SCADA and Industrial Control Systems (ICS) Industry Solution Brief

CHALLENGES

Critical infrastructure operators face many challenges in securing SCADA/ICS Networks

- Improving visibility to network traffic, usage and associated risks
- Protecting unpatchable critical assets from sophisticated threats
- Safely allowing external access and usage of networked applications
- Reducing incident response time and complexity

SOLUTION

Our next-generation security platform protects SCADA/ICS networks via

- Deep packet inspection technology that provides intuitive and actionable intelligence about network traffic
- Granular control over applications, users, content, and web traffic
- Native threat prevention against both known and unknown threats
- Centralized management that expedites forensics and remediation

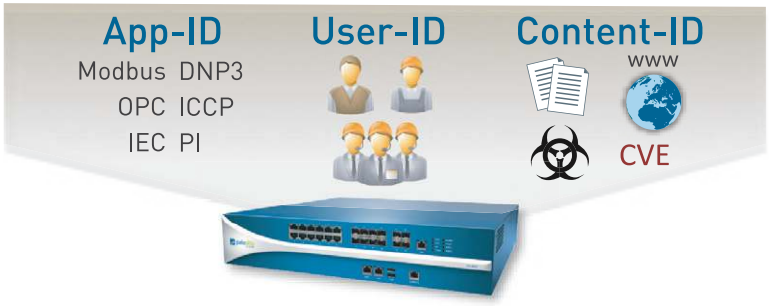
BENEFITS

The benefits that come with our network security platform include

- Increased situational awareness that promotes faster incident response and security policy improvement
- Least privilege access model reduces the attack footprint and promotes safe IT-OT integration and use of web/SaaS
- Tightly coupled threat protection that deters modern malware and APTs across their entire attack lifecycle

NEXT-GENERATION SECURITY THAT PROTECTS CRITICAL ASSETS, ENABLES SAFE MODERNIZATION AND KEEPS UPTIME HIGH

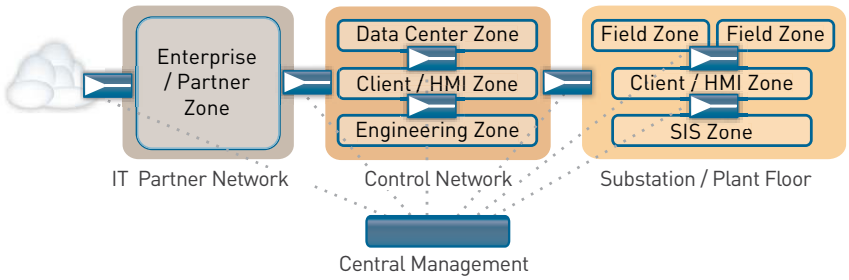
Palo Alto Networks® next-generation security platform can be used to protect SCADA and ICS networks in a range of critical infrastructure industries including Energy, Water Utilities, Transportation and Manufacturing. At the heart of this platform is an advanced classification engine which includes App-ID, User-ID and Content-ID. This engine provides the improved traffic visibility and control as well as the native support for threat prevention, web security, and mobile security which legacy, stateful-inspection firewalls cannot provide.



Palo Alto Networks Next-Generation Security Platform

- **App-ID** identifies all applications on all ports all the time (vs. port/protocol)
- **User-ID** identifies users or user groups (vs. IP address)
- **Content-ID** scans the content for data/files, threats, URLs

Deploy our platform across your control centers, remote stations and enterprise for a unified architecture that simultaneously protects critical assets from threats while enforcing a segmented and more intuitive least privilege access model based on users, applications, and content.



End-to-End Next-Generation Security with Central Management

paloalto NETWORKS®

- Secure the use and administration of data center servers in the PCN
- Safely integrate enterprise and 3rd party support networks
- Limit substation/plant traffic to control protocols and approved applications
- Enable safe web access and use of SaaS applications
- Natively protect against exploits, viruses, and spyware on a sitewide basis

APPLICATION SIGNATURES FOR SCADA AND ICS

Backing up our capability to control applications is a large, searchable database of application signatures for general IT as well as SCADA and ICS protocols and applications.

■ Modbus	■ OPC
■ DNP3	■ OSIsoft PI
■ Ethernet IP	■ Cygnet
■ IEC 60870-5-104	■ FactoryLink
■ Synchrophasor	■ ICCP

Sample Application Signatures for SCADA/ICS

In addition to having a base application signature, specific protocols such as Modbus and IEC 60870-5-104 have function control capabilities which allow monitoring and control of sub-functions such as reads and writes.

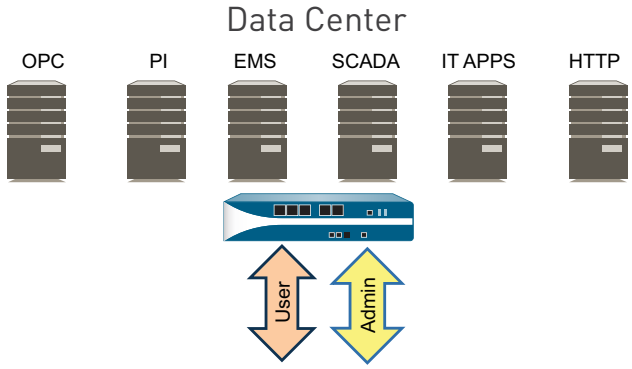
Modbus Function Control Signatures
Modbus-base
Modbus-write-multiple
Modbus-write-file-record
Modbus-read-write-register
Modbus-read-write-single coil
Modbus-read-single-register
Modbus-read-multiple-registers
Modbus-read-input-registers
Modbus-encapsulated-transport
Modbus-read-coils
Modbus-read-discrete-inputs
Modbus-mask-write-registers
Modbus-read-fifo-queue
Modbus-read-file-record
Modbus-read-holding-register

Modbus Function Control Example

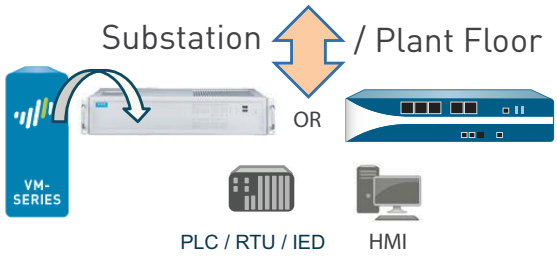
Any application which currently does not have a signature in our database can be addressed by our engineering team. Alternatively, we provide customers the ability to create custom signatures.

IMPLEMENT LEAST PRIVILEGE NETWORK ACCESS MODEL

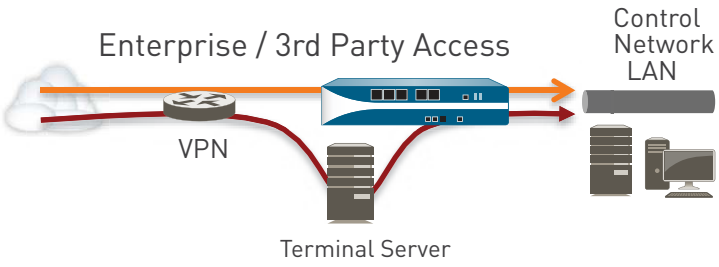
Apply segmentation best practices described in standards such as ISA-99 and IEC 62443 to define security zones. Then implement our next-generation security platform as a powerful conduit to employ a fine-grain, least privilege network access control model. Some example use cases include the following.



- Allow usage of approved applications in the data center
- Control users, content and apply QoS for specific applications
- Restrict usage of administrative applications to authorized data center administrators (SSH, Telnet, SNMP, FTP, etc.)
- Control access to URLs and SaaS based applications



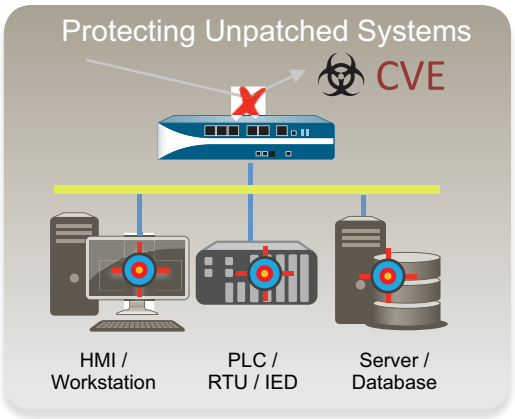
- Use standard appliance for controlled environments or ruggedized server plus VM-series virtualized appliance for harsh environment
- Limit traffic to control network protocols and limited set of approved applications/protocols for administration/alarms
- Track all command-related packets by user to help with event correlation



- Allow access from enterprise for select users and applications, e.g. historian access for finance analyst
- Monitor and control third-party VPN and terminal server access
- Implement time of day policies along with application and user identification to limit exposure
- Consistently enforce next-generation firewall rules on mobile devices via our GlobalProtect™ offering

IMPLEMENT A LIFECYCLE APPROACH TO THREAT PREVENTION

Modern cyberattacks and APTs rely on stealth, persistence, and the skilled avoidance of traditional security throughout the lifecycle of the attack. Palo Alto Networks offers an end-to-end approach to these threats that leverages the unique visibility of our next-generation firewall, combined with a cloud-based malware analysis environment in which new and unknown malware can run and conclusively be identified.



Threat Signatures for SCADA/ICS Specific Vulnerabilities

In addition to antivirus and antispyware signatures, our threat database includes signatures for exploits such as

- Vendor-specific exploits for HMIs, SCADA masters, historians, and other application software
- Protocol specific exploits for Modbus, DNP3, and ICCP
- General IT applications and operating systems

Employ these signatures to protect unpatchable systems from exploit and reduce downtime associated with security incidents.

Our world-class threat research team tracks vulnerability alerts from multiple public and private organizations to ensure thorough and timely coverage.

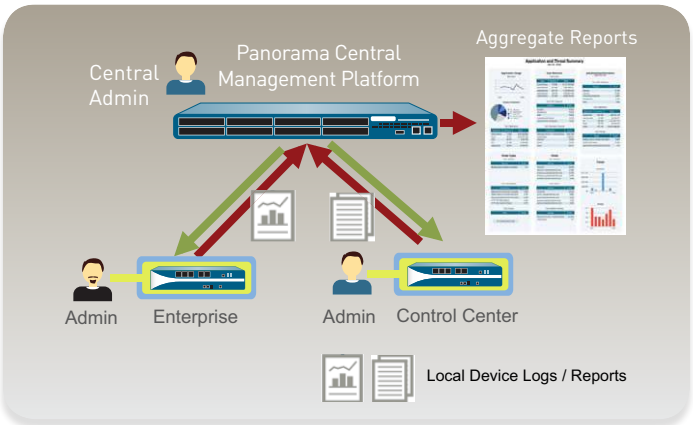
Wildfire: Protection Against Unknown Malware

Attacks against critical infrastructure have become increasingly sophisticated and exploit zero day vulnerabilities. To help combat so called "Son of Stuxnet" attacks, organizations can leverage Palo Alto Networks WildFire™ infrastructure hosted in the public cloud, enabling any Palo Alto Networks firewall to add the ability to detect and block unknown malware. However, if you prefer not to use public cloud services, the WF-500 provides the ability to deploy WildFire as a private cloud on your own network.

CENTRAL MANAGEMENT AND REPORTING

Security installations in SCADA and ICS are often highly distributed with policies that are very different from traditional IT policies. Panorama central management platform makes management and intelligence gathering easier by

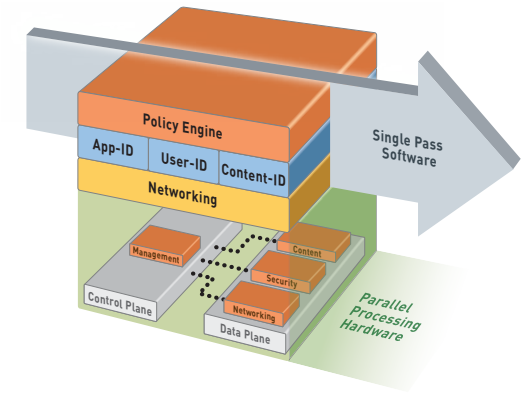
- Enabling centralized deployment of distinct IT/OT policies and configurations on geographically dispersed firewalls
- Supporting role based administration for added security
- Providing powerful centralized reports which facilitate forensics and regulatory compliance to standards such as NERC CIP and CFATS
- We also partner with many of the key SIEM vendors to ensure seamless integration and the ability to make use of the new level of visibility that our platform provides.



ARCHITECTURE BUILT FOR PERFORMANCE AND UPTIME

Implementing security in control networks must not adversely impact availability or performance. Our security platform was designed from the ground up to address next-generation security requirements while delivering performance and availability.

- Single-pass, parallel processing architecture (SP3) performs classification functions in a single pass for each packet
- Separate control plane and data plane ensures that intensive management processes don't impact data flow
- Function-specific parallel processing hardware engines deliver optimal performance
- Support for high-availability/redundancy schemes and QoS

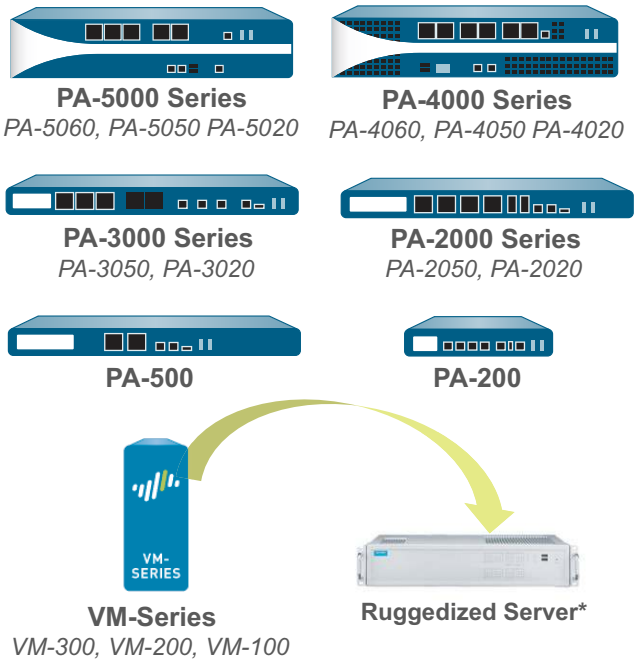


A BROAD PORTFOLIO OF APPLIANCES THAT ADDRESS A RANGE OF USE CASES AND ENVIRONMENTS

Palo Alto Networks offers a full line of purpose-built hardware appliances that range from the small PA-200 for segmentation of smaller security zones to the largest PA-5060, which is designed for high-speed datacenters. The same firewall functionality that is delivered in the hardware platforms is also available in the VM-Series virtual firewall which can be implemented in ruggedized servers for use in harsh environments like substations.

WANT TO KNOW WHICH APPLICATIONS AND THREATS ARE ON YOUR SCADA OR ICS NETWORK?

Palo Alto Networks can show you exactly what your firewall has been missing with the Application Visibility and Risk Report (AVR Report). The AVR Report provides a business risk assessment based on the analysis of the application traffic traversing the network, taking into account the different types of applications, how they are being used and the relative security risk. By looking at the associated risks along with how the applications are being used, administrators can make more informed decisions on how to treat the applications via a security policy.



* Servers compliant ot IEC 61850, IEEE 1613, Class 1 Div 2 standards are available from third party partners.

Generating an Application Visibility and Risk Report involves deploying a Palo Alto Networks next-generation firewall within the network where it monitors the application traffic traversing the Internet gateway. At the end of the data collection period, an AVR Report is generated that provides an analysis of the application traffic, the overall security risk rating, and the related business risk. The report closes with a detailed look at how effective the existing technologies are at supporting and enforcing the customer application usage control policies.

Contact your local Palo Alto Networks representative today to learn how your organization can receive a complimentary AVR Report.

paloalto NETWORKS®
the enterprise security company™

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