INDUSTRIAL CONTROL SYSTEMS

Targeted attacks against national, critical infrastructure are serious threats that must be addressed with the highest priority, given how these systems are responsible for controlling water, gas, electricity, transportation and numerous other key systems that contribute to our daily lives. The fact that bringing any one of them down has the potential to bring common, daily activities to a complete stop is unnerving. In the quest to move forward into the cyber age, operators of these once air-gapped, serial systems deployed commercial off-the-shelf products to bring them into the Internet Protocol era. Although these products provide the desired connectivity, they have also made these systems vulnerable to the same threats enterprise networks face.

I. EXECUTIVE SUMMARY

The Security Reference Blueprint for Industrial Control Systems enables operators to reduce operational risk, prevent system breaches, and become compliant with both government and internal governance while leveraging existing infrastructure, maximizing ROI on existing equipment using the Palo Alto Networks Security Operating Platform, with next-generation firewalls deployed in strategic locations.

II. SECURITY CONCERNS FOR INDUSTRIAL CONTROL SYSTEMS OPERATORS

With the rapid expansion of the internet, companies today look to find a competitive edge in the ever-changing marketplace by gathering and ingesting reliable, quickly obtained data from both interior and exterior sources. The operators of ICS have been pressed to keep pace with this ever-evolving trend or risk losing market share. The need for reliable and fast access to data representing what's happening in one's own system, as well as the competitive market, can mean the difference in record profit margins or bankruptcy. Now that these serial networks have been modified to operate in IP networks through the use of commercial off-the-shelf, or COTS, products, most of which do not provide any additional security, these once serial, air-gapped systems face the same advanced persistent threats, malware and insider threats as their enterprise counterparts' systems. These day-to-day threats are of concern to the enterprise IT, but even more so to the operational technology systems, because unlike enterprise systems, OT systems cannot be easily updated and retooled to address the constantly changing threat landscape.

Designed to control physical processes with as close to 100 percent uptime as possible, these systems are difficult and costly to take offline due to the impact they could have on production and surrounding environments. Due to the functional requirements placed upon these systems, the equipment refresh cycle is greatly extended. It is not uncommon to find one that has been operating for close to 25 years on the original hardware and operating system.

At the time of deployment for these older systems, little or no consideration was given to security, let alone best practices. With a refresh cycle often four times longer than those of enterprise systems, little is often done that will disrupt production, such as the upgrading of system/network security. Practices adamantly endorsed and enforced on today's network-connected systems were of no concern when these systems were first deployed, due to the air-gapped nature of the control systems network. Two-factor authentication, complex password enforcement and network segmentation were not given consideration because most didn't believe these systems would be accessed in the manner they are now. The information boom and the need for up-to-date information in terms of nanoseconds have caused a mad dash to integrate these systems into the enterprise network. Systems that do not have the processing power or hardware to keep pace with the cyber age are operating on today's internet through the use of COTS systems that provide connectivity with little or no security, leaving the systems exposed to modern-day threats.

An effective security strategy that incorporates key security principles can address the types of exposures and damage cited above as well as reduce operational network inefficiencies caused by unauthorized applications or misuse of network resources. This paper discusses how Palo Alto Networks Security Operating Platform enables operators of industrial control and SCADA systems to implement these principles to detect and prevent threats to the controls network as well as improve their network deficiencies while reducing complexity and unnecessary overhead.

III. REFERENCE BLUEPRINT GOALS AND SECURITY PRINCIPLES

Described in this reference blueprint for ICS is a framework using the preventive capabilities of the Palo Alto Networks Security Operating Platform and various models of next-generation firewalls. Using this blueprint will enable IT and OT professionals to maintain or improve facility operations while maintaining the availability of the plant network and protecting plant processes. It can also help with ways to:

- Block threats associated with vulnerabilities connected to end-of-life operating systems and legacy hardware.
- Protect production networks from critical downtime and service interruptions.
- Prevent data breaches and the loss of sensitive, proprietary product information, procedures and recipes.
- Highlight key network infrastructure assets that require extra scrutiny to preserve security and prevent data leakage or physical damage.
- Identify network security deployment and manage best practices.
- Comply with relevant regulatory requirements as well as the operators' internal governance, such as the NIST Cybersecurity Framework, NERC CIP and CFATS.
- Provide the look and feel of a single, homogeneous network while retaining heterogeneous network operations and dependencies.

Unlike most industries, security risk in a plant operation environment can affect the reputation and financial well-being of the company as well as the community at large. The impact of a breach can affect the living conditions and environment of the immediate surrounding area and beyond and, in worst-case scenarios, result in loss of life.

Like other industries, ICS/SCADA networks have also been affected by advanced attacks as well as less targeted but equally damaging malware infections from unwitting users. In addition to the security risk, operations personnel often waste

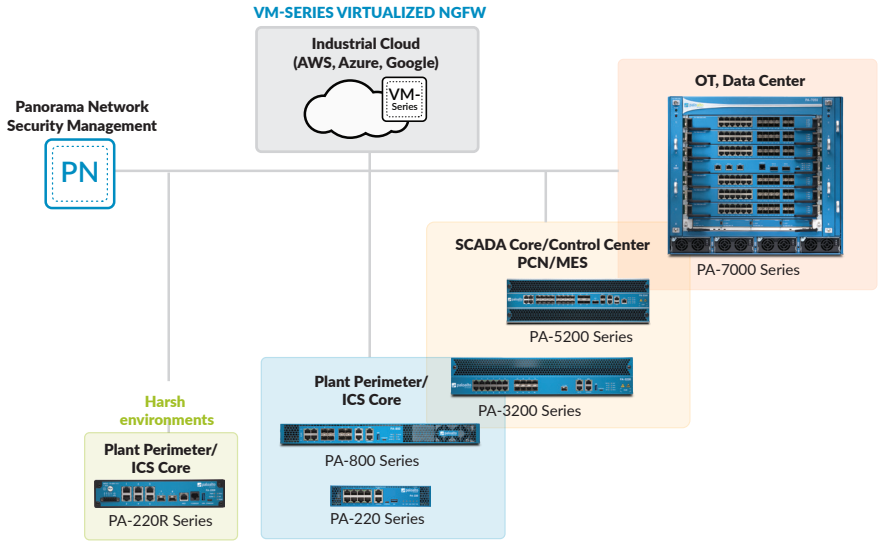

Figure 1: Consistent network security across your industrial enterprise

precious network resources on unauthorized or unnecessary applications. Although not directly related to security, these rogue applications present a risk to the operational networks that can be just as dangerous.

There are several types of threats that affect ICS/SCADA networks. Two of these affect any unprotected organization: opportunistic malware with no specific targeted victim and exploits for any instance of its targeted, vulnerable application. The third type of threat to production networks is targeted attacks. These three types of threats can be prevented with an approach that relies on next-generation security and some key security principles, including native threat prevention, to protect the company's intellectual property, control processes from interruption or downtime, and prevent unauthorized access and leakage. These core principles include:

- Complete visibility, effective control and enablement of ICS/SCADA applications.[1]
- Virtual segmentation to prevent the movement of malware through the network using a Zero Trust approach.
- Protection of the automation network from endpoint to endpoint. The network needs to be the enforcement point.
- Technology capable of identifying advanced malware, both known and unknown, and preventing zero-day exploits.
- Timely reporting to enable IT/OT, cybersecurity and intelligence professionals to coordinate actions.
- Immediate and automatic sharing and distribution of threat intelligence between systems.

The following sections address each of these principles in detail.

IV. CORE SECURITY PRINCIPLES

Policy-Based Application Visibility and the Use of "Positive Enforcement"

To effectively and efficiently protect control systems networks, security and network teams require clear visibility into whatever enters and leaves these networks. Visibility into the applications, as well as the individuals and/or teams using them, is paramount, especially since most protocols used in the controlling of these processes are considered to be at-risk.[2] Using an application-based firewall, IT/OT teams can develop contextual, policy-based decisions regarding which applications to block or allow for specific user communities or groups requiring access to the ICS network. This provides much more flexibility when needing to cater to the needs of specially designated network users or groups of users while drastically reducing the threats to the controls network.

To move to an application-based threat prevention model:

- Start by placing an application-based firewall in monitor-only mode, and begin the process of documenting all network traffic, paying close attention to the applications and protocols that currently traverse the controls network. For harsh environments, use either the PA-220R ruggedized next-generation firewall – specifically design for such applications – or a VM-Series virtualized next-generation firewall on a ruggedized server.[3]
- Once you've identified the applications and protocols necessary for production, develop a strategy to implement application-based firewall rules that align with the business and production objectives, and move to place the firewall in-line to enforce these policies.

1. These three activities alone help to reduce the attack surface and minimize needles bandwidth consumption.
2. Protocols inherently flawed by design, such as Modbus, which is unauthenticated and unencrypted.
3. For more information about Palo Alto Networks ruggedized hardware, please contact your sales representative or visit: https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-220r

- Once in place, iteratively lock down applications according to the approved strategy, and enforce consistent security policy rules for users and groups with similar access and application requirements.

Application-based policies can help control access in the following ways:

- Identify frequently used applications so you can more easily highlight unknown or potentially risky applications. You can first monitor traffic across your firewall to learn what's legitimate – or not – and put a traffic classification strategy into place.
- Identify risky applications, for instance:
  - Cloud-based file sharing sites, such as Dropbox® and Box
  - Data transfer and exfiltration
  - Suspicious DNS
  - Peer-to-peer
- Look for other dynamics within your environment, such as:
  - Port scanners and/or vulnerability scanners
  - Third-party networks that are not approved
  - Communications between sites and/or devices that normally have no reason to communicate
- Build groups for traffic to always block:
  - Applications such as Tor®, BitTorrent® and Dropbox.
  - Services provided by the enterprise that are not needed in the controls ecosystem.
  - IP ranges including geolocation – does your control system need to talk to IP addresses in China?
- Identify, monitor and analyze all encrypted traffic, especially from systems and sites external to the controls network ecosystem. Many applications and websites use encryption for privacy, but malware authors are increasingly delivering encrypted malware payloads. All encrypted network traffic should be examined for the presence of malware or inappropriate usage.

By implementing granular application identification, not just port-based filtering, operators of ICS networks are in a position to gain greater visibility and more precise control as well as reduce their risks significantly.

Virtual Segmentation With Zero Trust

The largest threats to the ICS environment may originate from the adjacent business network. As an example, a targeted attack against a Ukrainian operator of ICS/SCADA systems for the electric power industry in December 2015 left 1.4 million customers without service for several hours.[4] Attackers used spear phishing and social engineering techniques to deliver a Microsoft Word document with malicious VBA macros to drop the BlackEnergy malware, Kasidet backdoor and Dridex

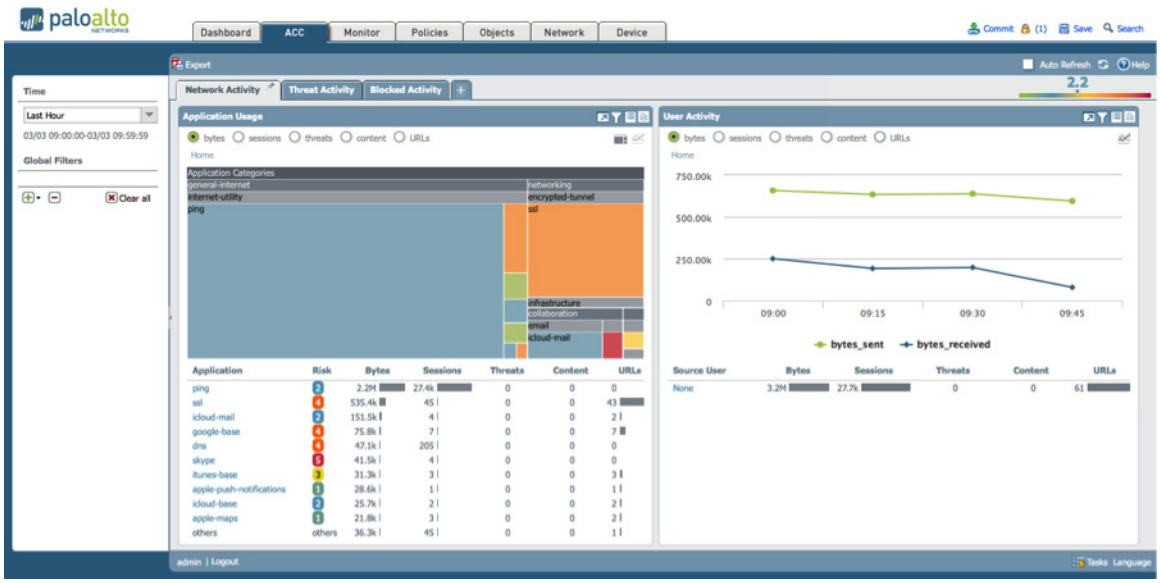

Figure 2: Palo Alto Networks Application Command Center

4. Lipovsky, Robert, and Anton Cherepanov. "BlackEnergy trojan strikes again: Ukrainian electric power industry." Welivesecurity.com. January 4, 2016. https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

banking Trojan. The attackers were able to penetrate their target network as well as successfully establish a beachhead and remain undetected for a significant period of time while continuing evasive and damaging actions. As this attack shows, the impact to an ICS/SCADA system can be far-reaching with devastating effects.

The Zero Trust approach, first outlined by Forrester, makes it very difficult for such an adversary to succeed. This same approach makes it hard for everyday malware to move across the network. Based upon verification of all users, devices and applications traversing your network, establishing Zero Trust boundaries[5] effectively compartmentalizes your user groups, devices and/or data types, such as PLC and Modbus data.

There are four major benefits to segmenting your ICS/SCADA ecosystem into discrete zones with a next-generation firewall:

- **Limit the attack surface area.** Segmentation protects sensitive parts of your network, such as vulnerable PLC/RTU, older end-of-life servers and workstations that cannot be patched.
- **Limit pivoting and exfiltration.** Segmentation limits both the amount of data that is compromised in a breach and the attackers' ability to move around the network unseen.
- **Focus and limit the scope of compliance.** Fewer devices, workstations and servers are subject to compliance audits.
- **Mark a clear line between IT and OT.** By establishing zones, the delineation of who is providing services and support is easier to define.

Virtual segmentation can focus on isolating and protecting systems based primarily on the level of sensitivity of data contained within the zone and the level of risk if that data is exposed. All NGFWs, from the PA-7000 Series to the PA-220R as well as the VM-Series, can be configured to block all traffic into the zone as well as use whitelisting to allow only known, trusted traffic. Whitelisted applications are then continuously monitored for security vulnerabilities and malicious activity. This tactic stops unknown, malicious software from entering the zone. It can be configured to authenticate which users have access to data or applications within the zone. This also reduces the effort required to demonstrate compliance (e.g., during an audit) by limiting compliance reviews to only the type of data stored in the zone.

These Zero Trust boundaries, zones or virtual segments of the network enable you to defend each zone from any malicious traffic either entering or exiting that zone. To prevent malware movement and defeat lateral movement of advanced attackers through your network infrastructure to thwart the attack, it is necessary to apply the controls at all of these key entry and exit points. Virtual segmentation zone examples include:

- Applications and database historians used for trending and production analysis (e.g., Industrial SQL, Incuity, PI).
- Level 1 device that connects to physical devices and controls the process (e.g., PLC, RTU, AMI).
- Access to business partners and ICS vendors that provide support (e.g., Honeywell, Siemens, ABB).

Each zone and network should be protected by its own policy, which brings several benefits. Beyond validating the whitelisted applications and their intended users, features of the Security Operating perform several other important security functions on traffic entering and exiting a zone:

- Threat Prevention blocks malicious files with signatures for known threats.
- The on-premises deployment includes options for resiliency and controlled exchange of threat intelligence with the cloud-based environment for improved efficacy.
- URL Filtering blocks access to malicious websites and URLs, sharing newly discovered malicious domains and IP addresses with the community cloud as they're discovered.

By applying this Zero Trust approach, operators of industrial control systems can protect this critical infrastructure's operation and sensitive data from unauthorized applications, or users from exfiltration, reduce the exposure of vulnerable systems and prevent the movement of malware throughout both the enterprise and control systems networks.

Protection Across the Network

Zero Trust scales well, and networks designed with this principle at remote locations and the core become more homogeneous despite the numerous heterogeneous ICS networks that may exist. All networks are built on the same principles of zones and positive enforcement, making it possible to seamlessly merge the IT and OT networks yet still have totally autonomous systems.

Private, Public and Hybrid Clouds

Zones allow companies to compartmentalize systems and traffic as needed in line with mandated compliance requirements, with the added benefit of end-to-end visibility, allowing first responders to move quickly on possible issues.

5. Some organizations use virtual local area networks to segment their network, but VLANs simply isolate network traffic – they are unable to enforce the control of privileged information. In addition, by itself, a VLAN cannot inspect traffic for threats.

After applying the application whitelisting and Zero Trust regimen to remote field locations and the network perimeter, security teams can pursue the same for the heart of their data centers. Today, with the maturation of virtualization technologies, operators of ICS systems have a host of options for their data centers, from a traditional data center architecture to a private cloud, public cloud or hybrid public/private cloud. Many of these asset owners have begun considering the adoption of cloud architectures (mostly private) for future use in enterprise and ICS/SCADA ecosystems. Implementing virtualization for existing applications within the data center reduces costs, improves security and provides a foundation that simplifies future migration to a full private cloud architecture within the ICS.

Although Zero Trust addresses the protection of both north-south traffic entering and exiting the data centers and east-west traffic between applications within those data centers as their own segments, it is worth noting a few more considerations for these environments:

- **Reliability:** Consider active/active high availability for your north-south boundary firewalls to continuously synchronize their configuration and session information, ensuring that, in the event of a hardware failure, no traffic is lost and performance is not degraded.
- **Centralized management:** Use centralized management to ensure policies can keep pace with the rate of change to your virtualized workloads. In VMware NSX® deployments, automate firewall provisioning through predefined APIs.
- **Policy consistency:** Centrally define and consistently apply policies on all devices to reduce complexity that could lead to gaps in threat protection. Use centralized management to serve as a single point of control for all firewalls, both physical and virtual.

Endpoint Protection

To effectively protect all points on an ICS network, security teams should comprehensively enforce the Zero Trust model, down to the endpoint. Particular attention should be paid to the endpoints where threats from external sources can impact critical operational procedures and controls, such as any connected HMI. This is particularly true where the owner-operator may be running legacy endpoint systems or those with unpatched or unpatchable systems, such as Windows® XP, that are no longer supported by their vendors. All endpoints should be covered by your endpoint security strategy, including virtual and physical desktops, laptops,[6] virtual and physical servers, and, where possible, connected devices running real-time operating systems[7]– regardless of patch, signature or software update levels.

There are two main threats to the endpoint: executable malware and exploits that target specific application vulnerabilities. It is critical to protect against both, but exploit prevention is particularly important – even within whitelisted applications – as zero-day threats can appear at any time.

To effectively protect the endpoint:

- Employ lightweight agents to monitor for both exploit techniques and malicious executable files.
- Apply policy-based restrictions. Administrators can easily set up policies restricting specific execution scenarios. For example, you may want to prevent the execution of files in the Outlook® .tmp directory for a particular file type directly from a USB drive.
- IT/OT security teams should also enforce the Zero Trust model for mobile and specialized devices. There are three major categories for mobile and specialized devices to consider:
  - Windows or Mac® laptops
  - Smartphones and tablets, such as industrialized iPad®, iPhone® and Android® devices
  - Specialized devices running Windows CE, such as most models of industrial HMI touch panels

Depending on the type of device, you should incorporate these capabilities into the security program for mobile devices where possible:

- Use secure connectivity – via a VPN tunnel over the internet and back to the controls network – to protect communications.
- Regularly check all devices to ensure they have updated security protections.
- Identify and address all mobile malware found that could affect your production network.
- On devices verified to be up-to-date and free of malware, establish granular policies to determine which users and devices can access sensitive applications and data from a mobile device. The policy criteria can be based on application, user, content, device and device state.

6. Laptops can be especially at risk if users access vulnerable public networks, such as Wi-Fi hot spots at hotels or airports. If a returning user then connects an infected laptop to your corporate or controls network, the risk of infecting other systems undetected increases significantly.
7. Traps is applicable to some real-time operating systems, such as Windows CE. You should conduct testing to determine the impact to your systems.

- Identify device types, such as iOS, Android, Windows and Mac devices.
- Identify device ownership, such as personal or company asset.
- Identify undesirable, insecure device states, such as rooted or jailbroken.
- Control data movement between apps on mobile devices.
- On an ongoing basis, apply the same scanning apply the as that on the network: ongoing exploit and malware protection for mobile threats, and URL filtering for malicious websites.

Advanced or Zero-Day Attack Prevention

Advanced attacks and zero-day malware must be handled swiftly, and automation must be used to ensure threat prevention immediately upon attack or zero-day discovery. This is critical to prevent subsequent evasion and attack attempts. As any unknown file attempts to enter a trusted perimeter or network zone, that file should be "detonated" in an advanced malware execution environment for static and dynamic analysis, as well as for automatic signature generation for any discovered threats to all deployed firewalls.

Timely Reporting – Threat Intelligence and Correlation

Cohesion between IT, cybersecurity and intelligence professionals is important for reducing the threats to any network. Coordinate across endpoint, data center, networking and security teams to understand the potential threats to your network, improve security, ensure immediate access to priority events, and enable automatic sharing and distribution of intelligence. With the Security Operating Platform, this coordination and collaboration is easier because of the interoperability across all of the security capabilities discussed above. Individual Security Operating Platform and management views can be customized per administrator or department while still sharing views into alerts and other activities of interest across the entire network. See more information about the improved reporting and threat intelligence possible in the next section.

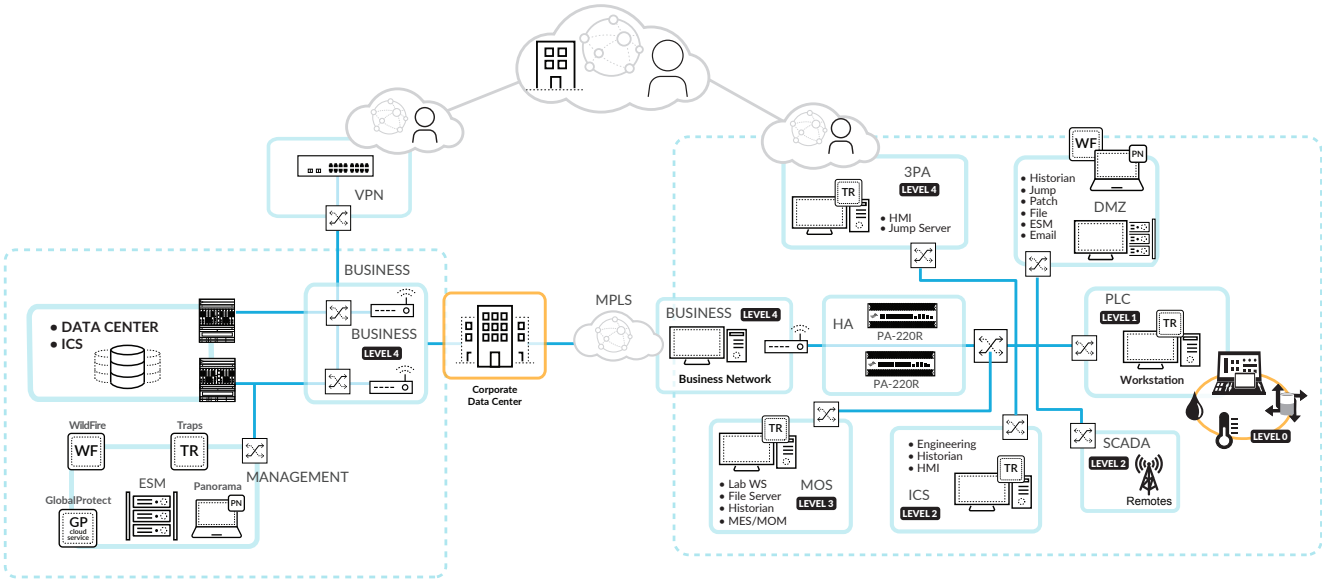

Figure 3: Reference blueprint for Industrial Control Systems

V. THE SECURITY REFERENCE BLUEPRINT FOR ICS

This section provides a high-level reference blueprint for industries using ICS/SCADA systems. This blueprint incorporates the security principles using the Security Operating Platform with various next-generation firewall models to protect OT environments from the endpoint to the network core. Although your architecture decisions,including the appropriate virtual segmentation and NGFW model to use, will be determined by your own unique network requirements, the example blueprint in Figure 2 segments the network into security zones based on the generic ISA 95 model, which could be applied to automation environments across multiple industry sectors. With options like the PA-220R or VM-Series firewalls on a ruggedized server available to address harsh environments, you can achieve Zero Trust network design and segmentation in a manner that keeps you compliant.

Level 4: Business Logistics Systems

The Business zone contains processes and systems relevant to the running of the enterprise business. Services found at this level include email, file sharing, customer web services, internet access, HR systems and others. From a reference point of view, the business zone, as it stands in relation to the industrial control network, should be treated like the internet and with the same level of concern. All traffic coming from this zone should be treated as potentially housing threats, and inspected. All traffic being sent into this zone should be inspected to ensure that information is not being redirected to destinations outside of the company's control but only to the personnel and systems that require the data.

DMZ

At a remote plant facility, the "demilitarized zone," or DMZ, provides a place where IT/OT can exchange services and data in a controlled, restricted fashion on a need-to-know, need-to-access basis. Services found in this zone typically include patch management, data backups for the local plant, antivirus management systems, jump host servers, deployment systems, and any other server or system that may require information data exchange between OT and IT.

As previously noted for the principles of Zero Trust, all traffic into and out of the DMZ – as with any other zone – can be scanned by Palo Alto Networks next-generation firewalls to guard against malicious payloads or inappropriate data leakage, through services including:

- **Threat Prevention** – covers malware, exploits, and command and control
- **URL Filtering** – blocks access to known malicious websites
- **WildFire** – detects and stops zero-day malware
- **Credential theft prevention** – blocks transmission of corporate credentials to domains associated with phishing

Level 3: Manufacturing Operations Systems

Devices and services in the MOS zone are concerned with managing the operational environment and workflow to produce the products. Items found in this zone would be replica data historians, performance management systems, simulations and modeling tools, manufacturing execution systems, and manufacturing operations management systems – MES/MOMS, respectively. With these devices and services zoned off, security is now able to control and enforce what data is allowed to enter and leave this area.

Level 2: Control Systems

The ICS zone contains devices responsible for the real-time control systems that supervise, monitor and control the physical processes. The devices typically found would be the human-machine interface, engineering workstation and operation alarm system data historian. These systems are of special concern because of what they do and the fact that, in most companies, these devices are running on end-of-life operating systems that are no longer supported.

These internal endpoints, often running on Windows XP with SP3, Windows Vista®, Windows 7, Windows 8.1, and Windows Server® platforms, can be protected with Palo Alto Networks Traps™ advanced endpoint protection to ensure that any exploits on vulnerable systems, regardless of patch status, are immediately thwarted. The agent will automatically prevent attacks by blocking techniques, such as thread injection. When unknown executable files are discovered, Traps will automatically query WildFire® malware prevention service with a hash and submit the unknown files to assess their standing within the community.

Another major concern for these systems is the fact that they control deterministic processes and applications like antivirus, which must reside in memory and run the risk of slowing down system response. Using the Security Operating Platform, it is possible to protect these critical assets without negatively impacting system performance, with the platform acting as a remediating control because antivirus, malware and zero-day prevention sit in-line in front of the systems on a separate appliance. Also, by using any Palo Alto Networks NGFW to provide these services, you protect all devices at the same level, at once, simplifying management.

Ruggedized mobile devices, including both PCs and handheld mobile devices, can be protected by Palo Alto Networks GlobalProtect™ network security for endpoints. All unidentified files should be sent to WildFire for static and dynamic analysis of potential mobile threats. Enable two-factor authentication for even more protection of mobile devices.

Level 1: Intelligent Devices

Devices found in the PLC zone are responsible for sensing and manipulating the physical processes. With the move to IP, these once-serial devices have been upgraded or retrofitted with Ethernet ports to play in the industrial internet of things, or IIoT, era. In many cases, the concern was to get the data to the teams that needed it as quickly as possible, with no concern for security. Devices placed in this zone are items like programmable logic controllers, remote terminal units, programmable relays, analyzers and, possibly, an operator workstation, all of which may suffer from common, default or shared passwords, or lack of two-factor authentication. By placing these items into a segmented PLC zone, the security team is now able to leverage services like Active Directory® or LDAP as a means to restrict access by user or user group and log access from across the network.

Level 2 or 3: SCADA

In the reference model, devices placed in this zone are dealing with remote data collection, usually done with some form of RF technology. Information being brought into the system is important but not necessarily time-sensitive or critical in nature. Physical security of devices connected in this zone is difficult due to their remoteness and structures in which they may be housed. The spotty nature of RF, and the remote distance, can make these devices easy prey for compromise. Attackers have time to remove and replace devices, modify the operating systems, or do network reconnaissance with little fear of being caught.

Level 3: Third-Party Access – Optional

Rather than place third-party vendor access in the DMZ, where there is still the possibility of exposing workstations and servers housed there to external threats, the ideal deployment would be to create a separate zone just for remote vendor/support access.

Using the Security Operating Platform to segment the network using the above baseline delivers salient benefits, including:

- Ability to verify service-level agreements.
- Total visibility into traffic entering and leaving your production network, with the ability to alert or block known and unknown malware, advanced persistent threats and zero-day exploits.
- Restriction of access based on user or user groups.
- Restriction of access based on schedules.
- Restriction of protocols to only those necessary for support and maintenance.
- Enforcement of two-factor authentication.
- Definition of enforcement levels on a per-vendor, per-person or per-user group basis.

Threat Intelligence and Correlation

The combination of these products and their integrated reporting capabilities allows security administrators to coordinate insights to improve security, ensure immediate access to priority events, and enable automatic sharing and distribution of intelligence.

This coordination and collaboration is easier with interoperability across all of the security capabilities discussed previously. Individual next-generation firewall and management appliance views can be customized per administrator or department while still sharing views to alerts and other activities of interest across the process control network.

Within the process control network, Palo Alto Networks provides prioritized, actionable security intelligence on attacks that merit immediate attention through AutoFocus™ contextual threat intelligence service. AutoFocus builds on billions of threat artifacts from more than 26,000 WildFire subscribers and applies unique, large-scale statistical analysis, human intelligence from the Palo Alto Networks Unit 42 threat intelligence team, and tagged indicators from your organization, plus a global community of cybersecurity experts also using the service. AutoFocus provides full context on attacks, such as who is attacking, how they are attempting to compromise the network, and if any indicators of compromise are already present on the network.

Often, organizations in the same industry face attacks by the same adversary. In industries that utilize ICS and SCADA systems, there is a growing interest in disrupting these systems for a multitude of reasons, ranging from corporate espionage to crippling a country's critical infrastructure. The need to act swiftly is great. WildFire enables swift sharing of threat signatures so that all parties can benefit from threats discovered across all organizations within your industry, while AutoFocus enables organizations within the same industry to understand what others have seen.

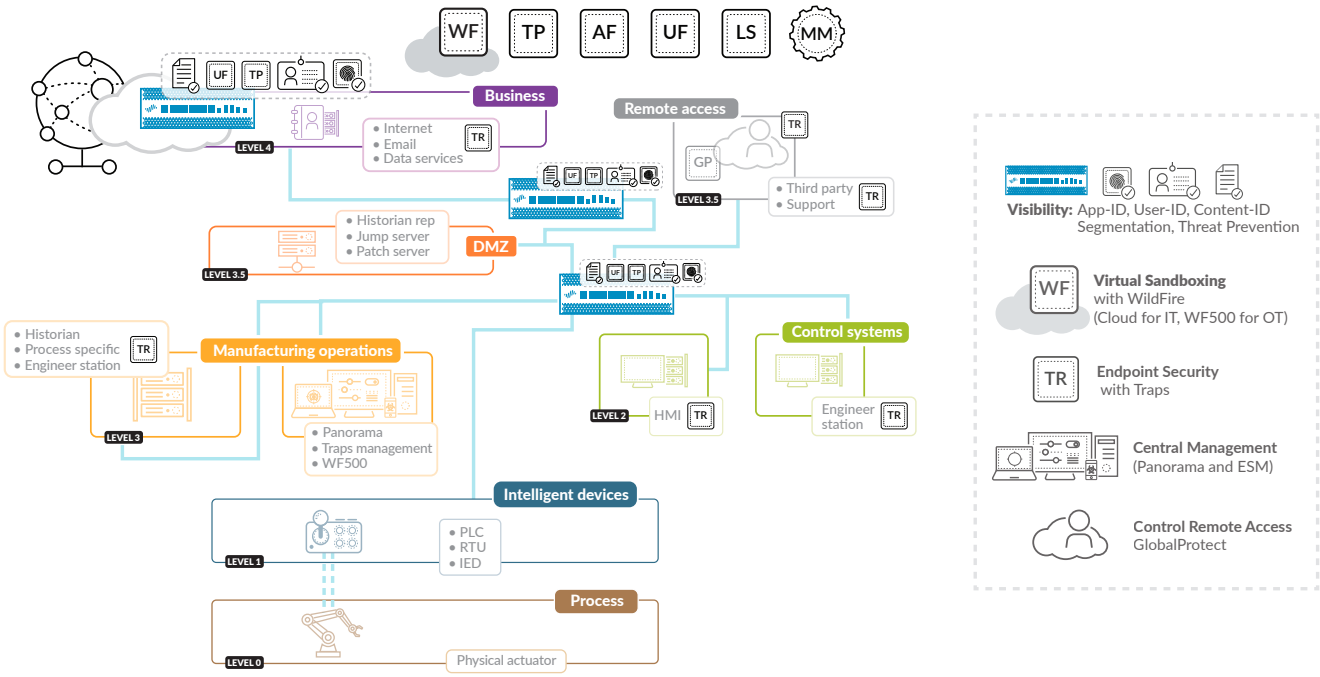

Figure 4: Security Framework enables Zero-Trust in ICS/SCADA

Through MineMeld™ threat intelligence syndication engine, an open-source tool or part of AutoFocus, organizations can integrate public, private and commercial intelligence feeds. Moreover, AutoFocus can also feed indicators into MineMeld, which can then automatically create new prevention controls for Palo Alto Networks security appliances. Ultimately, this enables organizations to take action on the indicators of compromise by generating new prevention-based enforcement for their security services.

Migration to Palo Alto Networks Security Operating Platform

When you are ready to realize the threat prevention benefits of the Security Operating Platform, the Expedition migration tool makes it easy to migrate from IP/port-based firewall rules in legacy firewalls[8] to application-based rules in our next-generation firewalls while minimizing the risks of the change. What also facilitates this transition is the powerful Application Command Center in the next-generation firewall, which depicts the top applications and sources in your network, as shown in Figure 4. This delivers the visibility necessary for understanding the needs of your particular organization while making decisions on how best to reduce risk.

A phased approach via documented change control is highly recommended. Successful deployments typically first perform a like-for-like migration of firewall rules to the Palo Alto Networks firewall component of the platform. Then, after about 15 days, the deployment team uses the migration tool to begin the iterative process of defining application-based policies to replace the legacy port-based policies. After the last migration phase, the port-based rules are removed and the application-based policies remain.

In future phases, the deployment team can work with the security team and operations control to take full advantage of the application policies technology by restricting access to individual applications based on the desired criteria, such as Active Directory security groups or location-based user IP address ranges.

Functional Area	Supporting Capabilities of the Security Platform	PA-220R NGFW	WildFire	Traps
Identify	Identify network traffic and usage at granular levels	x		
	Applications, ICS protocols, protocol functions	x		x
	Users and user groups, IP address, countries	x		
	Files, data strings, URLs, domains	x	x	x
Protect	Reduce the number of attack vectors, including applications, protocols, domains/URLs, user and other segmentation	x	x	x
	Protect unpatched systems from zero-day exploits and never-before-seen malware	x	x	x
	Prevent malicious use of ICS protocols	x		
	Secure mobile and virtualized environments	x	x	x
	Prevent data exfiltration	x	x	x
Detect	Detect unauthorized use whether malicious or non-malicious	x		x
	Decrypt encrypted traffic to identify stealthy malicious traffic	x		
	Detect known threats and unknown threats that have never been seen before in the wild (IPS, AV, malicious domains/URLs, command and control, "Son of Stuxnet" attacks)	x	x	x
	Correlated detection can be performed on the network or at endpoints	x	x	x
Respond	Shared context between application, user and threat/content information increases intelligence, which simplifies forensics process	x	x	x
	Cloud-delivered threat intelligence provides automated threat analysis and protections for both endpoints and the network	x	x	x
	Integration with other security devices, such as real-time SIEMs, enriches the analytics	x	x	x
Recover	Protections from cloud-delivered threat intelligence are automatically disseminated to endpoints to prevent attacks on the network and endpoints	x	x	x
	Knowledge of any impacted devices is provided back to centralized management and can be remediated	x	x	x
	Easy deployment of any additional policies/segmentation to improve security posture	x	x	x

Table 1: Security Operating Platform capabilities aligned to NIST Cybersecurity Framework

8. Palo Alto Networks Expedition migration tool is compatible with Juniper, Cisco, Check Point, Fortinet and McAfee configuration files.

Regulatory Compliance

Today, many different industries use ICS/SCADA systems to automate and optimize the products and/or services they produce or deliver. Some of these industries have regulations, with extremely costly penalties if compliance is not met or kept. Others, including Oil and Gas, do not, at least at the time of this writing, but see the day coming. Either way the Palo Alto Networks Security Operating Platform can help an organization meet and exceed governance, whether it's from the business's internal compliance group or a government entity.

Summary

Owner-operators of ICS and SCADA systems who implement these effective security controls with the Zero Trust prevention focus of Palo Alto Networks Security Operating Platform can protect the process controls network, segment and isolate the controls network, protect process data and maintain regulatory compliance, all while enabling the most demanding of users and ensuring the security of the network.

To learn more about how the Security Operating Platform can help secure your ICS/SCADA infrastructures, contact your local sales representative. Make sure to ask about a complimentary **Security Lifecycle Review** that will help you to understand which applications, risks and threats – both known and unknown – may exist in your critical infrastructure networks.

Also, ask about our hands-on workshop for ICS/SCADA networks, in which you'll get guided, hands-on experience with the Security Operating Platform. The workshop is designed to give you an enhanced understanding of how our products can solve your problems and improve your organization's security posture. All workshops consist of a virtual lab environment with step-by-step directions and an expert instructor who is available to guide you. No other experience compares to the hands-on practice you get at a Palo Alto Networks ICS/SCADA hands-on workshop.

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

security-reference-blueprint-for-industrial-control-systems-wp-021119