



Toyota Motor Europe Secures Massive LAN/WAN Using TippingPoint Intrusion Prevention Systems

The Challenge: When choosing winning business and security strategies, smart companies look to emulate Toyota Motor Corporation (www.toyota.com), a top-ten Fortune Global 500 company with 264,000 employees and annual sales of \$153.3 billion. The automaker's philosophy of lean, "just-in-time" production methodology, also known as the Toyota Production System (TPS), is widely recognized as the gold standard of manufacturing. Fittingly, TPS's supply chain management (SCM) requires a world class IT infrastructure that is fast, reliable, and, most of all, safe from a growing array of cyber threats.

At Toyota's European headquarters in Brussels, top IT security experts continuously strategize on how to combat threats to the company's Gigabit Ethernet LAN and its hub-and-spoke wide area network (WAN), which encompasses 25 national distributors and 40 manufacturing, parts and logistics centers, plus suppliers in 30 countries. Each Toyota site has secure connections to adjacent networks at one or more of 2,784 sales outlets.

Because Toyota Europe's plants operate 24/7 and request parts and materials from suppliers only when needed, the automaker must ensure that its WAN is always available. This level of security also must extend to Toyota's Brussels LAN, where the company hosts its enterprise applications, including Oracle Financial and Enterprise Resource Planning (ERP) software. "We set the performance bar very high," said Richard Cross, information security officer, Toyota Europe. "We simply cannot tolerate a single network outage due to a Denial of Service (DoS) flood or other cyber attack." Toyota Europe was already deploying security measures, when

the team in Brussels saw an opportunity to bolster the company's preparedness. "Toyota believes in 'continuous improvement,'" explained Cross. "In that spirit, we wanted to create a total security event management system that would take our existing security infrastructure to the next level." As a result, Toyota Europe sought a proven intrusion prevention system (IPS). The solution had to be highly interoperable, and easy to manage, configure, and update, with robust reporting features for viewing, sorting, and reporting events. Moreover, the security solution could in no way compromise network performance.

Why TippingPoint

To find its solution, Cross and his fellow security officers at Toyota Europe researched security solutions from TippingPoint, Cisco, Symantec, McAfee and ISS. They eliminated the Cisco system because they found it costly and cumbersome to manage. After doing head-to-head concept testing between the TippingPoint IPS and ISS's Proventia system, Toyota Europe concluded that the TippingPoint IPS was "the best security appliance on the planet."

"The TippingPoint IPS is the best security solution I have come across. Its performance has been nothing short of amazing. The solution more than paid for itself within the first year."

Richard Cross
Information Security Officer
Toyota Europe

Toyota Europe found their conclusions confirmed by SC Magazine, which ranked the TippingPoint solution “the Best Security Solution 2005.”

“TippingPoint IPS systems are the smartest, most advanced security solutions available,” said Cross. “They’re the simplest to deploy and manage because they’re standards-based and can interoperate with all kinds of hardware. You can’t go wrong with TippingPoint.”

The_Benefits

Using the TippingPoint solution, Toyota Europe now has the pervasive security it needs to safeguard its SCM and other networked business systems from DOS attacks, worms, spyware, Trojans, and viruses, plus a host of other potentially devastating attacks that could put the brakes on the automaker’s European operations.

Toyota Europe found the TippingPoint security solution so effective in blocking malicious traffic it placed the IPS as a powerful sentinel at its headquarters’ Internet gateway. Regardless of the number of filters used or the volume of traffic, packet flows move through the IPS at wirespeed with an imperceptible latency of less than 215 microseconds. This ensures that Toyota Europe’s applications run optimally, while being transparently and automatically protected from threats.

In addition, the Digital Vaccine® real-time inoculation service of the TippingPoint IPS ensures that devices are always updated to thwart the latest threats and often protect in advance of attack. Toyota Europe receives new filters weekly or immediately when critical vulnerabilities emerge, guarding operating systems and other network components. Moreover, unlike other security appliances that require manual inspection and approval of filters and signatures, the Digital Vaccine service automatically updates Toyota Europe’s network with virtually no intervention by IT staff.

Toyota Europe installed the TippingPoint security solution in under an hour and recorded a rapid 60 percent drop in the level of disruptive activity entering the network. “As information security officer for a major enterprise, I deal constantly with security threats and their solutions,” said Cross. “The TippingPoint IPS is the best security solution I have come across. Its performance has been nothing short of amazing. The solution more than paid for itself within the first year.”

Cross is particularly pleased with the TippingPoint Security Management System (SMS), a hardened appliance that allows him to collect comprehensive, real-time reports and graphs on traffic statistics, blocked attacks, and information on network hosts and services. Because it can manage multiple TippingPoint devices, the SMS ensures scalability. By automatically distributing the Digital Vaccine filters, the SMS optimizes effectiveness and lowers the total cost of ownership. The TippingPoint IPS’s intuitive graphical user interface further increases the solution’s ease of management and decreases cost of ownership. Featuring comprehensive reporting for all security-related events, the security solution lets Toyota Europe monitor all security-related events and record baselines for network performance. What’s more, because the TippingPoint IPS monitors the traffic from Toyota Europe’s branch locations, the Brussels office can detect the presence of threats and vulnerabilities on adjacent networks, trace them back to their IP address, and eliminate the risks.

“Our Brussels network supports our entire European operation,” concluded Cross. “Network failure is not an option, and the TippingPoint IPS is a lynchpin in our security arsenal. In fact, our experience with the TippingPoint IPS has been so good we are actually rewriting our security standards to insist that all our sites incorporate it.”

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS

European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450

Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999