CASE STUDY

MOXFIVE

Microsegmentation:
Sensitive Engineering Drawings & Schematics

Case Background

An engineering firm experienced a ransomware incident that resulted in the threat actor's theft of sensitive engineering schematics. The client decided not to pay the ransom and was concerned about the potential for a retaliatory reinfection. While Endpoint Detection and Response (EDR) software was put in place to provide blocking protection and enable an investigation, the client wanted to "ring-fence" systems containing critical data to further protect against reinfection and lateral movement across the enterprise.

Business Challenge

As the client was losing revenue by the hour, MOXFIVE proposed to immediately implement a software-based microsegmentation tool in order to quickly provide an additional measure of control over network activity beyond an EDR tool's capabilities. Additionally, as this was early in the recovery phase, solely relying on EDR resulted in additional risk due to potential gaps in visibility and detection. MOXFIVE was able to get a ring-fence setup around critical assets within a few hours and identified suspicious attempts to access the perimeter of that fence. This information was quickly relayed to the client and forensic provider and the activity was swiftly terminated.

Conclusion

This scenario illustrates both the value of a defense-in-depth strategy and the effectiveness of microsegmentation during incident response and recovery efforts. Using this approach, not only did the recovery stay on track while avoiding additional damage, the security of the client's sensitive engineering files was maintained. MOXFIVE's microsegmentation strategy and implementation enabled a rapid, secure, and effective recovery.

RESULTS

- **Complementary deployment alongside EDR provides increased endpoint visibility and protection within minutes**
- **Prevented reinfection and re-attack during recovery**
- **Allowed instant containment of threat**
- **Increased confidence in client ability to protect customer data**
- **Product dashboard provides deep visibility into asset inventory**

OTHER USE CASES

- "Crown Jewels" protection
- Virtual isolated environment for recovery
- Legacy OS protection
- Backup isolation
- Application infrastructure isolation

MOXFIVE is a cybersecurity company helping organizations respond to incidents and minimize the risk of future attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. Through a combination of our technical experts and proprietary platform, we bring order to chaos and deliver a tailored incident response approach and resilience-minded path forward for clients of all sizes, faster and more efficiently. .

www.moxfive.com
(833) 568-6695
info@moxfive.com