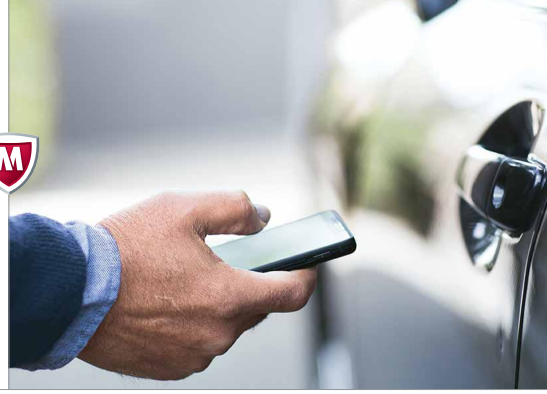
Case Study

United Automotive Electronic Systems Co., Ltd Relies on Intel Security for Comprehensive Security



UAES

Customer profile
Joint venture of the United Automobile Electronics Co. of China and Robert Bosch GmbH of Germany

Industry
Automotive

IT environment
3,000 computer terminals

Challenges
A Complex Security Landscape
UAES IT technical staff was lacking a unified view

McAfee solution
- McAfee Data Loss Prevention
- McAfee Endpoint Protection Suite
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator software
- McAfee Network Security Platform

Results
- Strengthened compliance with internal policies
- Extensible compliance reporting
- Protects over 3,000 endpoints from email, web, and application-generated attacks

United Automotive Electronic Systems Co., Ltd Relies on Intel Security for Comprehensive Security

United Automotive Electronic Systems Co., Ltd (UAES for short) was founded in 1995. Located in China, it is the joint venture of the United Automobile Electronics Co. of China and Robert Bosch GmbH of Germany. The company is headquartered in Pudong New Area in Shanghai. The production locations are in Shanghai, Wuxi, Xi'an, Wuhu, and Liuzhou. The technical centers of the company are located in Shanghai, Chongqing, and Wuhu. UAES has effectively integrated local research and development with the leading technology around the globe in order to provide quality products and services for domestic automobile manufacturers in China, and in order to provide technical support to meet the increasingly stringent regulatory requirements.

With its strong local research and development capacity and production capacity, United Automotive Electronic Systems Co., Ltd is committed to providing customers with advanced and complete automotive power train and vehicle control system solutions, and it is also dedicated to making contributions to actively reduce fuel consumption, CO_2 emissions and protecting the environment.

A Complex Security Landscape

Since the business of UAES is related to the front-end development of different systems, UAES has a high demand for information security. Its information security environment has changed over time, becoming more and more complex. Consequently, information security definitions and requirements have greatly varied at different times.

In the beginning UAES dealt with security by preventing and killing viruses. As the security risks of the enterprise have gradually transitioned from virus attacks to sensitive information leaks and other dimensions of data, UAES has started extending security control to data loss prevention and other areas.

According to the UAES head of security, there has never been an information or data loss prevention software / hardware in the company. "Basically (for information and data loss prevention) we rely on management processes, human-based surveillance, and continuous enhancement of security education among our employees." The head of security states that UAES initially set simple restrictions on employees' operational behavior at the office, such as forbidding the installation of unauthorized software, requiring the use of company-owned mobile storage devices to transfer files, requiring that outgoing documents obtain the necessary management approval before being sent, setting permissions for different roles to restrict employees' access to files, etc. These methods were limited to regulation levels, and the implementation of these regulations was reliant on management processes and the control of employee awareness and conduct. Therefore it was inevitable that there could be the potential of a data loss which was a huge risk to the company.

"The following situations could easily occur without data loss protection: an employee could send an email that includes sensitive data attachments, but due to carelessness, he or she types in a wrong recipient, thus resulting in the leakage of sensitive data; there may be a few employees who would use their own USB drive to copy extremely sensitive business data, such as classified technology documents or the company's financial statements; there may also be cases in which an individual employee unintentionally shares to the public network data that he or she did not realize that the data was confidential," he said.

And now the information environment of United Automotive Electronic Systems Co., Ltd is much more complex. This is because behavior on the

Internet is more complex. Getting the whole picture of security incidents and malware threats throughout the environment was a challenge.

For most businesses, collecting, correlating and prioritizing log events is extremely time consuming. This requires the technicians of United Automotive Electronic Systems Co., Ltd to monitor the security status of all systems, including mobile devices and personally-owned devices that have access to its network, and to prioritize these threats and take necessary action in a timely manner.

For example, during the process of information management, UAES IT technical staff was lacking a unified view, which means when at risk, they are only able to view and analyze the daily logs of different devices, from the daily logs of firewalls, switches, software systems and AD domains, to the daily logs of other related anti-virus software, etc., hoping to figure out what triggered the security threat by studying these daily logs.

But in practice, this kind of method takes a lot of time, and also demands that analyst personnel have technical expertise in all areas. Because of this, it can be impossible for the IT department, with its very limited staff, to quickly detect security vulnerabilities, and prioritize and resolve threats.

With respect to these security issues, United Automotive Electronic Systems Co., Ltd required an effective overall security solution to provide optimal protection from virus and security data leaks for rapid threat detection in today's big data environment. At the same time, this system must also be easy to work with from deployment to later operation and maintenance.

After careful consideration, United Automotive Electronic Systems Co., Ltd has chosen a complete set of solutions provided by Intel Security, including major solutions in anti-virus, data security, network security, and risk-detection in the big data environment; it has applied centralized control management through the McAfee ePolicy Orchestrator (ePO) management platform with simplified deployment operations, avoiding the fragmented nature of various security products.

Protection From Threats and Data Loss and Risk Detection in Big Data

As the flagship product of desktop terminals of Intel Security, Endpoint Protection Suite solutions show great performance in the anti-virus protection area.

For example, concerning real-time malware and virus protection, the program can help more than 3,000 internal PC terminals that are currently owned by United Automotive Electronic Systems Co., Ltd to quickly and effectively block viruses, Trojans, worms, adware, spyware, and other harmful programs that may cause potential confidential data theft and unwanted impacts on efficiency.

In addition, the program also helps United Automotive Electronic Systems Co., Ltd to protect email and web security, prevent malware and spam from entering employee inboxes, send warnings to employees before they click on malicious sites, and enable IT staff to flexibly allow or block the site, thus effectively ensuring compliance with the regulations.

The program can also monitor and restrict the use of removable storage devices, such as USB drives, to replicate data, thus preventing the company from losing control of the data.

Out of all of these, the unique ePO platform of Intel Security is the most impressive for UAES customers. The platform is a centralized, intelligent platform, which enables centralized control of Intel Security products. For example, using ePO platforms, United Automotive Electronic Systems Co., Ltd can perform easy installation and deployment of anti-virus software and virus database upgrades, fast and accurate positioning and killing of viruses, etc., on more than 3,000 computer terminals of all researchers, which can significantly free up the valuable time of our IT staff; at the same time, using ePO platforms, United Automotive Electronic Systems Co., Ltd can also develop USB drive usage policies on all computer terminals and record detailed information of all USB drive data copy events, such as the time of the replication, on which computer the data were copied, which data were copied, etc.

To meet the requirements for data loss prevention of United Automotive Electronic Systems Co., Ltd, Intel Security has provided a powerful data loss prevention product for both the host and the network, thus greatly reducing the possibility of sensitive data leakage.

On what grounds do we say that McAfee Data Loss Prevention (DLP) is powerful? Generally speaking, this professional data leakage prevention program can intelligently monitor, analyze, optimize, and prevent all actions concerning data on all the terminals. Picture this: No matter if it is research and development personnel or a business person of United Automotive Electronic Systems Co., Ltd sending an email with confidential content through a terminal or on the Web, or unintentionally posting an article containing sensitive content in a forum, or disclosing sensitive data in his or her personal microblogging, or using peripheral mobile devices to copy confidential data from the PC terminals of the company, the HDLP system will monitor and analyze the data before it leaves.

Once the data loss prevention system detects outgoing data that includes confidential data, such as research and development data and design related to different systems of automobiles, or other sensitive business data, the DLP system will automatically stop the action immediately to ensure information security.

At the same time, the UAES security administrator can also receive statistics on all behaviors regarding sensitive data transmission with the help of the DLP, allowing a clear understanding of other more detailed statistics, such as who sent out the sensitive data, as well as the time of each transmission, the quantity of the data sent out, etc.

Intel Security has also included an intrusion prevention system (IPS), which provides an application layer security protection, pre-admission and post-admission control, identity-based access control and host quarantine and mandatory access control. The performance of the McAfee Network Security Platform will not be affected if it provides comprehensive network and application security. The bandwidth of a single device can reach more than 10Gbps, which the other products cannot compete with.

In the current environment, the network environment that United Automotive Electronic Systems Co., Ltd is faced with is more complex. To help our customers achieve rapid threat detection, Intel Security offers a SIEM solution.

First of all, this solution can provide actionable security intelligence and a timely understanding of the big picture of security risks by collecting and analyzing relevant events, user information, system information, data, and risks, and countermeasure information in specific situations. Such a thorough understanding of the security situation can link the various security points to locate attacks quickly. It helps reduce response time and can provide automated responses to prioritized threats.

To put it simply, after the deployment of McAfee Enterprise Security Manager (SIEM), UAES can collect all of the logs (from the hardware level, the software level, the system level, etc.) and then prioritize these logs under the rules of association in order to spot any risks quickly.

For example, we consider there to be information security risk according to association rules when SIEM is analyzing various logs and finds that there have been five consecutive logins in the system on a certain terminal, and that in other logs, there are malicious hacking behaviors as well as different behaviors of the query into terminal network accounts, etc.

“But in the past, if a customer information security incident occurred, our security technicians had to go to different places to view the logs to try to determine where the problems had possibly originated, which is very inconvenient,” the head of company security at United Automotive Electronic Systems Co., Ltd said.

And now with SIEM they can quickly analyze logs and events. What UAES finds even more helpful is that SIEM has about 190 kinds of association rules already built into hardware, making it easy for users to operate and use.

SIEM has provided United Automotive Electronic Systems Co., Ltd with many more security advantages. Like other products of Intel Security, the SIEM can also be integrated with ePO, optimizing threat tracking and risk assessment.

"Compared to other SIEM solutions, McAfee Enterprise Security Manager is simple to deploy, is ready to use out of the box, has very powerful functions, and is obviously effective," the head of company security said.

Of course, SIEM can provide reports in different formats, providing hundreds of reports out of the box. Whether it is for an engineer or for the CIO of United Automotive Electronic Systems Co., Ltd, the solution can automatically generate different reports with customized content.

A Centralized and Schematized Vision of the Future

From the anti-virus function to data loss prevention system, from email security to the quick response of security in the big data environment, the range of solutions and services that Intel Security has provided for United Automotive Electronic Systems Co., Ltd has deeply impressed the UAES team. The UAES head of company security said: "The featured platform of Intel Security impressed us the most. On the McAfee ePolicy Orchestrator (ePO) platform, we can rapidly deploy Intel Security solutions for different security areas and maintain the system in a very simple way with this solution, which has many powerful functions. The solution can address all our past, present and future security needs."

As far as the company's future security development is concerned, UAES plans to take it in a centralized and schematized direction. It will no longer use the security management method other companies rely on, which is the scattered result of unconnected security solutions. Our plans for the future of security management incidentally match the product features of Intel Security. The platform is the most outstanding feature of Intel Security, as it enables security products from different directions to integrate and connect in the core ePO platform, thus presenting a more powerful and more intelligent security solution for its customers.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com