MAGNUS™
TECHNOLOGIES

Does Your TMS Pass the Stress Test?

4 Keys to Evaluate the Data Security of Your Core System

Expert Analysis of TMS Vulnerabilities from a Professional Hacker

Matthew Carpenter is a senior technology strategist of cybersecurity firm GRIMM, specializing in hacking systems at a national and state level.

This guide shows how to improve TMS security with cloud services and enterprise technology.

People are the most important assets of trucking and logistics companies. Data is a close second. When key employees quit it causes a disruption but losing access to data can bring a business to a screeching halt.

Cyberattacks and other unforeseen events that cut access to information systems must therefore be treated as existential threats.

Trucking and logistics companies have traditionally deployed core transportation management software (TMS) with client-server architecture. This is the only model currently offered by the largest TMS vendors in the industry.

Maintaining on-premise servers and other client-server infrastructure requires upfront investments in hardware and software. It also requires significant overhead and ongoing investments in data security.

Improving data security is one of many reasons why trucking and logistics companies are migrating to enterprise-class TMS platforms with a software-as-a-subscription (SaaS) model.

On average, it takes transportation companies 192 days to detect a breach and another 60 days to contain it.

Finding Vulnerabilities

Gross negligence is rarely the reason data breaches occur. Employees at all levels recognize the necessity of data security but most are unaware of weak links in systems and how the vulnerabilities can be exploited by outsiders or insiders.

This awareness is essential for data security, explains Matthew Carpenter, a professional "white hat" hacker. Carpenter is senior technology strategist of GRIMM, a cybersecurity firm, and founded its company's cyber-physical exploitation group. He specializes in hacking systems at a national and state level.

When deciding between client-server and cloud-based TMS architecture — or any software platform — the most important factor, he says, is to determine if a cloud-based provider will do a better job of protecting your data than you could.

The answer depends on the platform's capabilities in four key areas:

1. Physical Security
2. Monitoring IP Traffic
3. Intrusion Visibility
4. Business Continuity

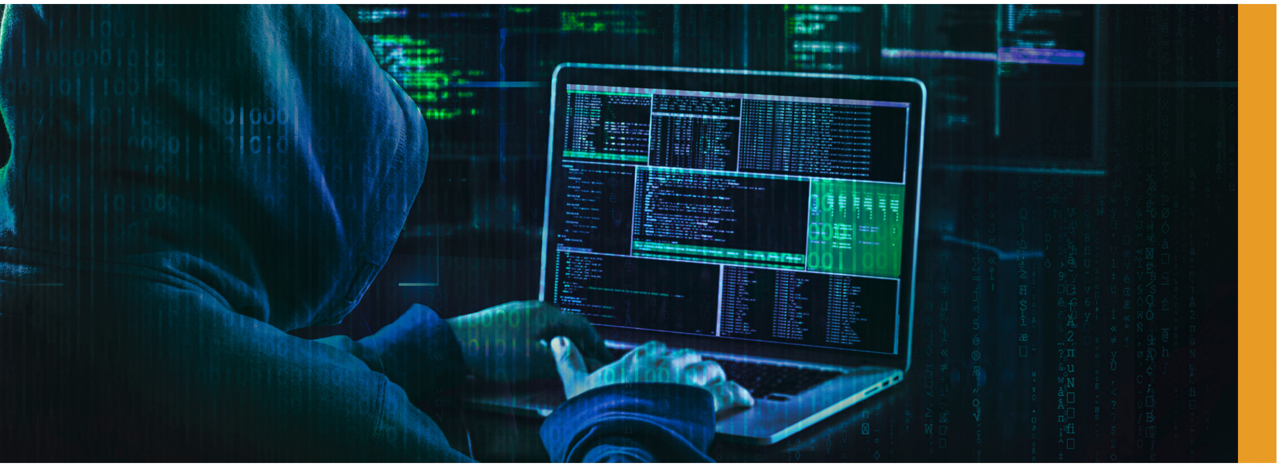
This guide provides useful tips to improve data security with SaaS-based TMS versus client-server architecture in these four areas.

1 Physical Security

The physical security layer of information systems is just as important as the virtual layer, Carpenter states. It is much easier for people to access sensitive data and disrupt a business from within by having physical access to servers and other system components.

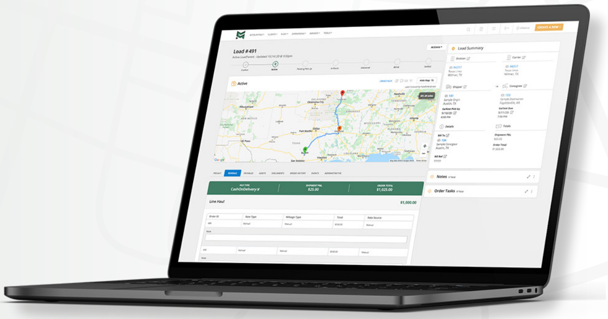
SaaS Advantage: This model defers the risks of physical access to vendors who will do a better job of consistently maintaining and securing computer systems than you would. Leading cloud computing providers, such as Microsoft Azure or Amazon Web Services (AWS), adhere to very high standards for controlling and monitoring physical access. Their standards are "far better than what a trucking company could do," said Nick Crown, chief operations officer of Magnus Technologies, which provides an enterprise SaaS-based TMS for trucking and logistics companies.

Client-Server Advantage: This may be the preferred risk model for companies that want to maintain visibility and control over physical access. Some may feel more comfortable using their own electronic locks, cameras, card readers, and hiring practices. Large businesses and government entities, for example, may want extremely valuable data – like nuclear launch codes – to stay on site, Carpenter says. Managing all the details of physical security at a high level adds monetary and complexity cost.



2 Monitoring IP Traffic

As an expert hacker, Carpenter knows that most cybercrimes start with attacking a domain controller to access user accounts. By stealing user credentials, attackers can then login to a system and continue to penetrate additional security layers until they get what they want, he explains.



SaaS Advantage: An enterprise SaaS based TMS uses advanced protocols and encryption techniques to establish a secure channel of communications between the system and web browsers of authorized users. Secure protocols for accessing SaaS-based TMS systems include Transport Layer Security (https) and Secure Socket Layer (SSL). They are the same protocols that consumers and businesses use for online banking.

Client-Server Advantage: Companies with on-premise servers can keep a certain number of applications and data protected by firewalls and set up their servers to allow communications through a virtual private network (VPN) rather than connecting to devices over the open Internet. Problems with the speed or availability of a local internet service provider will disrupt remote VPN connections to on-premise servers. Also, a strategy that hackers can use to get through VPN access is by infiltrating personal devices of employees and then finding a route into their companies' IT systems.

Key Point: The SaaS model may only allow secure protocols to access the systems, and TMS servers may be sequestered in their own little "security arena" protected by firewalling from everything else. However, a Client-Server model is more likely to allow other computers systems to be in a similar security arena, like workstations where people surf the web or check email and open attachments and, as such, are more likely to be open to malicious attackers through spear-phishing, Carpenter explains.

3 Intrusion Visibility

Preventing physical intrusions is much easier than blocking virtual ones. To protect data, organizations need to maintain control and visibility of all IP traffic running on their networks, and then quickly identify and make sense of any exceptions that occur, Carpenter said.

That is not an easy task. On average, it takes transportation companies 192 days to detect a breach and another 60 days to contain it, according to research by IBM.

SaaS Advantage: With the SaaS model, TMS providers can rapidly deploy security patches and updates to the software because customers are using the same version. TMS vendors that use leading cloud computing service providers, such as Microsoft Azure and AWS, can leverage world-class technologies and expertise to limit post-breach access. For example, a TMS provider can use advanced SIEM (security information event management) systems from cloud services that automatically identify problems and take actions that prevent disruptions.

Client-server advantage: Companies that choose to run TMS platforms on their own servers must invest in their own network monitoring systems. They also need IT experts on staff who understand how to detect and resolve data security breaches and fix processes to prevent the same things happening again, Carpenter explains.

4 Business Continuity

Disaster recovery and business continuity are important factors to consider when evaluating TMS options. In the event of a cyberattack or other major event, such as a hurricane, recovery speed is essential for a business to access critical IT systems and data.

SaaS Advantage: SaaS-based TMS providers that use leading cloud computing services typically include data backups as part of the subscription. This is one of several reasons why trucking and logistics companies of all sizes who have data centers are moving enterprise applications to the cloud.

Magnus Technologies, provider of a SaaS-based enterprise TMS for trucking and logistics companies, has an agreement with a leading cloud computing services provider to back up customer data in 5-minute increments. If necessary, in the event of a natural disaster or other disruption, Magnus will immediately switch a customer to a different computing environment with full data recovery.

"We do all of that seamlessly and use best-of-breed technologies and practices to ensure minimal data loss risk," said Matt Cartwright, CEO of Magnus.

Client-Server Advantage: Companies may do a good job managing data backups and other tasks associated with maintaining on-premise servers. They may also feel confident in their ability to restore service quickly with their own resources, but these activities also cost more than using cloud services that operate at scale. Also, on-premise servers will not be available for remote access by workers if the local internet service is down or service is slow.

Conclusion

The client-server model requires trucking and logistics companies to make ongoing investments in data security and business continuity. The complexity of knowing where to make investments and manage new technologies is rapidly increasing.

With a SaaS model, companies of all sizes gain the data security advantages of enterprise SaaS-based TMS and cloud computing services at enormous scale and levels of sophistication.

The same cloud services infrastructure that meets the needs of the largest, most security-sensitive businesses, also supports transportation companies with a resilient, high-security TMS that requires zero capital outlay and overhead.

> *The complexity of knowing where to make investments and manage new technologies is rapidly increasing.*

About Magnus Technology Group

Magnus Technology Group, headquartered in Austin Texas, has 20 years of experience designing, developing, and delivering enterprise TMS software. Magnus is the first software provider in the transport and logistics industry to offer an enterprise SaaS-based TMS that is affordable and scalable to fleets of all sizes.

The Magnus TMS platform is modular and works seamlessly with the Magnus Driver App and Magnus Carrier Advantage network to deliver a complete, end-to-end mobile dispatch and order fulfillment solution for truckload and LTL fleets to maximize profitability and growth.

To learn more visit www.magnustech.com

8601 Ranch Road 2222
Building 1 Suite 100
Austin, TX 78730

(877) 381-4632

MAGNUS™
TECHNOLOGIES