CASE STUDY

Ransomware consistently evades antivirus systems

Challenges

- Ransomware would evade Dexion’s security defenses and arrive in an email attachment
- Users’ operating systems, encrypted files, and on-premises file servers would get corrupted
- It would take the IT two whole days to recover files and clean systems after an attack
- Antivirus solutions had little protection against ransomware and advanced malware

Reasons for Choosing Malwarebytes

- Simple deployment: Malwarebytes’ deployment tool pushes the software to endpoints and handles everything on the back end.
- Versatile protection: Malwarebytes effectively mitigates all kinds of malware, ensuring that endpoints are protected from any kind of threat.
- Wide reach: Malwarebytes can be deployed on a range of technologies and protects Dexion’s servers, laptops, and desktop systems.
- Cloud console: Malwarebytes’ centralized management system allows instant insight into the details of an infection, including the user, time, how the user was infected, and remediation measures taken.
How Malwarebytes Solved the Problem

- **Restored hours of time** for the infrastructure team by eliminating the need to constantly remediate systems
- **Proactively protects users** from malicious websites, downloads, attachment, redirects, and other threats
- **Provides visibility and actionable data** for compliance and user training
- **Training sessions and handouts** help employees learn to recognize threats and avoid system compromises

“Malwarebytes helps us avoid breaches and stay in compliance. With Malwarebytes, it is like I have a security analyst inside every user’s computer at a fraction of the cost of hiring one.”

Andrew Luu, Infrastructure Manager
Dexion Asia Pacific