Vernovis Keeps Production Running

CASE STUDY: CYBERSECURITY

The Challenge

A manufacturing company with 19 factories and a datacenter, experienced a cybersecurity breach that was crippling their network. Their servers rebooted every single day for three weeks and their team did not have the knowledge or skillset to identify the cause or address it. They had contacted several other vendors for help who all told them the only option was to shut down production until the breach was rectified.

The Approach

Vernovis provided a team who was onsite within hours and informed the company that they could remediate without shutting down and losing production hours. The Vernovis subject matter experts identified there was an active virus breakout and detected 384 instances with 30-35 different variants, the most prominent being TrickBot. Some of the viruses dated back four years.

Within two days, the Vernovis team stabilized their environment

and within four days, the company was secure.

The Result

It was paramount for the team to be able to contain and eliminate the virus breakout without stopping production. In doing so, Vernovis saved the organization an unquantifiable amount of revenue and enabled them to return to business operating standards within four days. The company's environment is stable and Vernovis' team implemented proactive security measures including firewall and anti-virus.

Consultant-driven results

384 viruses
contained and removed

0 hours
of stopped production

2 days
to remediation

4770 Duke Dr., Suite 180, Mason, OH 45040 | 513.234.7201
169 S. Liberty St., Powell, OH 43065 | 614.569.5212
www.vernovis.com

VERNOVIS Inc. 5000