High-profile data breaches and the proliferation of advanced persistent threats have changed the security conversation; it’s no longer a question of if your organization’s data will be compromised, but when. Technologies deployed to protect against attacks must also be able to quickly and completely remediate attacks when they are able to penetrate the network.

Iron Bow Technologies approach to cyber security is to help organizations achieve resiliency. That means staying up-to-date with the latest attacks and defense methods, aligning security solutions with business needs and compliance requirements and working to keep IT systems operational in the face of mounting threats.

**REMITDATION AND RESPONSE**

The possibility of malicious attacks entering the network will always exist. It is critical to have the security tools in place before attacks happen to speed response time. Having immediate visibility into how the attack entered the network and how wide it spread helps lessen the impact.

Iron Bow helps determine the best tools 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.

Once the attack is stopped, remediation begins immediately not only at the attack entry point, but also across the network to ensure similar vulnerabilities have not and will not be exploited.

**CYBER STRATEGY**

With the right tools in place, the remediation and response to attacks becomes much easier to manage, but the tools are only helpful if they are part of a bigger security strategy. Iron Bow helps customers develop well-defined plans to use in understanding the attack, securing the environment and remediating issues in a way that stops the fundamental attack vector.

**IRON BOW IN ACTION**

Remediation and response technologies and plans must be in place before an incident compromises data. Planning for the worst minimizes impact and speeds resolution. For example, a recent ransomware attack was identified and stopped using the tools in place. The organization could see that files on local computers and on file shares were being encrypted, but could not make sense of why those files were being targeted. Based on the traffic the attackers were using an account that had full read write access as well as laptop and active directory rights. The organization was able to cut off a branch organization that looked to be the source and at the same time limit write access for all users to stop the flow until the root cause was identified. Next Gen IPS was used to show where traffic was exfiltrated and look for matching signatures. Netflow-based tools provided visibility into all flows traversing the network.
and quickly identified the malicious flows. Anti-malware agents identified any files that were known malicious and quarantined them helping identify possible source computers. Once the initial computer and attack was identified, they implemented remediation for all machines that addressed the current attack as well as all machines to prevent and future attacks.

Iron Bow has the expertise and experience to ensure that the root cause of an attack is discovered and the appropriate steps are instituted to remediate against the attack and keep the attack from occurring again.

**STRONG.** We have the expertise and experience to quickly get to the root cause of an attack and ensure that it does not happen again.

**FLEXIBLE.** We customize plans, technologies and systems to meet specific business needs.

**TARGETED.** The goal of a resilient strategy is to give the needed visibility into attacks to lessen the impact.