational disruptions. Protecting these accounts helps maintain overall business resilience and can help to reduce the “blast radius” of a potential compromise.
- **Compliance and Regulation:** Many regulatory frameworks and industry standards (such as PCI-DSS) require security controls to protect against unauthorized access to accounts with elevated permissions.

Proactive Strategies to Protect Admin Accounts

Since admin accounts offer full access to a system, this makes them a prime target for hackers. Protecting them is critical. Additionally, we also recommend managing and securing service accounts (aka non-human accounts) that have elevated permissions. Below are considerations and key security controls that help reduce the risk of unauthorized access to these “keys to the kingdom” accounts.

- **Privileged Access Management (PAM) Solution:** PAM solutions help secure, manage, and monitor privileged access to critical systems. Key features include the ability to monitor and log privileged access, automate provisioning and deprovisioning of privileged accounts (i.e. account check-in and check-out), and a centralized secure vault to store privileged credentials.
- **Password Vault:** Password vaults securely store admin account credentials and enforce strong password policies. They also enable strict access controls to ensure only authorized personnel can retrieve admin credentials.
- **Secrets Manager:** A secrets manager is a broader tool designed to store & manage a wider range of “secrets” that go beyond just passwords. This can include API keys, encryption keys, certificates, and passwords. Secrets managers ensure that secrets are protected, so only authorized users or systems can access them. Similar to a password vault, it unlocks the ability to implement granular access controls to ensure that only authorized applications and users can access stored secrets.
- **Multi-Factor Authentication (MFA) for Admin Accounts:** Implementing MFA for access to admin accounts requires an additional verification step beyond just a password. This adds an extra security layer around the authentication process if the administrator's credentials are compromised.

What resources are available for policyholders to implement controls to protect admin accounts?

- **Our article on MFA (which includes admin accounts)**
- **Our article on Securing Access Controls**
- **Peer reviews of PAM solutions from Gartner**

Remote Desktop Protocol (RDP)

What is Remote Desktop Protocol?

Remote Desktop Protocol (RDP) is a Windows service that allows users to remotely connect to a Windows machine. More simply, RDP allows someone on remote Computer A to login to Windows Computer B as if they were physically sitting at the system. Historically, businesses expose RDP to the Internet as part of a common remote access method to enable their users to more easily access company systems and data. IT consultants also historically leveraged RDP to assess and fix their clients' systems remotely.

Why are policyholders required to properly secure or move away from use of RDP?

Threat actors commonly target external facing RDP as a primary method of gaining access to an organization's network. This is done using stolen credentials or brute forcing weak user credentials. Once an initial foothold is accomplished using RDP, threat actors will move undetected in your environment and deploy malware. This often leads to ransomware infections.

Organizations that continue to use RDP expose themselves to an increased likelihood of attack since a large number of threat actors focus efforts on breaking in using this mechanism.

What resources are available for policyholders to help secure or find an alternative to RDP?

Learn how to secure RDP or move away from its use entirely through the **RDP article on the knowledge base.**

Securing Funds Transfer

What is fund transfer fraud?

Funds transfer is the movement of funds from one party's bank account (sender) to another party's bank account (receiver).

This process is heavily targeted by cybercriminals, in which they will redirect funds to a bank account under their control, otherwise known as **funds transfer fraud.** Funds transfer fraud is extremely damaging to any organization that is a victim of these attacks, as oftentimes attacks will involve a significant amount of funds and stolen funds are unrecoverable. Attackers will use various social engineering techniques such as email spoofing or business email compromise to carry out funds transfer fraud at organizations ranging from small local businesses to multinational corporations.

Out of Band Authentication (OOBA)

Out-of-band authentication involves using separate channels for authentication. For example, the channel that is used to authenticate a user is completely separate from the channel used by the user to log in or perform a transaction.

In the case of executing electronic payments, OOBA is a secondary verification method with the requester of a funds transfer through a communication channel separate from the original request. An example of this would be calling a known and trusted phone number to confirm a change in payment instructions sent via email from a vendor.

Why are policyholders asked to implement OOBA?

Performing funds transfer fraud is quite difficult with a layered approach in place. This is because both channels would need to be simultaneously compromised for a threat actor to be successful, ensuring that funds transfers are initiated, executed, and approved in a secure and authorized manner. Additionally, OOBA reduces the chances of a cybercriminal successfully completing a fraudulent funds transfer because most lack the time, resources, and technical sophistication to outmaneuver these security measures.

Find more guidance on implementing OOBA and other best practices through the **Securing Funds Transfers article on Corvus's Knowledge Nest.**

Zero Trust Network Access (ZTNA)

What is ZTNA?

Zero Trust Network Access (ZTNA) is a category of security technologies that provides secure remote access to applications and services. Access is established after a user has been authenticated to the ZTNA service, which acts as an access broker. The ZTNA service then provides access to permitted applications on the user's behalf through a secure, encrypted tunnel. Users are then only allowed access to certain applications and areas of a network that have been authorized for their user account.

Why should policyholders replace their existing VPN solution with ZTNA?

VPNs were designed to grant complete access to a network over a private encrypted tunnel for remote employees to connect to corporate resources. While this may seem like a practical solution, VPNs lack the flexibility and granularity to control exactly what users do and which apps they can access.

This can lead to unfettered access for an attacker who iis able to steal even a single employee's credentials. Additionally, VPN devices sit on the edge of a network and vulnerabilities in these devices can lead to total compromise of an environment. Unpatched VPN solutions are targeted by attackers and used as a point of entry to carry out an attack.

VPNs provided organizations with a remote access solution when alternatives to remote desktop was needed. Zero Trust Network Access (ZTNA) aims to build upon the foundations of remote access that VPN's taught us. These fundamental challenges are overcome by incorporating key concepts of Zero Trust.

Think of a VPN as a master key that allows everyone the same access into an office building. An attacker that stole a legitimate employee's key would gain unauthorized access into this building. Now picture this same building with different keys that only have access to specific rooms and areas throughout the building. Employees are only given the keys to their office and there are partitioned areas that only specific people can access. In the secure version of this office building, a master key isn't handed out to every employee. The benefits of the locked down and secure office are obvious — and this is exactly what ZTNA does for a corporate network.

Implementing a ZTNA solution significantly reduces the surface area for an attack and validates users and devices, which enables secure remote access to your organization's resources. ZTNA is the next generation of remote access technology aimed to defend against next generation attacks.

Corvus Finding

Corvus has identified that organizations using VPNs with a history of critical vulnerabilities and threat intelligence showing active exploitation are 3x more likely to experience a security incident. Corvus encourages policyholders to implement a ZTNA solution.

What are some of the foundational elements of ZTNA?

Verify and Validate: Strict verification of users an devices and constant examination of device posture and user behavior throughout their session. Only allowing the users and devices that are confirmed to be legitimate

Least Privileged Access: Limits the information each user and device can access based on identity and context to mitigate the risk of data exfiltration and unauthorize access. Only allowing approved users and devices to access applications they are approved to access.

Continuous Monitoring: Logging of user activity and authentication requests to provide deep visibility into risky user behavior. Full visibility for security teams to rapidly investigate suspicious activity.

Micro-segmentation: Isolates applications and data within the network to shrink the blast radius of any potential attacks.

What resources are available to help policyholders implement ZTNA?

- Learn more about the advantages of ZTNA in **this article.**
- **A Complete Guide to ZTNA.**
- **Peer reviews** of ZTNA solutions from Gartner.
- Thinking of implementing a ZTNA solution? Get started with this **list of Implementation Considerations.**

About Corvus

Corvus offers smart solutions for cyber risk, with comprehensive coverage paired with expert guidance for policyholders to improve their security and respond to emerging threats. Smart Cyber Insurance® is written on paper from Travelers Excess & Surplus Lines Co (A.M Best A++ Superior) and Hudson Insurance Group (A.M. Best A+, XV). Contact your Territory Manager or reach out to flock@corvusinsurance.com today for more information.