CASE STUDY

Midsize manufacturer implements Antigen Titan Defense Complete after ransomware attack

A midsize metal manufacturer was turned upside down when the Conti ransomware group launched an attack on their network. The threat actors had infiltrated the manufacturer's network several months before carrying out the ransomware attack, with strong indicators that an initial access broker was involved.

The ransomware attack encrypted the manufacturer's systems and data, bringing plant operations to a grinding halt and resulting in lost revenue, employee wages, and line stoppage. After several days of downtime with no progress in restoring operations, they brought in the incident response and recovery engineering experts at Antigen to help them remediate the attack and restore operations. The team performed a complete forensic investigation and restored the organization's files from backup systems, helping them get back up and running within five business days of beginning their investigation—and this enabled the manufacturer to avoid paying the $2 million ransom.

Because of the quick work of the Antigen team, the manufacturer avoided contractual fees and reputational damage with customers as well as suppliers.

Antigen discovered some gaps in the manufacturer's security program that needed to be remedied in order to build up their defenses to withstand a similar breach.

First, the Antigen team discovered that the Conti threat actors had accessed the organization's system via a vulnerable version of Exchange. To remedy this, Antigen helped the manufacturer convert from on-prem Exchange to M365, as well as obtain E3 licensing to support business growth.

COMPANY

Manufacturer with multiple plant locations

CHALLENGE

Ransomware attack shut down production for nearly two weeks

No EDR/MDR solution to detect attacks

Zero trust not employed to restrict threat actor movement

Cyber insurance with $1M deductible did not make them whole after halted production

SOLUTION

Antigen's DFIR and recovery engineering teams helped the plant restore operations within five days from the start of their investigation. They migrated from on-prem Exchange to M365, and implemented Antigen Titan Defense Complete. The next-generation cyber insurance provides them financial protection moving forward to sustain them from future incidents if they occur.

The ransomware attack halted operations and resulted in lost revenue. Without Antigen's efforts this could have been a much worse outcome for them.

CASE STUDY

Midsize manufacturer implements Antigen Titan Defense after ransomware attack

Antigen also noted that the manufacturer was not using an EDR or MDR solution that would have helped to detect an attack like this, nor was it employing a zero trust solution to restrict movement on a compromised endpoint.

Finally, the manufacturer did have cyber liability insurance, but they had a $1 million deductible. This means that before the insurance company would pay anything toward the damages incurred, the first million would be paid out of pocket by the manufacturer. Because they didn't have a next-generation cyber insurance solution, the manufacturer needed to pay over a half million dollars out of pocket.

The Titan Defense Complete solution, which is a next-generation cyber liability insurance solution that offers both technology and financial protection, was a perfect fit. Microsoft Defender for Endpoint was deployed as part of this security program, addressing the gap in EDR/MDR coverage. Using Illumio's zero trust segmentation technology alongside other solutions in the program, Antigen closed the gaps.

Finally, the manufacturer was able to obtain next-generation cyber liability insurance through Antigen's exclusive program—which includes a Service Assurance Warranty that serves as the first layer of financial protection for any future incidents. This eliminates the burden of having to pay out of pocket.

By implementing Antigen Titan Defense Complete, the manufacturer is now far less susceptible to a large-scale ransomware attack and has the financial protection to keep them from incurring out-of-pocket loss in future incidents.

ANTIGEN TITAN DEFENSE COMPLETE SECURITY PROGRAM

- Exclusive access to next-generation cyber liability insurance coverage
- Endpoint Detection & Response
- Managed Detection & Response
- Multifactor authentication
- Advanced email and cloud protection
- Zero trust segmentation

Please contact us to get started with Antigen Titan Defense Complete!

AntigenSecurity.com