dlrSecured

Automotive Endpoint Defender

Securing Your Dealership's Data and Technology

Retail Management System

Reynolds & Reynolds®

The State of Dealership Software Security

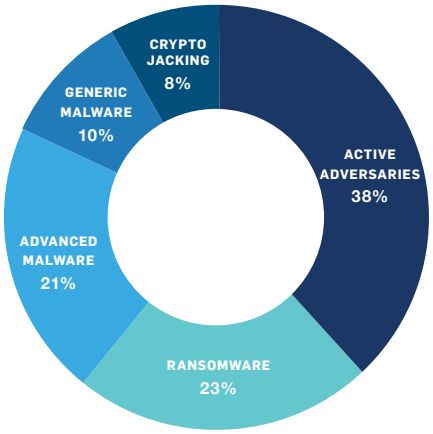
Global ransomware volume is on the rise, and predicted to keep growing far into the future. According to SophosLabs, 51 percent of organizations were hit by a ransomware attack in 2020 and 73 percent of those attacks were successful. [1]

Automotive retail is not immune to cyber attacks. If anything, dealerships are at an increased risk due to the amount of consumer information they must protect. Some notable attacks in the automotive industry include:

- DealerBuilt data breach which affected over 100 dealerships and their customers. [2]
- Volkswagen/Audi data breach which allowed access to over 3.3 million consumer records. [3]

51%
hit by ransomware

73%
of attacks were successful



Source: State of Ransomware Survey 2020

- A number of dealerships, dealer groups, and state dealer associations across the country have experienced direct ransomware attacks, stalling operations for days. [4, 5]
- Mercedes-Benz data breach that impacted over 1.6 million customers. [6]
- Nissan North America data breach that leaked source code for internal tools. [7]

Losing this valuable information can lead to fines and penalties, increased corporate liability, as well as the loss of customer confidence and future business.

So, how can you ensure your dealership is protected? The first step is implementing a security program that layers threat **prevention, detection, and response.**

[1] *Sophos Labs*

[2] Miller, T. (2017, January 27). Green Bay-area Honda dealership caught up in national data breach. *2First Alert WBAY.*

[3] *Dealers, brands must protect customer data.* (2021, June 21). AutomotiveNews. https://www.autonews.com/editorial/dealers-brands-must-protect-customer-data

[4] *Braman dealerships affected by cyberattack, report says.* (2021, April 20). Automotive News. https://www.autonews.com/dealers/braman-dealerships-affected-cyberattack-report-says

[5] *Protect Your Network.* (2021, June 23). Iowa Automobile Dealers Association Newsletter. https://iada.com/app/uploads/2021/06/062321AU.pdf

[6] *The Top Five Third-Party Data Breaches in June 2021, Revealed.* (2021, July 8). Black Kite. https://blackkite.com/the-top-five-third-party-data-breaches-in-june-2021-revealed/

[7] *Data Leak Hits Nissan North America.* (2021, January 6). IndustryWeek. https://www.industryweek.com/technology-and-iiot/article/21151660/data-leak-hits-nissan-north-america

Prevention, Detection, and Response

Prevention

Deny Threats Before They Run on a Device

Go above and beyond standard, signature-based prevention of known Malware. Using correlation techniques to link suspicious behaviours and activities, Automotive Endpoint Defender, a part of the dlrSecured cybersecurity suite from Reynolds and Reynolds, uses real-time threat intelligence software to connect the dots for you. The result is fewer security incidents and better protection against attacks and data breaches.

Stop Unknown Threats

Automotive Endpoint Defender uses deep learning, an advanced form of machine learning to detect both known and unknown malware without relying on signatures.

Deep learning makes Automotive Endpoint Defender smarter, more scalable, and more effective against never-seen-before threats. Automotive Endpoint Defender also includes anti-ransomware technology that detects malicious encryption processes and shuts them down before they can spread across your network. It prevents both file-based and master boot record ransomware.

Detection

Automatically Identify and Prioritize Threats

Detect New and Common Threats

Anti-exploit technology stops the exploit techniques attackers rely on to compromise devices, steal credentials, and distribute malware. By stopping the techniques used throughout the attack chain, Automotive Endpoint Defender keeps your dealership secure against file-less attacks and zero-day exploits.

Automotive Endpoint Defender includes advanced anti-ransomware capabilities that detect and block the malicious encryption processes used in ransomware attacks. Files that have been encrypted will be rolled back to a safe state, minimizing any impact to dealership productivity.

Prevention, Detection, and Response

Response

Secure Surveillance Around the Clock

With Automotive Endpoint Defender Managed Threat Response (MTR), your dealership is backed 24/7 by an elite team of threat hunters and response experts who take targeted actions on your behalf to neutralize even the most sophisticated threats.

Applying data science, threat intelligence, and the intuition of veteran threat hunters, we combine your company profile, high-value assets, and high-risk users to anticipate attacker behaviour and identify new Indicators of Attack.

How the MTR Team Operates:

- Proactively hunts for and validates potential threats and incidents.
- Uses all available information to determine the scope and severity of threats.
- Applies the appropriate business context for valid threats.
- Provides actionable advice for addressing the root cause of incidents.
- Initiates actions to remotely disrupt, contain, and neutralize threats.

Escalation and Response Options

MTR features three response modes so you can choose the best way for our MTR team to work alongside you during incidents.

Notify: We notify you about the detection and provide details to help you in prioritization and response.

Collaboration: We work with your internal team and point(s) of contact to respond to the detection.

Authorize: We handle containment and neutralization actions and will inform you of the action(s) taken.

Full Scope of Automotive Endpoint Defender Protection

Prevent	**Web Security:** Prevent end users from accessing websites that are hosting malware. Automotive Endpoint Defender checks URLs and IP addresses against a continuously updated database of “bad” examples.
	Web Control: Block users from accessing websites that are not allowed under your corporate policy. You choose which specific users and machines can access specific websites.
	Download Reputation: Downloads are given scores based on prevalence, age, and URL source and are grouped into reputation categories. These range from “Unknown” to “High Reputation”, helping ensure download safety.
	Peripheral Control: Control access to peripherals and removable media such as USB sticks and removable drives.
	App Control: Control the running or installation of specific applications. Can also be used to monitor application use across systems.
	Potentially Unwanted App (PUA) Blocking: Blocks applications that can introduce security risks or negatively affect machine performance.
	Deep Learning Malware Detection: Advanced machine learning detects malware or PAUs without using signatures.
	Live Protection: Enhances malware prevention by checking files against the latest malware in the Automotive Endpoint Defender database. This is accomplished by using real time cloud lookups.
	Host Intrusion Prevention System (HIPS): Protects against threats that are not yet known by detecting and blocking behaviour that is known to be malicious or suspicious.
	Data Loss Prevention: Monitor and restrict the transfer of files containing sensitive data.
	Exploit Prevention: Comprehensive exploit prevention software successfully blocks all known exploit techniques.
Detect	**Malicious Traffic Detection:** Monitors HTTP traffic for signs on connectivity to known bad URLs such as Command and Control servers.
	Active Adversary Mitigations: Utilizes a collection of techniques to block exploit behaviours that are commonly used by third parties trying to gain control of systems, modify applications, steal credentials, or perform various other techniques to gather information.
	Ransomware File Protection: CryptoGuard technology protects endpoints and servers by monitoring changes to files. When an event is detected, the process is automatically stopped and caching is used to revert files to an unencrypted state.
	Disk and Boot Record Protection: Monitors boot records and prevents any malicious modifications, preventing ransomware’s ability to perform a full disk encryption.
	Safe Browsing: Monitors browser behaviour and blocks malware attempting to modify the system.
Response	**Root Cause Analysis:** Get detailed information on a malware event or indicator of compromise. A data recorder is present on every machine; every time a security event occurs, a timeline of events will be recorded and sent for review.
	Automotive Endpoint Defender Clean: A targeted cleanup routine that occurs anytime a malicious event is detected. Includes cleaning files, infected applications, windows resources, and registry.
	Managed Threat Response: 24/7 lead-driven human threat hunting team that hunts and verifies potential threats.

For more information visit
reyrey.ca/automotive-endpoint-defender

Retail Management System

Reynolds & Reynolds®