CYBERSECURITY FOR THE OIL AND GAS INDUSTRY

A Platform Approach

Forming the largest industry in the world, oil and gas companies are engines of the global economy – and huge targets for cyberattacks. With increasing amounts of data, internet-connected devices and automation, cybersecurity is a higher priority than ever.

Oil and Gas Security Challenges

- Safeguard valuable intellectual property while working efficiently with partners.
- Prevent cyberthreats from impacting OT networks and causing product, safety or environmental failures.
- Secure big data in the cloud.
- Enable secure and appropriate access to corporate systems and smart devices in the field without putting critical systems at risk.
- Protect aging, vulnerable or unpatchable servers.
- Secure geo-diverse environments efficiently.

Secure Modern Oil and Gas Networks With a Platform Approach

The internet enables oil and gas companies to communicate effectively with suppliers, partners and service providers. The industry is employing digital approaches and the industrial internet of things, or IIoT, to improve product quality and uptime, optimize asset use, reduce risks and costs, and allow the boardroom to act quickly on real-time production information. With increasing connectivity and data sharing, today's oil and gas industry needs innovative, more efficient ways to thwart new threats and maintain security.

Palo Alto Networks® Security Operating Platform helps the oil and gas industry maintain efficiency and capitalize on innovative, cost-saving technologies – such as cloud, IIoT and mobility – without compromising security or operations. The platform offers real-time visibility and cohesive security for cloud, network, endpoint devices and content, reducing cyber risk. Integration, automation, speedy correlation, and the identification and provisioning of context on important threats all work to dramatically reduce events per analyst hour. You can scale security teams or next-generation security operations centers without adding more staff, while your existing security staff can improve response times, focus on critical events, and spend time anticipating and foiling future attacks.

Oil and gas companies around the world use Palo Alto Networks to:

- Automatically prevent new and known threats from affecting operations.
- Reduce risk with virtual network segmentation and role-based network access.
- Reduce total cost of ownership.
- Secure ICS/SCADA networks.
- Safely enable BYOD and other mobile use cases.
- Secure cloud use and SaaS applications.
- Extend operational life by protecting aging or unpatchable servers/workstations.
- Secure traditional and virtualized data centers.
- Improve SecOps/SOC effectiveness.

Automatically Prevent New and Known Threats From Affecting Operations

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 threat analysis environment 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 sensors every five minutes.
- Continuously update security appliances with intelligence on new phishing and malware sites, malicious links in emails, and command-and-control infrastructure to block any part of an attack.
- Block user credentials from being sent to unrecognized websites, foiling phishing attempts to steal usernames and passwords.

Reduce Risk With the Zero Trust Security Model

Simple-to-manage yet granular network segmentation is key to preventing successful cyberattacks while serving the diverse needs of employees, business partners, the supply chain and other valid network users. Palo Alto Networks enables oil and gas companies to segment networks to reduce the risk of threats moving laterally through the network and provide another level of access control to sensitive data or applications. Using Palo Alto Networks next-generation firewalls, you can:

- Protect valuable systems, such as ICS/SCADA systems or servers containing sensitive information, in their own network segments, ensuring least-privileged access while continuously scanning for threats and data exfiltration.
- Create role-based permission policies by making use of user information from a wide range of repositories, enabling IT teams to identify users and groups, not just IP addresses.
- Grant or deny user access to network segments hosting certain functions, such as joint venture access to systems, for another layer of security beyond usernames and passwords.
- Use east-west segmentation in virtualized public or private environments to prevent threats from spreading in the data center.
- Identify and monitor all applications traversing the network, and create policies that block or allow certain applications from certain network segments.
- Give administrators valuable insight through near-real-time, easily understandable reports to help them prevent security incidents.

Reduce Total Cost of Ownership

Eliminating point products increases the speed and effectiveness of threat prevention while reducing cost and management overhead. You can 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. Each security capability automatically correlates insights on emerging threats across endpoints, data centers, SaaS and cloud resources, ensuring fast responses to any threat without manual intervention. As you add security capabilities, coordination increases, as does return on investment. Add to ROI by protecting aging or vulnerable endpoints that no longer receive product updates, extending their operational life.

Secure OT Networks

ICS/SCADA systems are transforming from a collection of isolated, proprietary devices to interconnected systems that leverage IP and commercial off-the-shelf products. Although integration and IIoT optimize operations and reduce costs, they also increase the risk of cyberthreats. Beyond comprehensive threat protection, Palo Alto Networks Security Operating Platform secures control system networks in several ways, allowing you to:

- Identify ICS/SCADA network traffic, such as Modbus, DNP3, and CIP EtherNet/IP; the users on the plant network; and how they use applications. You can easily validate if users are following network usage policies and respond quickly to stop any anomalous use.
- Reduce the risk of cyber incidents by creating network segments with Zero Trust. Enforce role-based access controls with the least privilege as described in the ISA/IEC 62443 standard, and ensure safe, appropriate access for corporate users, vendors and partners.
- Protect legacy or unpatched control system HMIs, servers or hosts from known and unknown cyberthreats by using customized security zones, advanced endpoint protection or both.
- Secure remote access to the ICS network for valid employees and third parties monitoring critical equipment and business processes by enforcing acceptable use policies and security posture through a secure VPN.

Safely Enable Mobility and BYOD

Reduce risk and increase visibility of the users accessing your network whether or not your company owns their mobile devices.

- Secure Wi-Fi for employees' and contractors' devices by leveraging platform integrations with leading network access products for the mobile enterprise. Oil and gas facilities can enjoy secure Wi-Fi environments that limit exposure to threats.
- Protect mobile devices, no matter where they travel, with a lightweight network security client that consistently enforces security policies. For staff who bring their own devices, the client works with Enterprise Mobility Management platforms to separate business apps, data and traffic from the personal apps on devices, securing business content while respecting privacy.
- Separate more open Wi-Fi access environments from zones that house critical infrastructure or valuable data with virtual network segmentation.

Safely Enable Cloud Use and SaaS Applications

Palo Alto Networks virtualized platform deployments bring the security of the on-premise network to public and private clouds. Prevent successful cyberattacks on Amazon® Web Services, Microsoft® Azure® and Google® Cloud Platform environments while providing application-level control between workloads, policy consistency from the network to the cloud, fast deployment and dynamic security policy updates as workloads change.

SaaS applications are traditionally invisible to IT. Palo Alto Networks solves this problem by providing full visibility into the day-to-day activities of employees using SaaS applications, such as Microsoft Office 365®, Salesforce®, Dropbox® and more. Granular security policies help eliminate data exposure and threat risks. For example, you can deny data uploads to personal Box folders while safely enabling collaboration through your organization's Box environment.

Protect Aging and Vulnerable Endpoints

Some oil and gas facilities still depend on hardware running operating systems that are no longer supported. Advanced endpoint protection eliminates the need for constant patching and prevents cyber breaches on vulnerable systems by automatically identifying and stopping attempted exploits. Making use of the latest insights from threat intelligence also prevents new threats from affecting servers, desktops and laptops.

> *"The level of information is much more detailed, making the interception of malware much simpler. It allows us to gain greater visibility over what files users are running and block them if need be.*
>
> – Victor Ciurus, group information security lead, KMG Rompetrol

Secure Traditional and Virtualized Data Centers

Protect the data center perimeter and prevent lateral movement as well as 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

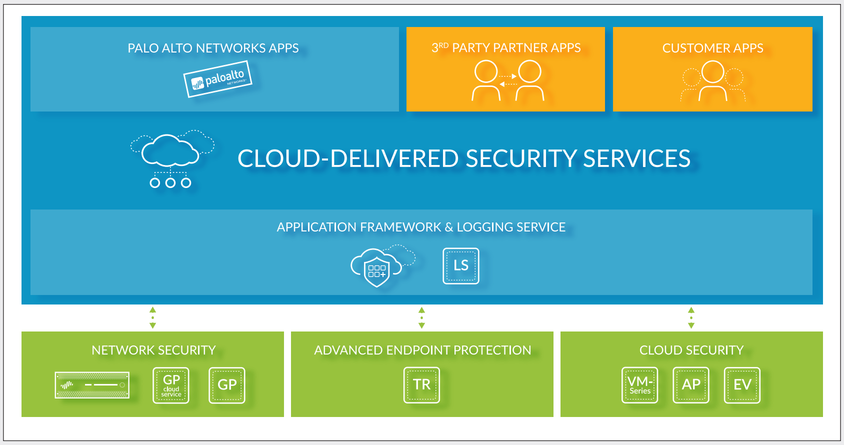

Figure 1: Palo Alto Networks Security Operating Platform

The Security Operating Platform

The Palo Alto Networks Security Operating Platform prevents successful cyberattacks through automation. It is easy to operate, with enforcement points and shared intelligence that work together at network speed to prevent ever-changing threats from affecting your operations or data. Accurate analytics allow you to streamline routine tasks and focus on business priorities. Tight integration across the platform and with ecosystem partners delivers consistent security across cloud, network, computers and mobile devices. Among the core elements:

- **Network security** employs next-generation firewalls to protect networked services ranging from branch offices of all sizes to perimeters, data centers and harsh environments. Integrated network security clients extend security policies and protections to employee computers and mobile devices in remote locations.
- **Advanced endpoint protection** safeguards servers, clients and mobile devices against the latest vulnerability exploits, ransomware and other malware delivered via any method, including email, UBS drives or other attached devices, and other channels.
- **Cloud security** provides the same protections as the network security components for private, public and hybrid cloud environments, as well as SaaS applications. Deep integration with native cloud services and automation tools speeds up multi-cloud deployments.
- **Cloud-delivered security services** employ global intelligence to filter content as well as detect threats and attackers. These services automatically create protections against new threats and attacks as well as continuously update endpoint, network and cloud sensors.

Palo Alto Networks has recently opened up the platform, enabling you to swiftly take advantage of security innovations that meet the unique needs of your industrial environment.

- **Application Framework** enables rapid development of custom and third-party applications that make use of data from the Logging Service and other cloud-delivered security services.
- **Logging Service** provides a secure, cloud-based repository for all application and appliance data logs, collecting data from various sources while eliminating the burden of scaling and maintaining on-premise compute and storage.

Palo Alto Networks apps include:

- **Behavioral analytics** that helps discover anomalous and malicious user or application activity inside the network.
- **Contextual threat intelligence service** for malware analytics and hunting tools for SOC teams.

For more information on the Palo Alto Networks Security Operating Platform, please visit **https://www.paloaltonetworks.com/products/security-operating-platform.**

access, and block certain types of content from leaving the segment. Use the Security Operating 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.

Improve SecOps/SOC Effectiveness

Every day brings thousands of new pieces of malware and targeted attacks, so identifying and providing context on important threats can dramatically reduce events per analyst hour.

With the Palo Alto Networks platform, your security teams can improve response times, focus on critical events and spend time anticipating and foiling future attacks without adding more staff. A contextual threat intelligence service accelerates analysis, correlation and prevention workflows by prioritizing threats and providing full context around them. It aggregates indicators of compromise from many threat intelligence sources so your security teams can take swift action, reducing manual labor and preventing threats from affecting operations.

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 define top risks due to usage, unknown applications, malware and more.

Customers in more than 150 countries and in every industry rely on us to improve their cybersecurity posture. For more information on Palo Alto Networks, please visit https://www.paloaltonetworks.com/company/about-us.

For more information on how we protect oil and gas industry networks worldwide, please visit https://www.paloaltonetworks.com/solutions/industries/enterprise/oil-gas.

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com