CYBER SECURITY

While mobile, cloud and virtualization technologies have led to enhanced business productivity they’ve also led to new attack vectors that provide lucrative targets for malicious actors. With more devices and systems connecting to an organizations’ network than ever before, the security conversation has changed dramatically. It is no longer a question of if but when your network will be breached. Our comprehensive approach to cyber security looks at your entire infrastructure and takes into account how your users access and consume data, applications and network resources. Our security experts provide support throughout the process of selecting and implementing security solutions. Iron Bow’s tenured and certified staff can assist you with all of your needs around network vulnerability and defense, policy enforcement, data access management and control, threat visibility and prevention, incident remediation and ultimately ensure that your security agenda is in line with your desired outcomes.

NETWORK DEFENSE

Protect data by separating trusted and untrusted networks and strengthening external borders against unauthorized access and attack. Use data from traditional perimeter defense to create context-aware solutions for greater visibility and granular access control. Our team looks at your network as a whole in the context of business goals. We recommend the best use of resources to enable multimedia collaboration, anywhere wireless communications, data center optimization and network visibility and monitoring. Most importantly, we balance the needs of competing enterprise technologies to optimize network performance.

POLICY ENFORCEMENT

Develop, automate and enforce authentication and authorization policies to control system and application access. Fully centralized, best-of-breed identity services allow dynamic device identification as well as policy enforcement by device class however the network is accessed (802.1X, VPN, 802.11, multi factor authentication, etc.). Know precisely who is accessing the network, on what device, from which location, what connectivity and when. We provide clear intelligence to develop, automate and enforce authentication/authorization policies to control system and application access.

THREAT VISIBILITY

Meet the challenges of a diverse and expanding threat landscape by gaining visibility into network traffic. Having a baseline of normal traffic helps raise anomalous events to the attention of those who need to act through alerts. Data from firewalls, Intrusion Prevention Systems and more are correlated with leading public security databases to provide the most up-to-date threat information. We use a combination of passive monitoring and active scanning to achieve the needed visibility.

NETWORK VULNERABILITY ASSESSMENT

Know your weaknesses through a combination of interviews, physical surveys and automated scanning. Network vulnerability assessments are a critical part of continuous monitoring to proactively determine vulnerability to attacks and provide verification of compliance with security best practices. We provide actionable findings to drive to immediate remediation as well as architecture recommendations.
REMEDIATION AND RESPONSE

Prepare for attacks. Remediation tools and plans should be in place well before an incident occurs giving immediate visibility into how the attack entered the network and how wide it spread. Iron Bow helps determine the best tools to do this by understanding the customer’s business, important assets and operational capabilities. With that insight, we have an understanding of where in the cyber kill chain we can best stop potential attacks and can recommend the best solution to remediate attacks when they occur. This defense in depth strategy ensures that attack vectors are identified to effectively block attacks and create a resilient network.

IRON BOW IN ACTION

Most organizations have well-defined security practices that have been in place for years without a major incident. This does not mean that they are completely secure. Our vulnerability assessments take a deeper look at network traffic to discover anomalies that may not impact performance or security today, but pose a threat nonetheless. In one case, we discovered, through a combination of raw data and user interviews, a client was open to malicious actors via several well-known and well-used workarounds. The weakness had not been targeted yet, but posed a huge risk. Iron Bow provided a detailed network vulnerability assessment and developed a prioritized plan for increasing the client’s security posture that dramatically shrunk the potential attack vectors, increased visibility aligned with their current budget.

ABOUT IRON BOW

Iron Bow Technologies provides IT solutions that optimize your work environment. We have built a team of tenured technology and project management experts with access to the most trusted and innovative solutions on the market. Through an unbiased consultative approach, Iron Bow assists you in assessing potential solutions, designing optimal future end-states, and acquiring new technologies. We take a holistic view of your IT investments and collaborate with all stakeholders from start to finish, to ensure our solutions are based on your requirements and not manufacturer agendas.

Industry Ranking

- CRN Solution Provider 500, Tech Elite 250 & Managed Services Provider – Managed Security 100 (consecutive years)
- Washington Post Top Workplaces (consecutive years)
- Virginia Business Best Places to Work in Virginia
- Washington Technology Top 100 (consecutive years)

Key Credentials

- Strategic Manufacturer Partnerships
- Cisco Gold Partner and Master Certification in Data Center and Hybrid Cloud, Security, Master Cloud and Managed Services Provider, as well as Architecture Specialization in Data Center, Collaboration and Enterprise Networking
- Cisco Americas U.S. East – Commercial Mid-Atlantic Partner of the Year
- Cisco Americas U.S. Public Sector: Architecture Excellence Award

STRONG. In-depth knowledge on the latest attack methods and how to defend against them.

FLEXIBLE. Customized cyber security reference architectures to meet domain and environment-specific needs.

TARGETED. Customized cyber security reference architectures to meet domain and environment-specific needs.