



Improved security at lower cost through best practices and technology solutions for a media multinational.

Globally, malware is expected to cost businesses a staggering USD 114 billion . Farsighted enterprises are therefore investing in robust endpoint security; and upgrading their protection and practices to keep up with the latest challenges.

Here is how Mindtree helped a global enterprise devoted to creating original content and effective digital advertising become more resilient in the face of malware threats.

The challenge

The customer was dissatisfied by the performance of their endpoint security suite for malware protection. Their malware detection and cleaning rate was very low; and they had faced three zero-day incidents within a year that altered Web content, their primary business strength. Consequently the customer was looking for a proactive solution to enhance effectiveness at a lower operational cost.

Specific concerns included:

- Firefighting zero-day infections (infections unknown to the security provider) involved considerable business risks, costs and effort
- Implementing a new endpoint security product as a solution would involve greater licensing costs, implementation time and effort


Our solution

Mindtree team proposed a solution that did not necessitate a change in endpoint security software, thereby avoiding considerable expenditure. Our approach was based on research of malware threats, possible responses and best practices deployed by others in the industry.

The team's investigation of the customer's security revealed that they were not following best practices recommended by the industry experts. We then conducted a detailed analysis of all antivirus security policies and recommended changes to make the customer more resistant to malware attacks.

Business impact

- Savings of USD 200,000 in licensing costs
- Savings of 1,000+ man hours compared to a new endpoint security suite
- 15% reduction in the number of malware tickets recorded
- No zero-day incident has been encountered since implementation of the new solution
- Average malware detection and cure rate increased from 3,000+ events per month to 33,000+ events per month



We also implemented two technology changes within the existing endpoint security suite. These changes were implemented across over 4,000 workstations and 1,000 servers within a span of one month.

- **Real-time threat protection:** This is a free solution that provides the customer with always-on real-time protection that safeguards and secures them from emerging threats. As a result, the customer can prevent damage and data theft even before a signature update is available. This makes endpoints smarter and safer from the zero-day infections.
- **Memory scans:** Scanning of memory and processes provides an early warning system for endpoint-protected computers. We enabled this feature as part of the customer's protection. Scans are unobtrusively completed in 30-90 seconds with no impact on end users.

About Mindtree

Mindtree is a global information technology solutions company with revenues of over USD 400 million. Our team of 11,500+ experts engineer meaningful technology solutions to help businesses and societies flourish. We enable our customers achieve competitive advantage through flexible and global delivery models, agile methodologies and expert frameworks.