UnderDefense
CYBERSECURITY

A Merchant Bank Puts Trust in UnderDefense for Incident Response and Post-Breach Recovery

About the client

The client is a small boutique investment bank that provides sophisticated, high-quality advisory and financing services to middle-market companies, family offices, investment firms, and entrepreneurs. They specialize in strategic advisory, capital raising, public & private markets investing, mergers & acquisitions, and restructuring.

Headquarters:	Florida, USA
Industry:	Investment Banking / Private Equity
Company Size:	10-49 employees
Client Since:	June 2021
Technologies and Tools:	SentinelOne EDR, Windows Server Update Services (WSUS), Dropbox, Sysmon, KnowBe4 Silver
Provided Services:	Incident Response, 24/7 MDR, vCISO, Incident Response Retainer
Internal IT Security Team:	No
Infrastructure:	Hybrid

Data-Driven Outcomes

90%
of threats are detected and resolved immediately

40+
Covered endpoints

330
Alerts managed outside working hours

26%
of contained threats could cause business disruption

992
Incidents investigated

CHALLENGES

- Poor security awareness and staff unpreparedness for cyberattacks
- Use of an unsecured Dropbox platform for file sharing, resulting in sensitive data exposure
- Zero endpoint protection
- Sensitive files on Dropbox were immediately encrypted and unrecoverab
- Lack of a Business Continuity/Disaster Recovery (BC/DR) plan

SOLUTION AND RESULTS

- Comprehensive cybersecurity awareness training for employees. Development of clear security policies to reduce risks of cyber incidents, ensure compliance with industry regulations, improve productivity, enhance reputation, and save costs
- Implementation and full configuration of endpoint protection software to improve overall security posture, prevent further infections, and eliminate the risk of data breaches
- Introduction of a secure collaboration policy and communication channels. Control of file-sharing activity to prevent unauthorized access and reduce the risk of sensitive data exposure
- Isolation of the infected system, plus determining the scope of the infection, restoring data from backups, and implementing measures to minimize downtime and the impact of data loss
- A comprehensive BC/DR plan to mitigate disruptions, prevent financial losses, and maintain critical business operations

UnderDefense

UnderDefense is a global leader in cybersecurity solutions. We are ISO27001 certified in cybersecurity, privacy and data protection. Our mission is to assure greater Cyber Resiliency and business continuity for small and medium-sized enterprises. Worldwide.

Address: suite 420, 111 John St New York, NY 10038, USA
Tel: +1 929 999 5101
email: help@underdefense.com
Website: underdefense.com