Redpoint CYBERSECURITY

USE CASE

CYBER RISK ADVISORY

THE PROBLEM

As the universe of sophisticated cyber threats, such as ransomware, continues to grow in volume and effectiveness, organizations in every industry are moving from a threat prevention strategy to a cyber resilience model for holistic cybersecurity. Organizations acknowledge that while blocking threats is still a critical priority, prevention will not be 100% successful. Cyber resilience requires organizations to also focus on the ability to respond to an attack, mitigating damage while protecting critical data and enabling recovery with assured data integrity to restore business continuity.

During a post breach risk assessment, a large law firm was found to have significant gaps in their on-prem network environment that would further threaten the security of their operations and client data. Redpoint's Cyber Risk Advisory Team was engaged to create an inventory of assets, train employees, implement email security and MFA, set up company-wide backup policies, migrate applications and infrastructure to the cloud, secure remote access, increase endpoint and enterprise visibility, implement patch management, and build a continual reporting policy.

TOOLS & TECHNIQUES:

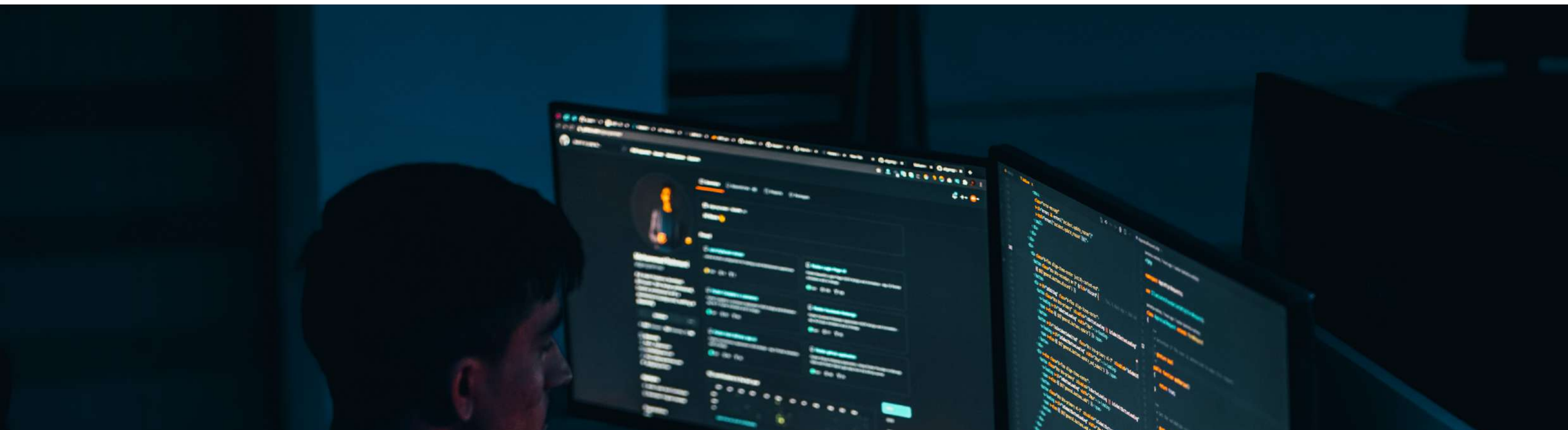
- Cloud Migration: Redpoint designed and implemented a cloud first strategy, migrating 100% of the clients on-prem environment to Azure hosted servers, file storage and databases. Further enhancing security compliance standards, establishing VPN connectivity, and optimizing management and monitoring of critical assets.
- Email Migration & Security: Migrating from an on-prem Exchange environment to Office 365 provided numerous advantages ranging from improved performance to enhanced email security and filtering capabilities. Additionally, Redpoint deployed a leading email security platform, i.e. Perception Point, creating a layered security approach with unmatched email threat prevention.
- Backups: Establishing cloud backup strategies in Azure that offered enhanced resilience, monitoring and ease of data recovery. Creating an environment of centralized management, on-demand recovery, redundancy and scalability for data protection and a reduced work loss tolerance.

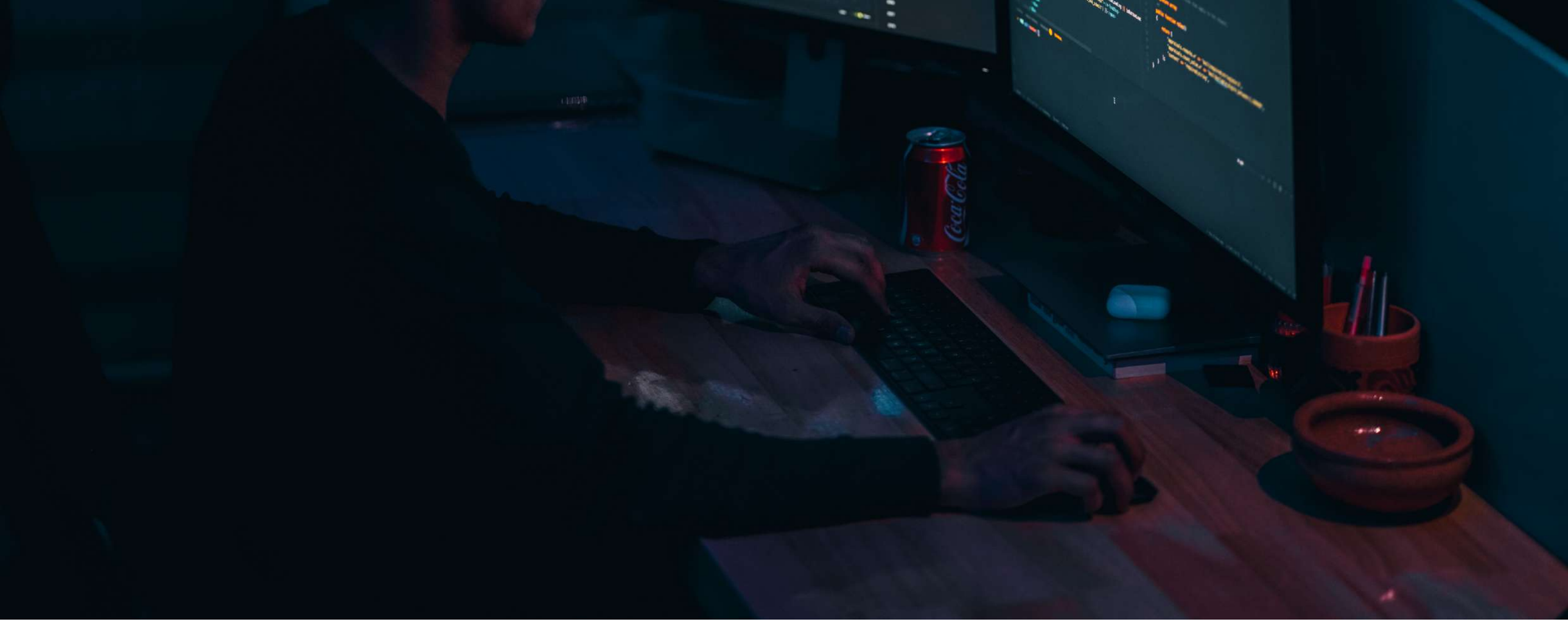
- Policy & Procedure: Specializing in risk management and compliance practices, Redpoint developed key policies and procedures that aligned with business operations and the NIST Cybersecurity Framework. Establishing standard operating procedures for threat detection, incident response, remote access and end user security.
- Helpdesk: The client's helpdesk practices were significantly improved through standardization of workstation images, enterprise visibility, process baselining, and implementing of best practices, resulting in a reduced ticket volume and improved response times.
- Managed Detection & Response: Redpoint deployed & calibrated Red Recon, which includes CrowdStrike and an array of best-in-class cyber tools to strengthen endpoint security and leverage cloud based EDR protection for detecting emerging threats; in addition to threat hunting practices and identifying persistence.

OUTCOMES:

Redpoint's Cyber Risk Advisory Team provided ongoing consultations with client leadership, technical staff, and service providers to plan and execute numerous infrastructure and endpoint enhancements, leading to a culmination of technology best practices and improved cybersecurity protection. Some of the notable outcomes include:

- A secure cloud architecture leveraging Microsoft Azure and optimized system hardening configurations.
- Established security controls that align with the NIST Cybersecurity Framework, with a focus on data privacy, user permissions, data encryption, policy development, and application controls.
- Reduction of the Firms threat landscape through implementation of best-in-class EDR threat protection and information security policies.
- User friendly helpdesk platform with refined standard operating procedures to improve tech support response times and improved staff satisfaction.
- High performance network and wireless infrastructure to support endpoints and cloud environment.
- Formalized perimeter security controls through firewall configurations, policy management, and network segmentation.
- Created incident response planning framework, with quarterly testing and training.





SUMMARY:

As found in many cases with similar cyber-attacks, organizations lack the preparedness and expertise to navigate such a complicated scenario and have limited documentation regarding Disaster recovery practices for ensuring business continuity. When leveraging Redpoints specialized teams and expert staff, our mission is to provide a thorough evaluation of existing practices, enhance controls, reduce risk of vulnerabilities, and strengthen the technology environment to protect against future threats.