Our Client

A major manufacturer supplying products to some of the world's largest pharmaceutical companies. The organisation employs 150 people and generates $50m annually.

The Initial Problem

When our client suffered a major cyber-security attack their IT security was significantly compromised. The 'bad actor' was able to access this system and encrypt the firm's core services and data, including:

- Active directory
- Email / Exchange servers
- File servers
- Backup copies
- VOIP Configuration and system
- All servers
- Several user workstations

Following the loss of data access the firm was contacted by the hacked demanding a ransom be paid to regain access to all the systems. The result of this cyber-attack critically halted all business operations for a full week before systems slowly were rebuilt or recovered.

Further Challenges

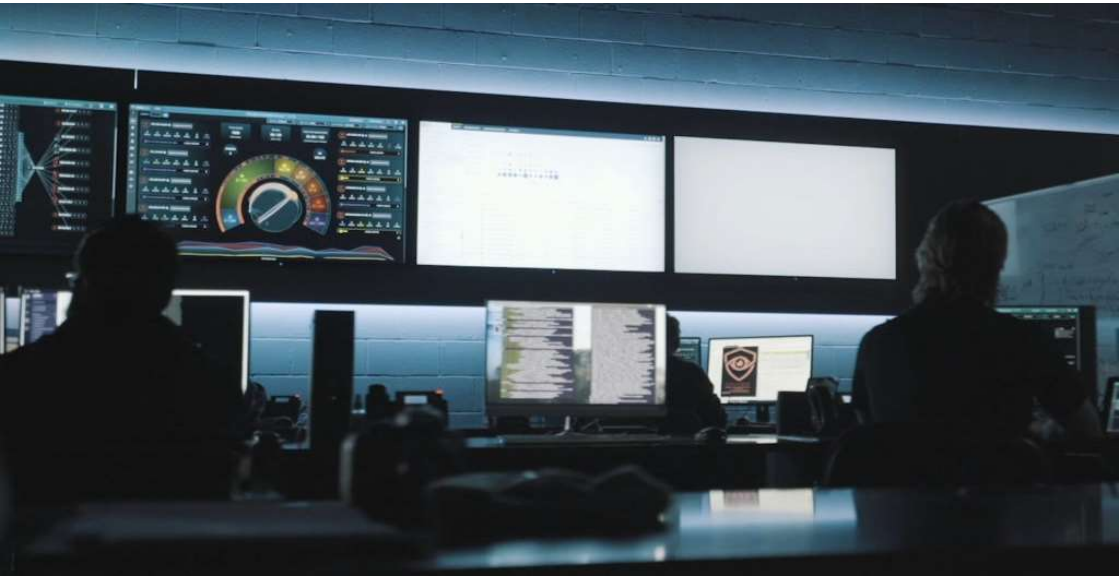
Feeling they had no choice, the firm paid $70k to the attacker to decrypt all the systems and files, although only 80% was ever recovered. Over the following weekend the firm was forced to migrate all its systems to the cloud, a complete rebuild of the Active Directory and email environment was needed to get the company back to a basic level of operation. Over the next month the business spent a further $40,000 with a technology partner to try to repair the damage and get back to business as usual.

However, the damage was already done and the company's brand reputation was impacted significantly. Clients started to ask questions about the cyber-security that was employed and a number started to re-evaluate their relationship with the firm.

Choosing CyFlare

Before approaching us, the client was already working with a network provider but didn't feel that they were getting experienced cyber security expertise or much value in comparison to the significant investment that had been made. There was no information security program or policy, many gaps remained and the senior team felt that the supplier's expertise was focussed around managing systems and networks rather than cyber security.

After an extensive evaluation process which included interviewing many of the better known cyber security specialists, we were selected because of our exclusive focus on cyber security and the interest, expertise and engagement demonstrated by our people.



Our Approach

We started work with our new client in August 2018. At this point there was no cyber security strategy and the tools that were employed to improve security were ineffective or incomplete.

We could immediately establish that the firm needed to significantly improve its security defences, active security monitoring, disaster recovery capability and capability for forensic research. Action was needed quickly to prevent another business critical breach of security.

After providing initial recommendations based on client priorities, budget and ease of delivery we set to work. Within 6 months all the security gaps were addressed and effective security solutions were deployed.

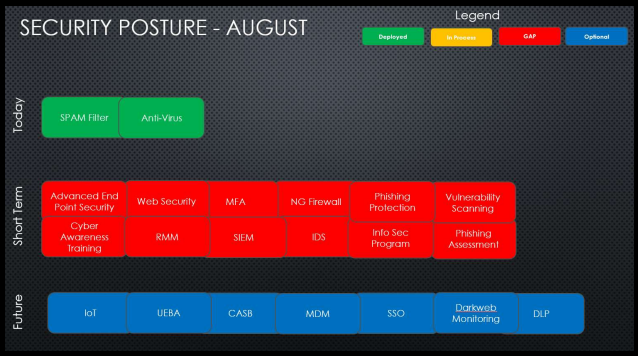
We also deployed our 'SOC In A Box' Breach Detection system to provide immediate visibility across the environment with a 24/7 Security Analyst Team to monitor for malicious activity. This unique system is able to bring together all the solutions we implemented.

CASE STUDY

FACT SHEET

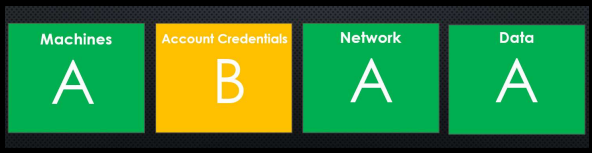
BEFORE

This image illustrates the security architecture before we started working with the client. The Red areas identify the gaps in security



AFTER

Our February 2019 scorecard shows a significant improvement. Malware was being blocked or contained on our client's machines, account exposure was minimal, layered defense systems prevent network breaches and all data is protected, backed-up off site and encrypted. Any security issues are notified to us in real time.



Our Client's Security Architecture In February 2019

The Results

Our client is delighted with our work. They now benefit from real-time comprehensive visibility of all relevant events which might compromise security. The protection we are able to offer extends to their datacentre, employee machines, user accounts and cloud infrastructure.

We now provide a fully managed solution for data security, assessing each security alert identified by our SOC in a box platform. This includes the firewall, servers, endpoint agents, cloud infrastructure and network monitoring. We assess vulnerabilities on an ongoing basis and proactively manage the firewall and web security gateway.

In 2019 we will be leading the way in assisting our client with a completely new network design with an in-depth integrated security programme. This activity coincides with a major investment as the business looks to double the size of its workforce and expand into a 150,000 square foot space and to develop global distribution centres.

Our outstanding service has ensured that we have a long-term relationship with our client and we look forward to working with them to build their future success.

About Us

CyFlare is a 24x7x365 Cyber Security Operations Center. We provide cyber consulting, penetration testing, SIEM management, compliance enablement and managed security services for several cyber security vendors.