Case Study

ThreatDown
Powered by Malwarebytes

NELLO Defends Against Ransomware and Finds Peace of Mind with ThreatDown MDR

NELLO is a steel manufacturer based in South Bend, Indiana. NELLO fabricates steel poles that connect wind and solar power and other sources to the electric grid. It also makes communications poles and towers used for radio, TV, etc. The company size is approximately 250 people, with an IT/security team of four individuals.

For endpoint security NELLO relied on Webroot Antivirus for 6 years—but Webroot did not prevent or respond to a ransomware attack which wiped out a significant portion of NELLO's data, including backups. While no ransom was paid, damages were approximately $8 million from paying employees during the outage, and liquidated damages from contracts. After Webroot's failure to prevent the attack, NELLO embarked on upgrading its security.

> "The ransomware spread quickly, and while Webroot tracked how it was moving around, Webroot didn't do anything to stop it. So, we decided it was time for a change and switched to ThreatDown. Now, we get more intervention and transparency about what our antivirus is doing and what threats it handles. Plus, with ThreatDown MDR, we can see exactly what's going on to stop attacks."
>
> **Tammy Orr, IT Manager**
> **NELLO**

Selecting a More Reliable Cybersecurity Solution with ThreatDown

When looking to replace Webroot, NELLO compared several antivirus products, including Kaspersky, ThreatDown, powered by Malwarebytes, Avast, and Microsoft Defender. Kaspersky was soon ruled out, however, due to security concerns. Avast had higher false positive rates, which NELLO was concerned would disrupt workflow. Microsoft Defender was slightly more expensive and posed support challenges. IT Manager Tammy noted, "We were worried about Microsoft not listening to us

Partner-At-A-Glance

Customer - NELLO
Industry - Steel Manufacturing
Country - United States

Displaced Solution

Webroot

ThreatDown Solutions

ThreatDown EDR
(Endpoint Detection & Response)
ThreatDown MDR
(Managed Detection & Response)

NELLO's primary concerns included minimizing false positives, ensuring effective ransomware protection, and having responsive support. Expense wasn't a major factor, given the potential cost of ransomware attacks. "Preventing ransomware was worth practically any amount of money," Tammy said.

ThreatDown, powered by Malwarebytes eventually emerged as the top option. "We knew ThreatDown was meant for modern threats and was highly recommended for businesses," Tammy recalled. ThreatDown also had low false positives and ‘acted as a canary in the coal mine’ according to Tammy, alerting her and her team to machine failures early.

The enterprise-level features of ThreatDown, such as remote management and patching capabilities, streamlined and saved NELLO some additional costs. "Being able to look at software and patch it was a great add-on," Tammy said. Tammy also mentioned the criticality levels for CVEs were more informative than those from Kaspersky, whose patch management a former employer of hers had used in the past.

Results

- **Significant Financial Losses** avoided by proactively preventing ransomware attacks
- **24/7 Threat Monitoring and Response** allows the team to focus on other tasks
- **MDR Team Detects and Deletes** infections before they cause damage
- **Peace of Mind** allows the team to rest without fear of missing critical threats

Ultimately, NELLO trusted ThreatDown to be more responsive to their needs, essential for their high-value machinery. “We’ve got pieces of steel worth $40,000 or more being processed by machines that have to run antivirus—we felt like we couldn’t trust Microsoft to avoid damaging pieces of steel, or to care if they did damage one,” Tammy said ThreatDown’s stated focus on working with small and medium sized companies made her feel she could trust ThreatDown to listen to her team more than Microsoft.

> “We looked at ThreatDown because we knew it was designed for modern threats. And it was up in all the rankings, like it was in the Top 10 recommended for businesses anywhere you looked. We needed a solution focused on small and medium businesses, and ThreatDown fit that bill.”
>
> **Tammy Orr, IT Manager**
> **NELLO**

Expert Monitoring and Rapid Response: The MDR Difference

After NELLO’s devastating ransomware attack, there was constant fear of missing something critical—Tammy and her team were aware of their limitations. "We can't handle everything alone. If a bad email comes in at 3 a.m., we can't be the only line of defense," Tammy explained. The need for specialized help was clear.

When ThreatDown Managed Detection & Response (MDR) became available, it was a huge relief to Tammy. "We loved the idea of ex-military or government security specialists monitoring threats while we're on vacation," she said. The MDR service offered a playbook-guided response, which was crucial, as Tammy and her team “didn't have a playbook and couldn't respond quickly enough.” The choice to trust an external MDR service was solidified after a positive conversation with the ThreatDown MDR manager. "He understood our unique challenges, like a factory machine rebooting and causing significant damage."

With MDR, Tammy and her team could get more sleep and take vacations. "ThreatDown MDR just finds threats and deletes them. They're able to clean up hard drives and registries without disrupting users," Tammy noted. She also appreciated how the MDR team, operating from different time zones, provided round-the-clock monitoring. "They don't get tired. They write to us with clear questions about our network activity. The transparency and trust are huge to me."

The MDR service has prevented infections, handled malware, and offered real-time action. "They found and deleted infections before we even had to get involved," Tammy said.

Confidence with 24/7 Monitoring: Peace of Mind Restored

After a harrowing $8 million ransomware attack that Webroot missed, Tammy and her team have gained significant peace of mind after switching to ThreatDown.

Feeling more confident that major attacks will likely be stopped now, Tammy appreciates the MDR team's around-the-clock monitoring and quick response to potential infections. Especially given the financial impact of the previous ransomware attack, the ROI of the ThreatDown MDR is clear. "MDR is like insurance; it's cheaper than the damage caused by ransomware," she emphasized.

> “After the ransomware attack, management realized the critical need for investing in security. The benefits of ThreatDown MDR became evident, providing 24/7 monitoring and rapid response to threats, convincing management of the importance of prioritizing security to avoid future costly incidents.”

Tammy Orr, IT Manager
NELLO

Find the right plan for your business

Be assured threats are never missed, lurking criminals are evicted, and critical incidents solved.

Learn more