

# BrandSafway boosts IT productivity globally

Stops advanced malware, ransomware, and downtime with Malwarebytes

## Business profile

BrandSafway is global provider of specialized services to the industrial, commercial, and infrastructure markets. The company offers access and scaffolding systems, forming and shoring, industrial services, and related solutions to more than 30,000 customers worldwide. BrandSafway turned to Malwarebytes to protect employees in 30 countries against cyberthreats.

## Business challenge

### Scaling protection with growth

BrandSafway has grown rapidly through mergers and acquisitions. With each acquisition, the company increased its global presence—and its attack surface. BrandSafway had a combination of McAfee and Symantec antivirus software on endpoints due to mergers, but transitioned to Microsoft System Center Endpoint Protection.

“Neither solution was protecting adequately against spyware and malware,” said Mr. Satinder Purewall, IT Director of Global IT Operations at BrandSafway. “The sheer number of attacks was overwhelming our service desk teams.”

Service desk IT engineers were spending days cleaning or rebuilding PCs. When machines were infected, remediation also took time away from users in the main office and on remote job sites. Cyberthreats reduced productivity and frequently re-infected systems. Cleaning up malware often required an IT engineer to access the system remotely for diagnosis and restoration.

“We needed much better, more sustainable protection,” said Mr. Purewall. “We began looking for a product that was behavior-based, instead of signature-based, to defend against malware and advanced threats like ransomware.”

## OVERVIEW

### INDUSTRY

Industrial services

### BUSINESS CHALLENGE

Stop the cycle of malware infection and reinfection and associated downtime

### IT ENVIRONMENT

Microsoft System Center, layered enterprise security

### SOLUTION

Malwarebytes Endpoint Protection

### RESULTS

Eliminated ransomware incidents

Stopped threats during new acquisitions

Saved thousands of hours of valuable IT staff time globally

Gained endpoint coverage visibility to further reduce operational risk



THE DIFFERENCE WITH MALWAREBYTES WAS NIGHT AND DAY. IT QUICKLY DEALT WITH NEW TYPES OF THREATS. IT'S OUR DEFACTO STANDARD NOW.

MR. SATINDER PUREWALL, IT DIRECTOR, GLOBAL IT OPERATIONS, BRANDSAFWAY

## The solution

### Malwarebytes Endpoint Security

Mr. Purewall and his teams were familiar with Malwarebytes as a remediation tool. Now, they turned to Malwarebytes and initiated a trial of Malwarebytes Endpoint Security to add a layer of protection to the company's endpoints running Microsoft System Center Endpoint Protection.

"For us it was a no-brainer," said Mr. Purewall. "Malwarebytes was one of the first solutions to provide behavioral-based threat analysis. When we trialed it, it was rock solid."

The team deployed Malwarebytes using Microsoft System Center Configuration Manager, bringing all users' endpoints under protection. Recently, BrandSafway acquired another company that was using a security solution from Cisco. Once again, Mr. Purewall and his team evaluated their options for endpoint security.

"We had a baseline antivirus solution and Malwarebytes as a second layer of protection against malware, spyware, exploits, and ransomware," he said. "The new company increased our user base by almost 40 percent, and the cost of scaling their existing solution was extremely high—with little incremental protection. We chose to stay with Malwarebytes."

### Reduced impact

Malware no longer drains productivity for service desk IT engineers or users. It works in the background blocking thousands of viruses, malware items, spyware, malicious websites, and dangerous links. BrandSafway hasn't experienced any ransomware incidents since deploying Malwarebytes.

"The difference with Malwarebytes was night and day," said Mr. Purewall. "It's our defacto standard now. If we turned it off, we'd have significant problems."

### Saving time

Prior to Malwarebytes, it was normal to take several hours to rebuild a PC and have to do it again the next day, because the system was still vulnerable to the same threat. With users and technicians around the world, fighting threats across multiple countries in multiple time zones and languages taxed the IT teams.

"Malwarebytes has been a huge time savings for our IT teams," said Mr. Purewall. "I can easily say that we've saved thousands of hours since we deployed it."

Malwarebytes alerts also save time. When Malwarebytes quarantines a threat that requires attention, it sends an email alert to the IT team. Technicians can immediately isolate and troubleshoot the specific device, deciding how to respond based on the severity of the issue.

### Covered and confident

"Having visibility into the protection on our endpoints is always important," said Mr. Purewall. We measure how well we're managing our installed base and ensure that we're minimizing the risk of disruption to our business."

The IT team can instantly see which version of Malwarebytes is running, ensure that machines are covered, and that all are upgraded. They correlate coverage data from Malwarebytes with data from System Center Configuration Manager to confirm coverage and use for planning purposes. The IT team is confident in Malwarebytes' ability to continue protecting endpoints even as threats change.

"Malwarebytes is quickly able to deal with new types of threats," said Mr. Purewall. "It has been dependable for us and has had tremendous impact on our ability to protect our endpoints, users, and productivity."



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



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



1.800.520.2796

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at [www.malwarebytes.com](https://www.malwarebytes.com).