CORVUS

Guide to 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 Corvus Smart Cyber or Smart Tech E&O insurance quote. These are steps that the underwriter has required 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) p.2

Endpoint Detection and Response (EDR) p.4

Backup Strategy and Process p.5

Email Security Filtering Tools p.6

Data Encryption p.7

Remote Desktop Protocol (RDP) p.8

Securing Funds Transfers p.9

Zero Trust Network Access p.10

CORVUS

Multi-Factor Authentication (MFA)

What is MFA?

Multi-factor authentication (MFA) is an authentication method that requires the user to provide two or more verification methods in order to gain access to an account. Rather than just asking for a username and password, MFA requires additional verification factors, which decreases the likelihood of a successful cyberattack. Typically MFA involves 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).

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 other 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 organizatinations, enterprise solutions such as DUO or Okta typically integrate with most systems already in use and provide additional security and monitoring features.

Multi-Factor Authentication (MFA)

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
- GSuite Documentation

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 Nest article on MFA

For policyholders looking to hire experts to help them implement MFA, Corvus offers an MFA Consult that can be requested via our simple form with no up-front commitment. We will then connect policyholders to vendors to assist at reduced, cost-effective rates.

CORVUS

Endpoint Detection and 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 Corvus Knowledge Nest.

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.
- CrowdStrike — Contact CrowdStrike through Corvus' Partner Link to receive a free trial and substantial discount following the trial.
- EDR Consult — For policyholders looking to hire experts to help them identify and implement the right EDR tool for their environment, Corvus has an EDR Consult that they can request via our simple form with no up-front commitment. We will then connect them to vendors to assist at reduced, cost-effective rates.

CORVUS

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.

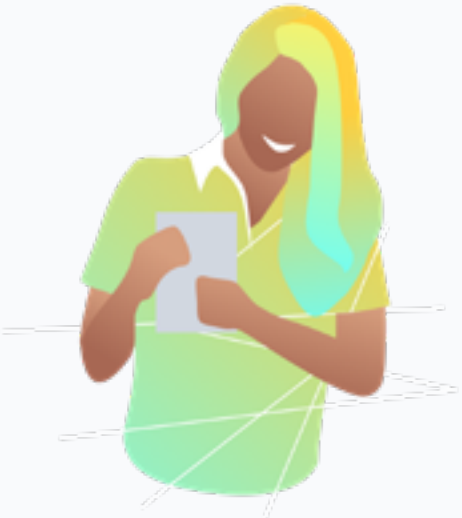
Why are policyholders required to have solid backup strategies?

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 cyberattack, if your system goes down, you are only as good as your backup. 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.
- For policyholders looking to hire experts to help them improve their backup strategy, they can request a backup consult through Corvus. We will then connect them to vendors to assist at reduced, cost-effective rates.



CORVUS

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).

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

- 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.

CORVUS

Data Encryption

What is data encryption?

Data encryption is a straightforward but powerful tool to protect sensitive information from threat actors. It translates data into another form so that only people with a secret password or key can see it. Taking adequate steps at your organization to guarantee your data is protected requires that you first know where encryption is already installed, and second, recognize where you need to take actionable steps for more secure protection.

Where are policyholders required to implement encryption?

The three main components of data encryption are Endpoint Encryption, Mobile Device Encryption, and Backups Encryption.

Endpoints: Endpoints are your organization's laptops and desktops. With these devices you want to ensure that the hard drives themselves are encrypted so that stolen laptop passwords alone won't enable someone to access sensitive data. While most Mac and modern Windows devices are encrypted by default, it is best for your organization to enforce and manage the devices with a centrally managed solution.

Mobile Devices: These are cell phones and tablets used to access company resources. Like endpoints, most Android and iOS phones and tablets are encrypted by default, but implementing a Mobile Device Management (MDM) solution is a great way to further reduce risk and validate compliance.

Backups: Backup files stored on disks should be encrypted at the file level as an added layer of security in the event a hacker should access your environment through a backdoor. Cloud backups are often encrypted but it's always a good idea to confirm with your provider.

Why are policyholders required to have data encrypted?

With increasing rates of cybercrime, encryption is crucial to protect and keep personal information from threat actors. If an unauthorized party should access your environment, having strong encryption controls can protect an organization's valuable information, help you comply with industry regulations, and can protect you from any breach notification laws.

What resources are available for policyholders to implement data encryption?

- Learn more in our Data Encryption Whitepaper
- A list of the top Endpoint Encryption Software in 2021
- Peer reviews of Mobile Device Management 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 Corvus's Knowledge Nest.

CORVUS

Securing Funds Transfers

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 cyber criminals, 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.

CORVUS

About Corvus

Corvus Insurance is building a safer world through insurance products and digital tools that reduce risk, increase transparency, and improve resilience for policyholders and program partners. Our market-leading specialty insurance products are enabled by advanced data science and include Smart Cyber Insurance® and Smart Tech E+O™. Our digital platforms and tools enable efficient quoting and binding and proactive risk mitigation. Corvus Insurance offers insurance products in the US, Middle East, Europe, Canada, and Australia. Current insurance program partners include AXIS Capital, Crum & Forster, Hudson Insurance Group, certain underwriters at Lloyd's of London, R&Q Accredited, and SiriusPoint. Corvus Insurance, Corvus London Markets, and Corvus Germany are the marketing names used to refer to Corvus Insurance Agency, LLC; Corvus Agency Limited; and Corvus Underwriting GmbH. All entities are subsidiaries of Corvus Insurance Holdings, Inc. Corvus Insurance was founded in 2017 and is headquartered in Boston, Massachusetts with offices across the U.S., in the UK, and Germany. For more information, visit **corvusinsurance.com**.

CORVUS

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 is 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.

Data Science & Security Insights

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.

Zero Trust Network Access (ZTNA)

What are some of the foundational elements of ZTNA?

Verify and Validate: Strict verification of users and 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 unauthorized 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.