NEXT-GENERATION SECURITY FOR AUTOMOTIVE ENVIRONMENTS

The automotive industry is on the verge of major change. With the internet of things and Industry 4.0, more demand for vehicle connectivity and autonomy are intensifying competitive pressures. Upcoming innovations from tech and shared mobility are disrupting traditional business and revenue. New business models are rapidly monetizing data for sectors such as use-based vehicle insurance, telematic services providers, smart cities, etc. As the industry adds new capabilities and enters new market segments, it also faces challenges in the form of cybersecurity, ever-growing complexity and the cost of managing IT assets. With the explosion of capabilities of internet-connected cars, devices, data and the people who access them, cybersecurity is a higher priority than ever.

Automotive Security Challenges

- Safeguard valuable intellectual property (vehicle and engine design), financial data and information from cyberespionage, ransomware and other threats.
- Prevent cyberthreats from impacting IT or ICS/SCADA networks and causing downtime or failures. High availability, reliable productivity, maximum data security and usability, and powerful reporting are musts for running smooth operations.
- Control access to corporate systems and automotive assets.
- Support smart devices, mobility and automation without introducing risks.
- Protect data in any private, public or hybrid cloud, specialized cloud services (telematics, user-based insurance) or SaaS environment while ensuring these environments do not introduce threats into the network.
- Streamline security policies and scale across all operations, regardless of size, geographies, applications and complexity.
- Thwart ransomware, spear phishing and other modern threats.

Secure Modern Automotive Networks With a Platform Approach

Digital technologies enable the automotive industry to communicate effectively with suppliers, partners, service providers and the vehicle. Distributed data hubs are established for analytics processing near major global markets to ensure secure, quick access to real-time insights.

This helps streamline the flow of information, enable real-time decisions and enhance automotive experiences. With more people and partners accessing more data and networked devices, today's automotive industry needs a better, more efficient way to thwart new threats and maintain security.

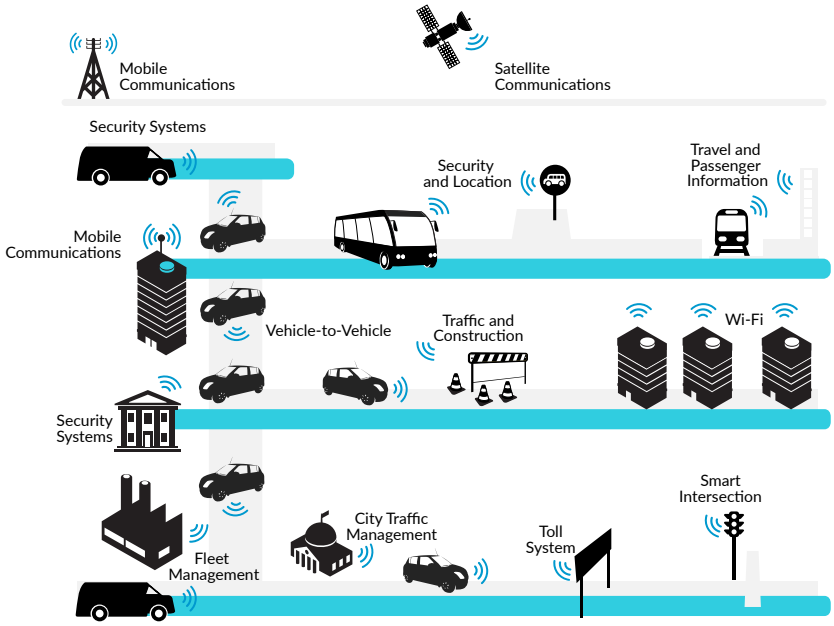

Figure 1: Connectivity systems for automotive environments

Elements of the Next-Generation Security Platform

These natively integrated elements share security context and work together to automatically prevent quickly changing threats from impacting your endpoints, networks or data. The platform approach reduces silos of information and manual intervention from overburdened IT and security teams.

- **Next-Generation Firewall**, in physical or virtual form, classifies all traffic – including encrypted traffic – and enforces policies based on applications, users and content without sacrificing performance.
- **WildFire™** cloud-based threat analysis service dynamically analyzes suspicious content in a virtual environment to discover zero-day threats.
- **Threat Prevention** includes IPS, malware protection, DNS sinkhole and command-and-control protection.
- **URL Filtering** continually updates with new phishing and malware sites, as well as sites associated with attacks, even blocking malicious links in emails.
- **Magna™** behavioral analytics detects suspicious anomalies in user and device behaviors, interrogates the source, and determines whether the initiating process is malware, allowing security analysts to swiftly shut down threats and prevent data breaches.
- **GlobalProtect™** network security for endpoints extends Palo Alto Networks platform protections to the mobile devices of employees, suppliers and third-party contractors.
- **Traps™** advanced endpoint protection eliminates the need for traditional antivirus and the constant updates they require.
- **AutoFocus™** contextual threat intelligence analysis service enables you to identify and prioritize important threats, understand their context, and view popular threats targeting your industry.
- **Aperture™** SaaS security service protects against known and unknown threats originating from SaaS environments, and provides detailed usage analytics and granular enforcement for all activity within sanctioned SaaS applications.
- **Panorama™** network security management, in physical or virtual form, reduces administrator workload and improves security posture with a single console to view, configure, create and distribute policies, as well as generate reports.

Palo Alto Networks® Next-Generation Security Platform helps manufacturers compete in the global marketplace and capitalize on new technologies without compromising security or uptime. The platform offers real-time visibility and cohesive, coordinated security across cloud, network, endpoint devices and content, reducing cyber risk.

The automotive industry around the world uses Palo Alto Networks to:

- Prevent new and known threats from impacting uptime with automated protections.
- Reduce risk and improve security posture with a Zero Trust security model.
- Streamline security operations and increase ROI.
- Safely enable IIoT, BYOD and other mobile use cases.
- Secure localized cloud services and SaaS applications close to where they are consumed over high-speed, low-latency connections for better performance and efficiency.
- Protect aging and vulnerable endpoints such as unpatchable servers.
- Secure traditional and virtualized data centers.

Prevent New and Known Threats From Impacting Uptime With Automated Protections

Palo Alto Networks offers coordinated and automated threat prevention, enabling you to embrace new technologies that improve your competitiveness while vastly reducing the operational burden on IT and security teams.

Our advanced malware analysis environment, WildFire, works with other platform elements to:

- Conduct dynamic analysis of suspicious content – even encrypted content – in a virtual environment to discover brand-new threats anywhere in the world.
- Trigger the creation of new protections, and automatically push them to the platform's IPS or URL Filtering capabilities in as few as five minutes.
- Continuously update security appliances with new phishing and malware sites, malicious links in emails, and command-and-control infrastructure, blocking any part of an attack.
- Block user credentials from being sent to unrecognized websites, foiling phishing attempts to steal usernames and passwords.

Palo Alto Networks Next-Generation Security Platform allows you to create and maintain a secure global automotive business. It enables the business to manage production facilities around the globe, with an empowered mobile workforce. The platform can identify threats to network security while simplifying the user and IT management experience. With Panorama, you can configure, manage and distribute security policies across the Palo Alto Networks platform and know that they will be applied to each branch office uniformly.

With Palo Alto Networks Next-Generation Security Platform, the industry eliminates ransomware while improving the effectiveness and efficiency of its entire security strategy. Now, you can identify and monitor activity globally at all sites, such as the top apps in use, the top threats, usage patterns, and more, all in one quick and simple view. The Palo Alto Networks platform provides preventive security and threat intelligence services for added protection against zero-day attacks. This can help you to meet the requirements of "SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" by:

- Enumerating all attack surfaces and conducting threat analysis.
- Reducing the attack surface.

[The] Zero Trust application- and user-centric security model allowed for specific, tightly defined exceptions to the overall segmentation architecture. This allowed specific users from one network to gain restricted access to another. With the Palo Alto Networks firewall, you can identify the exact application running on the network, all the way down to the Active Directory user identity. At the same time, you can define very specific and necessary exceptions for particular users and applications – without compromising the security posture of the system or requiring any network reengineering.

Reduce Risk With a Zero Trust Security Model

Simple-to-manage, yet granular network segmentation is key to preventing successful cyberattacks while serving the diverse needs of employees, subcontractors, the supply chain and other valid network users. Segment network zones based on asset sensitivity, and control which users and applications can access each segment, providing another level of access control to sensitive data or applications. The platform continuously scans for threats entering segments, reducing the risk of threats moving laterally through the network, while content scanning reduces the risk of data exfiltration.

- Protect valuable systems, such as IIoT/ICS/SCADA systems or servers containing sensitive information, in their own network segments.
- Create role-based permission policies based on users, groups and the functions of each, not just IP addresses.
- Prevent threats from spreading in the data center using east-west segmentation in virtualized public or private environments.

Streamline Security Operations

Integration, automation, speedy correlation and other tools in the platform dramatically reduce events per analyst hour, helping manufacturers build security teams or next-generation security operations centers that scale without adding more staff. Security staff can improve response times, focus on critical events, and spend time anticipating and foiling future attacks.

Reduce Total Cost of Ownership

Security capabilities that continuously communicate and update one another speed up new threat prevention while reducing cost and management overhead. Start with one capability and add new ones to the platform over time, growing protection levels without the cost and complexity of installing and managing new network devices. Consolidated visibility, policy creation, management, event logging, reporting and forensics across security capabilities simplify operations and compliance, reducing the potential for misconfigurations, outdated policies and overlooked threats.

Safely Enable Mobility and BYOD

Reduce risk and increase visibility in modern manufacturing environments, whether mobile devices are owned by your company or not.

- Secure Wi-Fi for employees' and contractors' mobile devices by leveraging platform integrations with leading network access solutions for the mobile enterprise. Factories and other locations can enjoy secure Wi-Fi environments that limit exposure to threats, while automotive companies can safely enable their networks.
- Add another layer of security and a secure VPN to mobile devices, and enforce acceptable use policies with GlobalProtect.
- Separate more open Wi-Fi access environments from zones that house critical infrastructure or valuable data with virtual network segmentation.

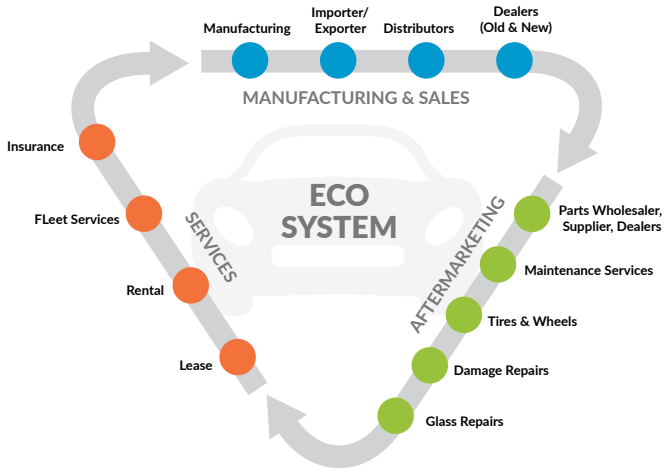

Figure 2: Automotive Ecosystem

Safely Enable Cloud Use and SaaS Applications

Extend the security of the on-premise network to public clouds. Palo Alto Networks VM-Series virtual firewalls provide the same capabilities for the cloud as our hardware appliances do for physical networks. Protect AWS® and Microsoft® Azure® environments from advanced threats while providing application-level control between workloads, policy consistency from the network to the cloud, fast deployment, and dynamic policy updates as workloads change.

SaaS applications are traditionally invisible to IT. Control which SaaS applications you allow with Aperture, and safely enable employee and partner activity within sanctioned applications.

Protect Aging and Vulnerable Endpoints

Some critical manufacturing processes depend on hardware running operating systems or browsers that are no longer supported. Traps eliminates the need for constant patching and prevents cyber breaches on vulnerable manufacturing assets by automatically identifying and stopping attempted exploits. By leveraging the latest insights from WildFire, Traps also prevents new threats from impacting endpoints, enabling you to adopt a mindset of prevention, instead of protection.

Secure Traditional and Virtualized Data Centers

Protect the data center perimeter, and prevent lateral movement and accidental data exposure, by segmenting the data center into several Zero Trust zones. Create policies for each network segment that define which users and applications have access, and block certain types of content from leaving the segment. Use the Next-Generation Security Platform to:

- Control and secure north-south traffic entering and exiting the data center.
- Control and secure east-west traffic entering and exiting VMs in the data center.

Getting Started

Start by gaining visibility into the users, applications and content in your network. Sign up for a free **Security Lifecycle Review**. This non-disruptive process will help discover unknown applications, threats, and bandwidth usage on your network and define top risks.

Palo Alto Networks is a **Gartner Magic Quadrant** Leader in the enterprise network firewall market for the fifth year in a row.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com