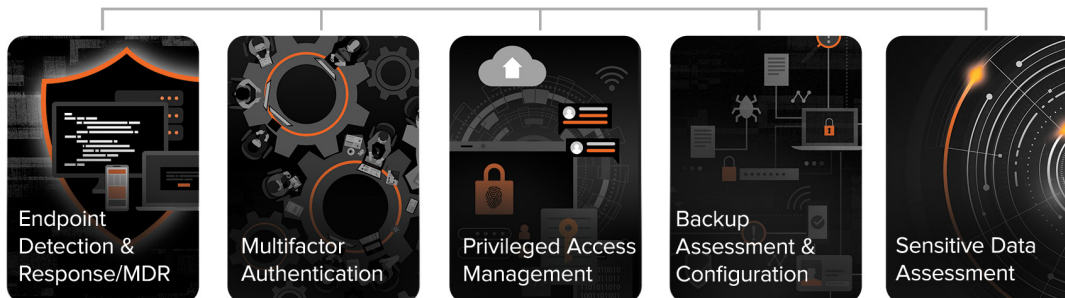# Security Controls & Cyber Insurance Coverage

Over the past year, MOXFIVE has seen cyber insurance carriers meaningfully increase the security controls they require from organizations to provide insurance coverage. In many instances, insurance carriers are unwilling to provide pricing if certain security controls are missing. While the list of security standards and models with which organizations could align can appear daunting, our approach is to focus on the basics and focus on solutions that will tangibly improve your IT infrastructure's resilience as well as present a more favorable risk profile to your insurer.

MOXFIVE will work with your team to:

- Establish timeline based on renewal dates to prioritize and execute workstreams
- Expedite implementation process by leveraging our partner ecosystem
- Provide verification of completeness of implementation for insurance broker and carrier
- Help reduce the cost of insurance - both premium and retention - while establishing a resilient cyber security roadmap to build towards

Priority Controls

Below is the priority bundle of controls that we recommend as a starting point.

Endpoint Detection & Response/MDR

Multifactor Authentication

Privileged Access Management

Backup Assessment & Configuration

Sensitive Data Assessment

Endpoint Detection and Response / Managed Detection and Response (EDR/MDR): We recommend that all servers and end-user systems have agents installed and blocking capabilities activated, including Next Generation Antivirus (NGAV) along with skilled staff monitoring alerts.

Benefits of working with MOXFIVE

IT & Security Expertise On-Demand

With a deep understanding of both IT operations and security, MOXFIVE Technical Advisors can provide the expertise you need and help determine the most efficient and cost-effective solution.

Access to Experts at Scale

MOXFIVE maintains an ecosystem of the industry's best technology experts and service providers so we can quickly assemble the right team with the skills you need.

Streamlined Process

MOXFIVE manages the selection, implementation and procurement processes to keep projects on schedule and minimize disruption.

Resilient Outcomes

MOXFIVE identifies gaps between business, IT and security objectives to build a more resilient environment.

MOXFIVE

Multifactor Authentication (MFA): Implement MFA for Internet-facing systems so that authentication requires more than just a password. Users often re-use passwords that can be exposed in other attacks and re-used against your systems. Make this initial access component of the attack lifecycle harder to succeed.

Privileged Access Management (PAM): Place 90% or more of passwords for privileged accounts under management of a tool that automatically rotates passwords and requires MFA to use the accounts to authenticate to resources.
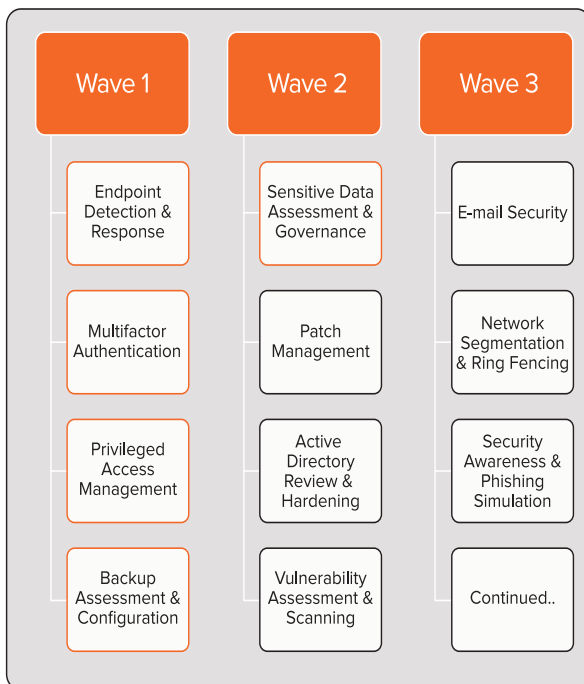
Backup Assessment and Configuration: Protect at least one backup mechanism from being corrupted deliberately by an attacker who has administrative-level privileges in the environment.

Sensitive Data Assessment: Understanding and proactively managing the vast amounts of information that helps run your business is critical in the midst of responding to an incident. Knowing and being able to quickly identify what data has been compromised helps your organization navigate legal and regulatory requirements around notifications.
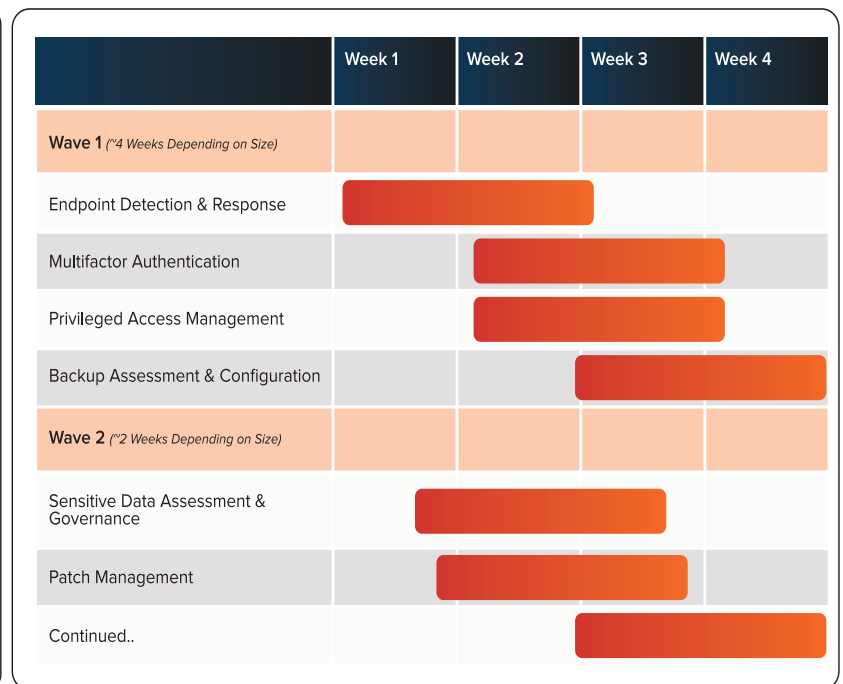
What Tactical Steps Should We Expect for Implementation?

At the beginning of Wave 1, we focus on the priority bundle that will address your ability to obtain insurance coverage at a reasonable price. We will then be able to continue to work with you on other initiatives that will assist reducing further cost and risk leveraging our resilience framework.

Assess & Prioritize

Wave 1	Wave 2	Wave 3
Endpoint Detection & Response	Sensitive Data Assessment & Governance	E-mail Security
Multifactor Authentication	Patch Management	Network Segmentation & Ring Fencing
Privileged Access Management	Active Directory Review & Hardening	Security Awareness & Phishing Simulation
Backup Assessment & Configuration	Vulnerability Assessment & Scanning	Continued..

Plan & Execute

	Week 1	Week 2	Week 3	Week 4
Wave 1 *(~4 Weeks Depending on Size)*				
Endpoint Detection & Response	███	███		
Multifactor Authentication		███	███	
Privileged Access Management		███	███	
Backup Assessment & Configuration			███	███
Wave 2 *(~2 Weeks Depending on Size)*				
Sensitive Data Assessment & Governance	███	███		
Patch Management	███	███		
Continued..			███	███

www.moxfive.com

(833) 568-6695

info@moxfive.com

MOXFIVE