Prescriptive

Support Hour Options:
Weekday: 8am-6pm 365 24/7

Managed Security Program

Let us take the weight off your shoulders

If you're serious about elevating your cybersecurity practices, this comprehensive security program is designed to meet all the needs of your organization.

Overview

Our cybersecurity program is built on a foundation of continuous auditing, ensuring ongoing visibility into your security posture and adherence to industry standards. Our auditing process follows established cybersecurity frameworks such as NIST, CIS, CMMC, SOC, and others, allowing us to proactively identify risks and recommend actionable improvements. This program also includes the development of incident response plans, business continuity plans, disaster recovery plans, and security improvement roadmaps to strengthen your organization's resilience. Our team works closely with your team to implement these improvements, ensuring they align with your existing infrastructure, business objectives, and compliance requirements.

Benefits of a Professionally Deployed Security Program

Reduced Risk: Proactively identify and address vulnerabilities before they become a threat.

Scalability: Ability to adapt quickly to changes in your business, ensuring your cybersecurity grows with you.

Better Resource Allocation: Free up internal teams from managing security, enabling them to focus on higher-value activities.

Expert Guidance: Access to specialized knowledge and recommendations to strengthen your security posture.

How It Works:

High-level cybersecurity readiness assessment:
- Establishes a baseline of the client's security posture.
- Identifies the most suitable cybersecurity framework tailored to their environment.

Comprehensive initial audit:
- Collects evidence to support compliance with the selected framework.

Review of audit findings & recommendations:
- Results in the creation of a security roadmap to guide necessary improvements.

Recurring auditing processes:
- Ensures continuous progress along the security roadmap.
- Makes necessary adjustments as new solutions, processes, and plans are rolled out.

Integration of new developments:
- Each new development is integrated into the ongoing audit process.
- Maintains and reinforces the client's compliance status.

Critical Focus Items:

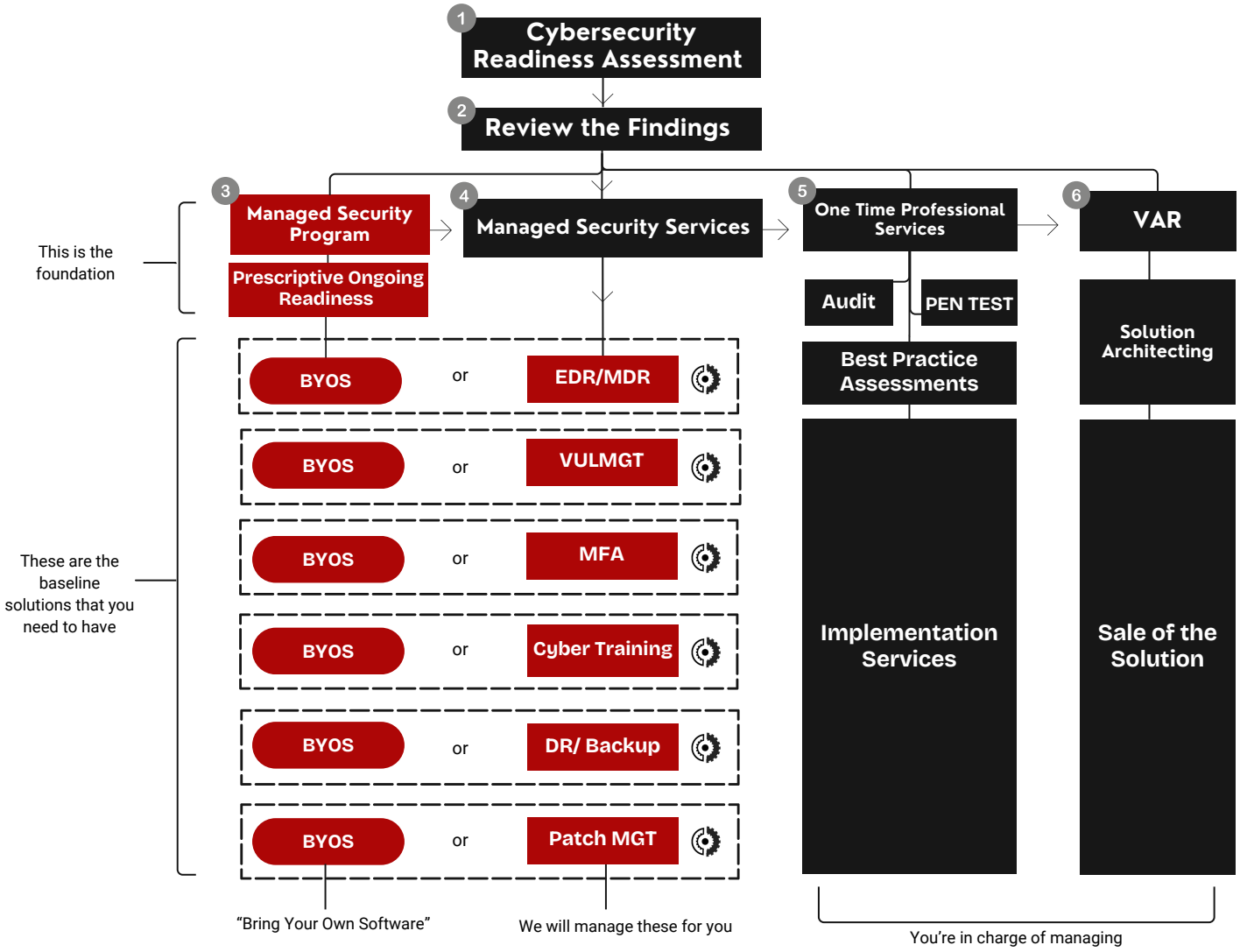
1. Strong Access Controls
2. Regular Vulnerability Assessments
3. Incident Response Plan
4. Employee Cybersecurity Training
5. Endpoint Detection & Response (EDR)
6. Data Backup & Recovery
7. Security Patching and Updates

Prescriptive

Support Hour Options:
Weekday: 8am-6pm 365 24/7

Managed Security Program

Prescriptive Cyber Security Engagement Workflow



Notable Positions Within the Prescriptive Security Approach

1. Perform a Cyber Security Readiness Assessment
2. Review the findings to align the business security needs to Prescriptive services
3. For customers needing to start from scratch, rebuild, or revamp their security program, we focus on building a co-managed security program built to the customer's compliance and security requirements.
4. For customers needing to supplement their security team with full time SME on various security tools, we focus on building managed security services tailored to the customer environment.
5. For customers that are audit and pen test ready, we focus performing the necessary audits and pen tests to validate and maintain compliance.
6. For customers that are audit and pen test complete, we focus on Solution Architecting to improve security posture and address gaps.

Email: info@prescriptive.solutions Phone: 888.252.3182 www.prescriptive.solutions