

# Textile Management Associates makes a clean sweep of ransomware

Protects assets and data with Malwarebytes

## Business profile

Textile Management Associates, Inc. operates as a holding company. Its subsidiaries produce carpet, as well as synthetic sports turf systems. After a ransomware attack encrypted business-critical data, the company turned to Malwarebytes to prevent its return.

## Business challenge

### Halting ransomware across the company

Headquartered in Dalton, Georgia, Textile Management Associates' subsidiaries play important roles in the manufacture of carpet and artificial turf surfaces. As malware, spoofing emails, and ransomware incidents increased, Textile Management Associates wasn't going to tolerate them.

"We began to see spoofing emails evading our spam filter," said Nathan Henson, Network Engineer at Textile Management Associates. "Our Symantec Endpoint Protection antivirus also missed several instances of ransomware, which encrypted data and created significant disruption."

Subsidiary CFOs received emails requesting wire transfers that supposedly were sent by the company's owner. Spoofed email recipients recognized the messages as fake. Even though recipients weren't fooled, the IT team had to spend several hours on each incident to determine where the fake emails came from and who sent them.

Ransomware incidents were even more time-consuming and costly. The largest attack encrypted several large computer drives containing product imagery, descriptions, and other critical sales data. Besides disrupting business processes, the drives had to be sent to data recovery specialists.

## OVERVIEW

### INDUSTRY

Manufacturing

### BUSINESS CHALLENGE

Avoid the disruption and costs associated with ransomware remediation

### IT ENVIRONMENT

Symantec Endpoint, layered enterprise security

### SOLUTION

Malwarebytes Endpoint Security

### RESULTS

Prevented future ransomware and malware infections

Enabled proactive, ongoing monitoring to target threats and reduce time spent investigating incidents

Simplified endpoint security management with "set-and-forget" ease of use



THE MOST IMPORTANT THING IS THAT THE COMPANY'S ASSETS AND DATA ARE PROTECTED. MALWAREBYTES IS A NO-BRAINER.

—NATHAN HENSON, NETWORK ENGINEER, TEXTILE MANAGEMENT ASSOCIATES

“I had used Malwarebytes in the past and knew that it would stop these threats,” said Henson. “I recommended that we deploy it company-wide on every machine. That’s what we did.”

## The solution

### Malwarebytes Endpoint Security

Textile Management Associates deployed Malwarebytes Endpoint Security for multi-vector protection that combines advanced malware detection, remediation, ransomware blocking, malicious website blocking and exploit protection into a single solution. Henson deployed Malwarebytes using a third-party deployment tool, rolling it out to hundreds of computers in less than four hours.

“Malwarebytes protects our entire enterprise for what we paid to recover a single drive,” said Henson. “We know Malwarebytes is working because we can see what it stops.”

### At-a-glance view

Henson and his team use the Management Console for ongoing monitoring of the company’s endpoints. Each day they review the top 10 clients with the most threats and exploits and ensure that all systems are updated. Data from the Management Console also gives the team insight into potential vulnerabilities.

If the same systems continually show up in the reports, the team can assess whether or not web filter controls should be tightened or other measures taken. If they suspect a problem on a specific PC, they will physically check the machine.

“With Malwarebytes, we can proactively focus on specific incidents and target threats, instead of having to guess,” said Henson. “It only takes one infected PC to ruin an enterprise. Malwarebytes makes it easy to have an enterprise-wide overview and drill down into the details.”

### Clean as you go

Henson set Malwarebytes policy to remediate threats as they are detected and quarantined. Textile Management Associates has had no more ransomware or malware infections, and the service desk no longer receives calls from users about odd system activity. Henson said that Malwarebytes is very lightweight on endpoints and servers, requiring few resources. Users didn’t even know that Malwarebytes was installed.

“The most important thing is that the company’s assets and data are protected,” said Henson.

“Malwarebytes is a no-brainer. It has never stopped. In deploying it to hundreds of computers, we haven’t had a single error. Malwarebytes is just easy.”



[malwarebytes.com/business](https://malwarebytes.com/business)



[corporate-sales@malwarebytes.com](mailto:corporate-sales@malwarebytes.com)



1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company’s flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at [www.malwarebytes.com](https://www.malwarebytes.com).