Case Study: IT Recovery

ESSINTIAL
ENTERPRISE SOLUTIONS

Essintial plays crucial role in saving customer $14M in Bitcoin ransomware demands

The Customer

Essintial's end customer is one of the world's largest multinational confectionery, food and beverage companies with a revenue in excess of $25 billion, annually.

Headquartered in Illinois, the company employs more than 100,000 people around the world in support of manufacturing, marketing and distribution of its products in approximately 165 countries worldwide.

What	Ransomware attack affecting 56,225 customer PCs
Where	98 North American cities and 73 territories and countries worldwide
Outcome	Recovery of U.S. PCs completed successfully in 3 weeks

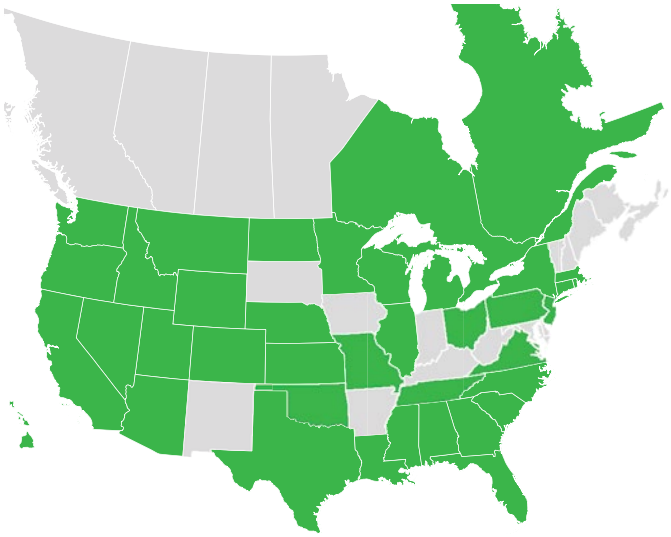
The Challenge

The customer experienced a malicious, far-reaching ransomware attack that impacted 56,225 users simultaneously worldwide, including 5,802 PCs across 98 North American locations. The attack — dubbed "WannaCry" — blocked access to the computer systems as the attackers required a ransom be paid before allowing access.

Initially, the customer was in a reactionary position as reports continued to pour in from individual users that had been victims of the attack. Even though the customer possesses robust internal IT services, they simply did not have enough resources, infrastructure or labor support to handle the number of PCs that needed re-imaged, nor the capability to track deliverables on the worldwide scale required.

The Solution

The OEM engaged Essintial to assist with this attack in two strategic ways. The first was for Essintial to provide supplemental on-site technicians to assist their IT team in re-imaging the affected machines across North America and minimize additional infections. The second engaged Essintial's business intelligence team to track and report on worldwide recovery efforts 24/7 until the customer had the attack under control with internal resources.



THANK YOU FOR YOUR GROUP'S HELP! THE TEAM I WORKED WITH IS VERY PROFESSIONAL AND VERY HELPFUL. **THANKS AGAIN FOR THE HELP ON SHORT NOTICE.**
— OEM PROJECT MANAGER

Once engaged, Essintial immediately began work to mitigate further damage by isolating PCs from unaffected servers while preparing the media and creating the image files for the on-site re-imaging. Simultaneously, team members worked to locate Essintial Certified Technicians in proximity to affected areas. These technicians were selected, trained, equipped and began re-imaging PCs within two days of engagement.

Within a day of engagement, Essintial's business intelligence team learned the customer's process, built from scratch their own recovery tool set to analyze and record the global deliverables, and setup round-the-clock shift coverage including weekends. This team automated processes and created customized daily reporting to meet the customer's unique and urgent needs. They served as the centralized HUB for all data, tracking real-time progress on each of the 56,225 computers across 73 different territories and countries worldwide.

The Results

Essintial quickly became a strategic partner in the ransomware recovery, accommodating priorities that had been ranked by the customer to ensure that the most critical systems were brought back online first. Essintial brought to the project ***the scalability and flexibility for rapid ramp-up*** — work began within hours of engagement — helping the customer to meet compliance regulations and ensuring that the project exceeded recovery-time-objectives (RTOs).

Within three weeks, Essintial was able assist the customer in quickly restoring operations and ***minimizing downtime, thus reducing the impact to the business***. Essintial technicians effectively restored 3,215 of the affected PCs in North America, upgraded with improved virus definitions to enhance system security, and reconnected to network operations. These efforts allowed Essintial to ***play a crucial role in saving the customer more than $14M in Bitcoin ransom*** that our customer avoided paying to the hackers.