CDK Global®

Network Security Simplified:

How to Protect your Dealership Reputation and Customer Data from Cybercriminals

If your data was stolen, what would you do? Would you even know?

Data risk is everywhere today.
What worked yesterday is obsolete tomorrow.

In this day and age, serving your customers includes protecting them from information breaches. Today’s cyber threat risks demand more than investing in the right technologies. The reality is that, security is not a destination – it requires continuous security intelligence defense with the right people, technology, and processes in place.

According to a 2017 study, the average cost of a single stolen data record is $141.[1]

Consider the $141 per record and multiply by let's say 50,000 records in the DMS as an example.

A dealer could be on the hook for upwards of $7 million or more, and that doesn't even consider bad press or headlines, private lawsuits, regulatory fines, the possibility of criminal penalties, and the fact that most small businesses go out of business six months following a breach.

The truth is that traditional security is now outdated security. Basic protection measures probably won't be enough to keep out professional cybercriminals.

A dealer could be on the hook **for upwards of $7 million or more.**

You’re a dealership, not a watchdog.

Turn the complexity of network security into a strategy to protect your business.

There is no shortage of ways that a dealership can become a victim of cybersecurity hacking. But few dealers have the time or resources to watch a screen and evaluate thousands of security events at all hours of the night. Mitigating today’s cyber threat risk requires network security technology that is deployed optimally, configured correctly, and monitored continuously to give the dealer a fighting chance of not making tomorrow’s headline news.

Hackers are choosing industries to target based on customer demographics and their perceived lack of security. With bank account information, credit card numbers and the personal data of new car buyers available within dealer networks, dealerships must take proactive steps to protect this data.

A network breach is a breach of trust. A loss of sensitive customer data will propel your dealership into the spotlight as headline news, which will erode the trust you built with customers—particularly those customers who were already concerned about providing their information to your salespeople.

Securing your network from cyber threats, hackers, and protecting it from malicious employees is no easy task—especially as potential threats become more sophisticated. Keeping up may seem impossible and you may not know where to start.

Ransomware is projected to attack a business **every 14 seconds** by the end of 2019, **up from 40 seconds this year**.[2]

Protect your customers around the clock with bumper-to-bumper coverage.

Cybersecurity: Is your dealership ready for modern threats?

Regulatory requirements, federal and state consumer privacy laws, and even many OEMs require dealers to proactively monitor their network for threats with real-time security event monitoring services. But only the combination of technology and expertise will provide the monitoring necessary for compliance, security, and peace of mind so you can focus on helping customers and moving cars off the lot.

This degree of monitoring requires advanced technology, and expertise that isn't generally available to a dealership—but it is now.

To help ensure dealership clients are compliant throughout their businesses, their networks, and their day-to-day data management, CDK Global developed Network Protect, a network security solution designed specifically to help dealers with network and data compliance. Managed security services from CDK and partner Nuspire Networks provide superior data threat detection and a managed service that takes responsibility for your network. A security information and event management (SIEM) service notifies the network admin in the case of a security event and also provides documentation and real-time visibility for compliance purposes.

Powered by:
nuspire
networks

CDK Network Protect provides **real-time proactive monitoring, incident response** and **remediation assistance.**

Features & Benefits:

CDK Network Protect includes:

- **Technology:** Award-winning technology geared for dealers and a higher level of service at a lower price point, with a more specialized service that can't be found anywhere else.
- **Expertise:** Thousands of dealers rely on CDK for network management, monitoring, and support.
- **Service Commitments:** CDK takes responsibility for incident response, follow-up, documentation, and system availability to ensure the highest level of quality, support, and response.
- **Reporting:** CDK and dealers have complete visibility into monitoring and support operations, with complete transparency into their network security to help with PCI, GLBA, and OEM compliance. Incidents are handled with the highest level of professionalism.

In the case of a security event, a security engineer will make a proactive call to the dealership and help with the remediation of the issue.

Powered by Nuspire and an advanced firewall by Fortigate, Network Protect is designed specifically for dealers.

With Network Protect, you'll get complete protection of your dealership's most sensitive data.

Count on Network Protect to defend your network with real-time threat monitoring, incident response and remediation services.

Secure the Network and Devices

Protect your network from security threats and exploits with advanced monitoring services at the gateway.

Cyber Threat Management and SIEM

Advanced reporting with simple-to-use, customizable dashboards, offers you the ability to track events as they are created.

Expert Security Threat Support

Maintain/troubleshoot UTM including SSL inspection, security policies, remote access VPN, and software updates.

Compliance and Regulatory

Provides controls for compliance concerns such as GLBA, SOX, and PCI.

Sources:

[1] Ponemon Institute, 2017 Cost of Data Breach Study

[2] Morgan, Steve: "Global Ransomware Damage Costs Predicted to Hit $11.5 Billion by 2019," Cybersecurity Ventures, November 2017.

CDK Global®

cdkglobal.com