CASE STUDY

Traditional anti-virus solutions didn’t stop the infections

Challenges

IT Manager, Erick Chng, is responsible for the security posture of Kee Song, a fast-growing food producer processing over 25,000 chickens daily and serving the most celebrated restaurants and hotels in Singapore. With the addition of online ecommerce, Chng faced new security risks in key departments including Finance, Customer Service and Operations.

• **Traditional reactive anti-virus solutions** did not adequately protect against ransomware, phishing and advanced cyber threats
• **Inability to prevent ransomware attacks** spreading within the company
• **Lack of visibility or detection** for infected endpoints
• **Unacceptable slow reporting time**, often taking weeks or months
• **Low server performance** with scanning leading to unacceptable long latencies

Chng urgently requested the company replace the three legacy solutions and select a new cybersecurity partner that Kee Song could rely upon for safe, robust operations.

Reasons for Choosing Malwarebytes

Chng had three important criteria against which he evaluated the leading security solutions:

• **Fast detection and prevention of malware**: Malwarebytes had industry awards citing fast detection and prevention of ransomware, phishing, zero-day, and newer attacks.
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.

Copyright © 2020, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.

• **Robust remediation:** Malwarebytes included automated Linking Engine remediation
• **Continuous innovation:** Malwarebytes invests in proactive AI and ML, Linking Engine remediation that removes threat artifacts linked with the primary payload, and multi-vector protection.

**How Malwarebytes Solved the Problem**

• **Detected infections in 90% of target endpoints** that three previous solutions missed
• **Threat reporting in < 48 hours as opposed to months,** if ever, with previous solutions
• **Remediation immediately stopped the spread** of commerce-threatening infections
• **100% visibility across all endpoints** including mobile platforms
• **Secured high-risk departments:** finance, customer service, and operations

"After Malwarebytes was up and running, the solution reported in under 48 hours that 90% of polled endpoints were infected. Remediation was so quick the infection stopped spreading. The scary part was that traditional anti-virus solutions previously deployed didn’t pick this up.

Erick Chng, IT Manager
Kee Song"