JUNIPER NETWORKS | Engineering Simplicity

White Paper

SOLVING INDUSTRIAL SECURITY CHALLENGES WITH IOT SOLUTIONS

A step-by-step approach to securing operational infrastructures with Juniper Networks

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The security challenges associated with Internet of Things (IoT) devices are familiar to anyone tasked with protecting resources in an organization. Security products protect some applications and some operating systems within the infrastructure. Simple signatures can be applied to protect common platforms from known threats. If these threats are new or uniquely advanced, behavior-based analysis can be applied to protect common endpoints. The looming challenge, however, is how to identify threats targeting new platforms and/or new operating systems recently introduced into an organization's infrastructure.

Digital transformation is having a significant impact on industrial organizations; the efficiencies gained by integrating business processes with mature infrastructures are considerable. But the risks and potential problems that new devices introduce are arguably larger. Where should we apply our efforts and investments to maintain our current security postures? This paper offers a step-by-step approach to securing operational technologies.

Introduction

In the past, organizations minimized risk by allowing only known hardware (managed by the organization) with known operating systems and known applications to connect to the network. Over time, as businesses (and users) began to demand more network access flexibility, companies responded by isolating unknown devices on "guest" or "bring your own device" networks. However, as companies invested more in network infrastructure and continued their digital transformation, they discovered they could realize business efficiencies by integrating "old" devices—those that had never been connected to global networks—with "new" networks. Many of these devices lacked standard TCP/IP communications or standard protocols.

Operational Technology (OT) devices are an example of these "old" devices. Relied on by businesses to operate production lines, monitor business processes, and accelerate production, these devices have been the bread-and-butter of many organizations for years. Integrating these solutions into newer networks can produce significant cost savings; the efficiencies gained by enabling OT administrators to remotely access these devices (whether within a building or from somewhere across the globe) are undeniable. Therefore, it's no wonder that the number of unknown and unsecured devices on organizational networks continues to grow. As is often the case, the pace of business has outpaced the ability to secure the infrastructure.

Although the future for OT security appears grim, there is good news. In many cases, the same technologies applied to known hardware, applications, and operating systems can also be reapplied to OT use cases, as well as to IoT devices in general. In some cases, traditional security technologies simply need to be tweaked in order to work successfully with the new use cases; in other situations, solutions can be built and integrated to solve these security challenges. In each of these cases, Juniper Networks can help.

Securing Operational Technologies with Juniper Networks

In many ways, the steps for securing OT device infrastructures are the same ones that organizations use to secure traditional infrastructures.

Steps to Securing Operational Technologies

1. **Know the business risk**: Understand and prioritize your business' high-value assets. Which parts of the infrastructure would be most devastating to lose? These should be your security priorities.
2. **Know the network**: Map your network to understand its layout. Know where your high-value assets reside. Create baselines to determine the expected communication patterns. Use these baselines to proactively identify threats.
3. **Segment the assets**: Reduce the attack surface by ensuring that vulnerabilities on one segment don't threaten valued assets on other segments. Segmenting with the proper controls is critical to minimizing the attack surface, allowing you to catch and quarantine threats faster.
4. **Control access**: Ensure that only users who require access to do their jobs are allowed on each network segment. Creating role-based access control or identity access management is key to a strong security posture.
5. **Monitor for unexpected behaviors**: Ensure that no new or unexpected endpoints appear, and make sure that all network communications are expected.

A Step-by-Step Approach

Step 1: Know the Business Risk

Task: The first step in securing your infrastructure is to understand and prioritize the value of your business assets. This can only be determined by understanding the related business objectives and strategies. If the IT organization doesn't have a seat in the executive board room, now is the time to make sure it does. Cybercriminals know the high-value targets in an organization's infrastructure, so it is imperative that the IT organization identifies and understands them intimately. In most organizations, it's fairly easy to determine which devices are of highest value to the business; they are the ones running the production lines, enabling manufacturing processes, monitoring production methods, and the like. But does the organization understand which databases store critical business data? Does it know what servers process business transactions? Does it understand where critical assets are stored, and who has access to the critical data? These questions (and many others) must be answered before developing and deploying a security strategy. In a business where staff is already spread thin, this business value mapping not only helps determine how to secure business assets, it also helps to identify which assets need to be secured first.

How Juniper can help:

Juniper® Professional Services has experts who can help organizations identify and prioritize assets through an assessment. Contact Juniper if you need assistance mapping business strategies and objectives to the prioritization of infrastructure assets.

Once the infrastructure is inventoried, secured, and monitored, Juniper Networks® JSA Series Secure Analytics with vulnerability/risk manager can monitor policies and network activity and provide a comprehensive risk report. Changing risk conditions can be identified and highlighted, enabling the organization to adjust as needed.

Step 2: Know the Network

Task: Once the business objectives and strategies are understood and the assets are prioritized, the business can start mapping the network to understand where the assets are located; some will have high business value and others will have low business value. In highly controlled industrial environments, the value of knowing what assets are on a network—and which don't belong—cannot be overstated. Additionally, understanding asset location is vital to creating a segmentation and isolation strategy (Step 3). Combining this information with business priorities from Step 1 will determine where tight budgets should be applied and which assets will be secured first.

How Juniper can help:

JSA Series Secure Analytics with threat manager profiles assets and creates an inventory. Any deviations from the current inventory are noted as the JSA Series platform continues to monitor the assets, watch network traffic, analyze log data, and perform vulnerability scans.

Additionally, Juniper Networks SRX Series Services Gateways can capture network traffic, identify communication patterns with predefined and custom signatures, and assist administrators in identifying unknown or previously unseen network traffic.

Finally, Juniper has Professional Services experts who can help organizations locate assets through an assessment. Contact Juniper if you need assistance assessing inventories and locating unknown assets within your infrastructure.

Step 3: Segment the Assets

Task: After prioritizing business assets and understanding where they are, the next step is to isolate high-value assets from those that do not belong on the same segment. Segmentation is extremely important for many reasons; first, it eases the administrative burden by grouping assets from similar categories or those with the same access policies. More importantly, it prevents breaches of lower business-value assets or assets with broader access policies from impacting higher value or stricter privilege assets. Although segmentation is important to minimize exposure in a cybersecurity attack, it also minimizes the risk of malicious insiders gaining easy access to unprivileged assets.

How Juniper can help:

Realizing that malware can be spread by simple network broadcasts, some level of security can be applied by simple network segmentation. Juniper Networks MX Series 5G Universal Routing Platforms, or EX Series Ethernet Switches and QFX Series Layer 3 switches can provide that segmentation.

Higher levels of segmentation can (and should) also be provided. SRX Series physical firewalls or Juniper Networks vSRX Virtual Firewall can be deployed to prevent unwanted network sessions and application communications. Once an organization has located assets and determined expected communications in the previous step, an organization can easily create security policies on the SRX Series firewalls based on endpoint communication, utilization of network ports and protocols, and business application signatures.

Application identification on SRX Series firewalls lets organizations monitor these segmented communications. Application firewalling on SRX Series firewalls enables organizations to control communication between assets based on application-level signatures.

Additionally, intrusion detection on SRX Series firewalls allows organizations to block previously identified threats and vulnerabilities on OT devices.

Organizations will find a large archive of existing applications (including industrial applications) and threat signatures already available in Juniper's signature packs. Juniper also provides a tool to create custom application and threat signatures for proprietary and custom-built business applications.

Step 4: Control Access

Task: Now that assets and applications have been mapped to business priorities and segmentation policies have been applied, it's time to determine who within the organization should have access to these applications, and then integrate this information with the security policies. It's a straightforward task, but it's more difficult than mapping assets to business value.

How Juniper can help:

SRX Series firewalls have multiple ways to identify users. For smaller organizations, a local user identification table can be configured on the platform. For larger organizations, the SRX Series device can reference more scalable authentication stores such as Active Directory/LDAP, Juniper Identity Management Service (JIMS), Pulse Secure UAC, or Aruba ClearPass. All options give security administrators the ability to apply specific user privileges to security policies configured to match endpoints, ports, protocols, and applications.

Step 5: Monitor

Task: No security task is complete without a feedback loop. The same is true for securing industrial infrastructures. Once the business value has been mapped to assets, and appropriate policies and access controls have been applied, it's time to monitor the system for changes. Malware threats change frequently, and so do the security postures and configurations of a business' assets and infrastructure. One accidental access control omission or policy oversight could mean immediate exposure for a high-value business asset. Continuous monitoring and analysis of a business' security posture, along with constant assessment of the threat surface for new vulnerabilities and threats, are vital for mitigating risk to important business processes.

How Juniper can help:

The JSA Series Secure Analytics platform comprehensively monitors an organization's infrastructure for changes, vulnerabilities, and associated business risks. On top of threat manager capabilities, customers can add vulnerability or risk manager to correlate logs, event information, and additional threat information (such as Qualys, Rapid 7, Tenable, and others). Additional capabilities include: risk assessment reports based on prioritization of business value assets; analysis of configurations, policies, and network activity; and modeling capabilities for simulations of attacks and network changes.

Juniper can help businesses by minimizing risk through the capabilities summarized below.

Table 1: A Step-by-Step Approach to Securing Operational Technologies

Task	Solution
Know the Risk	JSA Series Secure Analytics with vulnerability/risk manager Juniper Professional Services
Know the Network	JSA Series Secure Analytics with threat manager Juniper physical SRX Series or virtual vSRX firewalls Juniper Professional Services
Segment the Assets	MX Series 5G Universal Routing Platforms EX Series and QFX Series switches Juniper physical SRX Series or virtual vSRX firewalls with application identification, application firewalling, and intrusion prevention Juniper Professional Services to design, deploy, migrate, and operate the infrastructure
Control the Access	Juniper physical SRX Series or virtual vSRX firewalls with access control integration
Monitor	JSA Series Secure Analytics with vulnerability/risk manager

Conclusion

Securing networks and digitally transforming business while introducing new platforms and devices to the infrastructure are seemingly overwhelming tasks. IT administrators are asked to maintain security on a constantly evolving network infrastructure while ensuring no interruption to business operations. At the core of these activities is the desire to minimize business risk. Using the steps outlined in this white paper, businesses with OT and IoT devices can systematically prioritize business assets, map out the infrastructure, apply segmentation policies and access controls, and continuously monitor for infrastructure changes and new threats, maintaining a strong security posture.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity