5 MUST-HAVES FOR AGENCY CYBERSECURITY

Whether you’re replacing a traditional antivirus product, or supplementing an existing cybersecurity tool, your next-generation threat prevention and remediation solution must be compatible with your agency’s cloud-based, telework model.

![](graphic)

1. Third-Party Risk Management
   How do you make sure your agency is protected from risk introduced by any contractor who enter your environment? You need cybersecurity solution capable of discovering their endpoints and scanning to detect threats across your ecosystem.

2. Automation to Assist Staff
   Finding cybersecurity talent can be a struggle, and government have a more limited budget for IT and security staff. You need a cyber threat detection platform using automation to maintain your level of service and protection.

3. Effective Threat Hunting
   Be certain your cybersecurity solution has powerful, guided threat hunting capabilities. Discovering Indicators of Compromise (IoCs) quickly is imperative, so you can easily take action against weak points in the agency’s environment.

4. User Experience is Essential
   You were already migrating to the cloud and telework accelerated that initiative. Cloud-native endpoint detection and response (EDR) must have a good user experience: easy to deploy and manage for IT, unintrusive for end users, to be successful.

5. Response and Recovery
   It is critical to isolate infections fast and eradicate executables. However, you must also ensure the artifacts and other alterations aren’t left behind. For ransomware attacks, be sure you can roll back at least 72 hours to a pre-attack state.

MALWAREBYTES FINDS MORE
Your existing endpoint protection product may be leaving you exposed. In fact, Malwarebytes finds as much as 40% more malware and ransomware traditional products leave behind. Let us help your agency with better prevention and remediation.

Request a Demo >