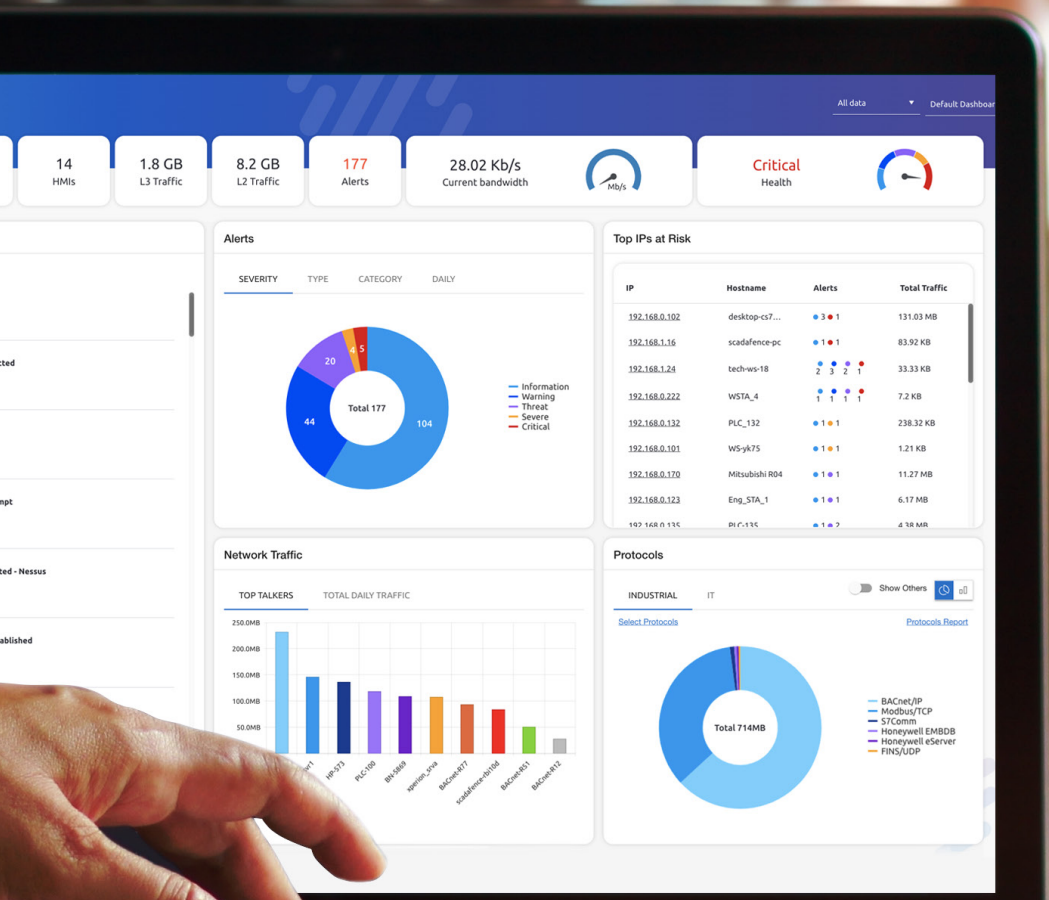
SCADAfence

THE BUYER'S GUIDE TO OT CYBER SECURITY



CONTENTS

What To Know Before Choosing A Vendor

If you are responsible for an OT/IIoT/ICS network of any size, you already know that cyber security must be one of your highest priorities. A proper security solution protects your network from internal and external malicious threats and safeguards the people working in your OT environment.

What you may not know is how to choose the best OT security solution for your organization.

This buyer's guide will lead you through the process of choosing an OT security solution, give you a deeper understanding of what makes OT security a unique challenge, and help you find the best solution for your organization.

Part I of this guide explains the full nature of the threat to OT networks, and explains how OT networks differ from IT networks as they relate to security.

Part II offers details of what to look for when choosing a solution, what features are must-haves, and the right questions to ask potential vendors.

Part I
Understanding The OT/IIoT Security Challenge

7 Reasons
Why OT Networks Are Hard To Secure

1 The Rising Threat to Industrial Control System (ICS) Environments

The FBI estimates that malicious cyber activity cost the U.S. economy 18.7 Billion dollars over the past five years. The NotPetya attack alone cost more than $1B, as A.P. Moller-Maersk and FedEx experienced approximately $300 million each in damages. Recently announced vulnerabilities such as Wind River VxWorks' Urgent11 and Schneider Electric TRITON/TRISIS, indicate that weaknesses compromising the safety and reliability of control systems exist in many Industrial Control Systems.

Each OT network contains a combination of elements that are there to control critical services and others that are there to ensure safety. Therefore, to protect both the processes and the actual workers, identifying and managing the vulnerabilities of OT devices is critically important.

2 Legacy OT/IIoT Devices Are Still Widely Deployed At Scale

The vast majority of Industrial Control System (ICS) components are outdated legacy devices. According to NIST, 85 percent of ICS devices currently deployed in the field are between 10-15 years old. Many, such as Programmable Logic Controllers (PLCs), process sensors, gateways, and workstations are no longer patchable and can't be upgraded due to technical or operational constraints.

Overall, OT devices are much more vulnerable than typical IT equipment for the following reasons:

1. Many OT devices were designed decades ago with the assumption that they would be deployed on air-gapped networks. They were developed during an era when cyber security considerations were not always factored into design.

2. OT devices often do not have powerful CPUs that are needed for implementing strong security mechanisms such as encryption or advanced authentication protocols. In most cases, no security measures have been implemented in OT devices.

3. OT devices are not always updated with the latest firmware and system updates, as is done in the IT world. Upgrading the devices would require undesirable downtime in the production environment and therefore it doesn't happen. Less frequent updates means more vulnerability to attacks.

These factors cause OT devices to be more vulnerable for much longer periods of time than their IT counterparts.

3 IT Security Solutions Don't Work In OT Environment

It may be tempting to use IT security solutions already in place (and paid for!) and adapt them to the OT environment. However, there are a number of reasons why that won't work.

Due to the complex intricacies of an OT environment, OT devices are much less open to scanning and testing routines, and therefore might contain hidden vulnerabilities that remain undiscovered.

Many tools such as firewalls, NAC and local agents like antivirus software are not applicable to industrial devices such as PLCs and remote terminal units (RTUs). Equipment vendors don't implement them, and they are not part of the approved configuration.

The OT equipment industry has still not reached the level of maturity of the IT world. Some vendors do not cooperate in the research and disclosure of their equipment's vulnerabilities and do not add their vulnerabilities to the CVE database.

Alongside the known and addressable (i.e. patchable) vulnerabilities, there exist many vulnerabilities that are either known but remain un-addressed, or even worse remain hidden and undocumented. This means that no CVEs are being listed and managed. This results in critical processes in OT networks remaining highly exposed to malicious actors.

4 High Deployment and Maintenance Costs

Since many OT networks are very large and dispersed, sometimes over thousands of miles, vendors often suggest placing sensors in each segment to collect and analyze information. However this can be cost-prohibitive and difficult to maintain long term.

5 Increased Remote User Access

Remote access to OT equipment was always a major Achilles heel in OT networks. The COVID19- pandemic accelerated this trend and now workers in all locations and industries require the ability to access OT networks remotely. These networks were not designed for remote access but the sudden onset of the pandemic left business owners with few options. Suddenly everyone had to work from home and there was no choice but to prioritize functionality over security.

The steep increase in supply chain and ransomware attacks originating from remote sessions proves the precarious situation we were left with.

Unlike IT equipment, legacy OT equipment usually lacks proper remote user security mechanisms. Remote sessions on OT devices are often not encrypted and have no user authentication.

Therefore, it is crucial to be able to monitor and understand how remote users are accessing critical devices inside the OT network and what actions they are performing on these devices.

6 False Positives and Alert Fatigue

Almost as dangerous as having no security on an OT network, is having too much of the wrong kind of security. Many OT security platforms issue a vast number of incorrect or unnecessary notifications. This creates a burden on security teams who have to verify and investigate every alert.

This leads to two negative effects:

It creates 'the boy who cried wolf' type of alert fatigue which can cause genuinely important incidents to get missed.

Many resources are required to review these alerts manually one at a time. Sometimes organizations end up hiring special analysts to investigate every alert. This has proven to be a costly and time consuming strategy.

7 Increasing Regulations And The Difficulty Of Measuring Compliance.

Due to the increase in attacks on industrial control systems and the vast damage they cause, governments around the world are attempting to strengthen their country's security through regulation. Industry and critical infrastructure sectors need to become compliant with regulations such as IEC 62443, CMMC, TSA, ISO 27001 Directive, and NERC-CIP to name just a few.

In addition, organizations want to more effectively measure and manage security implementation and initiate internal policies of their own.

However these regulations and policies often focus on whether controls are in place, with no adequate way to measure if in practice the policies have been properly implemented, or if they are effective. For example, a firewall might be in place as mandated, but there may still be unauthorized access if it is being bypassed by a rogue Wi-Fi antenna or inbound modem connection.

Now that we've outlined the specific challenges of protecting OT networks, let's discuss what to look for in a solution.

PART II

Choosing The Right OT Security Solution For Your Organization

In light of the challenges outlined above, it's recommended that all organizations relying on OT, implement a security solution that provides all of the following functionalities:

- **Asset Detection and Inventory Management**
  This will help you gain full visibility and manage the OT, IoT and IIoT asset inventory across your entire organization, including in multiple locations.
- **Threat Detection**
  You should be able to detect legitimate potential security threats and assure your organization's business continuity.
- **Vulnerability Management**
  The solution should identify the assets with known vulnerabilities in order to reduce the exposure of the OT networks to security threats.
- **OT Native**
  You'll need a solution that was created specifically for an OT network, and reflects a deep understanding of the OT process and is designed to integrate new types of OT devices easily.
- **Risk Management and Analysis**
  You will need to understand and manage the risk level of the OT/IIoT network to assist with making the right security decisions and prioritizing your security resources.
- **Remote User Security**
  You will need to monitor all of the remote user activity inside the OT/IIoT network.
- **Compliance**
  You will also have to manage your organization's compliance with policies and regulations across your extended OT/IIoT network.

Additionally, there are several other elements to look for in an OT security solution that will improve the experience of implementation and increase overall value and long-term satisfaction.

OT CYBER SECURITY SOLUTION ESSENTIALS

QUICK TIME TO VALUE

A SIMPLE AND COST-EFFECTIVE DEPLOYMENT

IT MUST BE EASY TO USE

IT HAS TO SCALE WELL ACROSS ALL YOUR SITES

IT MUST INTEGRATE WITH YOUR EXISTING IT SECURITY ARCHITECTURE

YOU NEED GREAT CUSTOMER SERVICE

Gartner, in their recent report, Innovation Insight for Cyber-Physical Systems Protection Platforms, mentions all of these as necessary elements for a successful security solution.
Gartner

Let's examine each of these in-depth...

Asset Detection and Inventory Management

OT/IIoT environments are notorious for their diversity of assets. The number of vendors and types of devices is vastly larger than in IT environments which tend much more toward homogeneity.

WHAT YOU NEED TO LOOK OUT FOR

A solution that is built to support various network models and technologies. It must have dedicated representations for SCADA systems, as well as for Distributed Control Systems (DCS) or other IIoT systems.

The ability to gather maximum information passively without actively polling devices. (active polling is also recommended as an optional means to gather information.)

A flexible solution that allows you to fill in user configurable fields.

A solution that enables integration with other organizational asset inventory for automatic enrichment of data via API or other means.

Effective Threat Detection With Minimal False Positives

Coping with countless alerts causes alert fatigue and results in missing important incidents. It also wastes your resources, is really time consuming, and renders your organization's threat detection efforts ineffective.

WHAT TO LOOK FOR

You need to find a solution that provides an advanced baseline that can cope with dynamic and complex networks. A granular baseline that analyzes each asset individually will provide the best results in terms of accuracy and low false positive rates.

The baseline should also automatically adapt to changes in the network and in the OT processes running on it. Make sure that the baseline doesn't need resets and restarts after changes in the network, as that would make the solution ineffective for large parts of its lifetime.

You need to find a solution that triggers a manageable number of accurate alerts, even if deployed in large or noisy networks, and not only in a testing lab (we've seen too many organizations make this mistake).

You need to find a solution with the ability to handle Denial of Service (DoS) and alert-storm use cases efficiently.

[1]Innovation Insight for Cyber-Physical Systems Protection Platforms by Katell Theilemann and Wam Voster. Aug 2022

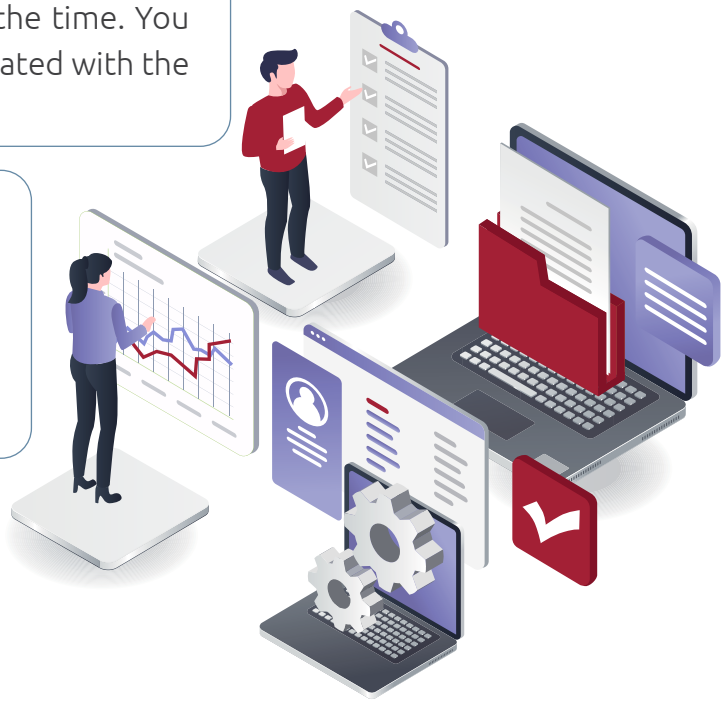
Vulnerability Management

A large OT network may contain literally thousands of devices, each with its own known vulnerabilities. The solution should identify each asset's known vulnerabilities in order to reduce the exposure of the OT networks to security threats. A proper OT security solution should make it easy to perform regular identification and prioritization of new vulnerabilities.

WHAT TO LOOK FOR

New vulnerabilities are being discovered all the time. You need a security solution that is constantly updated with the latest vulnerabilities.

Not all vulnerabilities present the same amount of risk. It's important to have built-in risk assessment and prioritization to help your team focus on addressing the vulnerabilities with the highest risk first.



Is It OT Native?

It is important to choose a solution that is especially built for OT networks, not adapted from an IT solution. It must have the ability to analyze OT network traffic and alert on any threat that might endanger the OT process.

WHAT TO LOOK FOR

As OT environments are very diverse, the solution you choose must allow you to define new ICS traffic rules, not just rely on built-in rules that are difficult to update.

If you are planning to inspect traffic variables, look for tools that can cope with a large number of variables, and have advanced options to group variables. The solution should also suggest variables to analyze, and not require manual work to set up, as this would be impractical on a large network.

Look for vendors that are responsive and willing to collaborate and support your needs for rare protocols or functions in a timely manner if needed.

Risk Management and Analysis

A long list of events and notifications does not always provide a balanced, accurate picture of the current level of exposure. Nor does it help with prioritizing the issues that need to be addressed. In order to understand the true risk to the organization and decide on an effective course of action to reduce it, look for a solution that analyzes the real-time traffic from a risk perspective.

WHAT TO LOOK FOR

- You need to find a solution that correlates between vulnerabilities and the criticality of the associated assets, for better prioritization
- A solution with the ability to analyze holistic architecture risks, not only single event risks.
- A solution that can correlate your risks to industry accepted models such as the MITRE ATT&CK for ICS framework.

Remote User Security

One can find in the marketplace many remote access security gateways, in comparison to more elegant monitoring solutions that do not require change to the network architecture.

WHAT TO LOOK FOR

- A solution that can correlate user activity across both IT and OT in order to understand who accessed which OT devices and track their actions. Many weaker solutions in the marketplace don't have an effective way of tracking OT activity back to its source in the IT network.
- You need to find a solution that doesn't require changing your network's architecture, and does not require additional costly components in-line.
- It is important to find a solution that is compatible with OT vendor's remote access solutions - such as cloud-based remote access which are not compatible with gateway solutions
- You need to find a solution that can provide automatic correlation of user activity. Gateway solutions require the administrator to manually review video recordings of sessions in order to do so, and this often doesn't provide insight into the traffic. It shows the screen recording but not the actual traffic sent.

Compliance

Regulatory requirements are increasing, as are organization-wide security policies. It is crucial to be able to measure and quantify to what extent these requirements are being met and accurately report the results to the business side of the organization.

WHAT TO LOOK FOR

- You need to find a solution that can correlate network events to regulatory or organizational compliance.
- Organizational dashboard for compliance to the standards in your industry, across all your sites
- Ability to integrate the compliance solution with other tools, so you will have one central compliance dashboard.

Time To Value

Look for a product that is easy to deploy, doesn't require pressing pause on your business for a complicated installation and provides near immediate results. Some products on the market require weeks for baselining and tuning and therefore take longer to deliver value, leaving your networks unprotected for extended periods of time.

WHAT TO LOOK FOR

- Short installation time, without the need for complicated installation.
- Baseline learning period of 1-2 days instead of weeks-months
- An adaptive Baseline - a baseline that automatically adapts to changes in your network and in the OT processes, instead of needing multiple resets and restarts upon any change in the network. Products requiring multiple restarts after changes are made to the OT network, can end up remaining in constant learning mode, and render that solution unusable.

Simple And Cost-Effective Deployment

Large distributed networks require cost-effective traffic analysis methods. A solution that relies on deploying hundreds of sensors in remote locations is impractical from budget and maintenance perspectives.

WHAT TO LOOK FOR

Flexibility. The solution should offer software as well as hardware options

You need to find a solution that supports sensorless deployment options. Sensorless solutions collect information by using network protocols such as NetFlow, ERSPAN, and others, instead of placing sensors in each remote segment.

Usability

Most existing tools have been developed with a focus on engineers, and are designed for advanced IT and SecOps experts. This makes adoption of these tools difficult, and the learning curve too steep. This in turn also affects your time to value.

In other cases, the tools are not flexible enough to fit into your organization's use case. Therefore, many advanced features remain unused and the money invested in these tools is wasted.

WHAT TO LOOK FOR

Ask if the solution's various capabilities are customizable to your organization. For example, check if they have customizable maps, rules, and allow users to add/disable data and features.

Be aware of the fact that some tools require advanced scripting and querying languages. This makes the product too complex and may make these tools unusable. Look for solutions that have an easy to use UX and UI and allow you to achieve data filtering and analysis without writing scripts and queries.

Look for solutions with a clear and straightforward UI. If you can't find your way around the different components during the evaluation phase, it will probably be difficult to successfully detect or respond to security incidents when it's in production

Scalability

Testing solutions in the lab is not the same as a production deployment, especially in large and complex networks. Performing traffic analysis on large amounts of data in many distributed locations can take a toll on local servers' memory, storage and CPU, as well as network bandwidth.

WHAT TO LOOK FOR

- Support for 'smart' sensors that can perform computation near the data source, so the solution will not overload the network with traffic sent between components.
- Ability to manage a large number of assets, in the tens of thousands from a single server, to reduce the number of managed components.
- Focus on capabilities that can deal with large amounts of data such as alert storm handling, data aging and more.
- Address throttling of data between system components to prevent uplinks overloading.
- Ability to collect data from remote locations without deploying sensors, but using network protocols such as NetFlow and others.

Integrations With Existing IT and Security Architecture

IT and OT networks are no longer separate entities. While OT needs its own security platform, it still needs to integrate with the IT side. Implementing an OT security solution as a separate "island" without the ability to share its notifications, or enrich other tools with its findings, is no longer an option in most organizations.

However, many times the integration aspect is handled as an afterthought. Prepare and validate a clear list of integration use cases before the project starts. Then make sure the use case you need can be handled by your chosen vendor.

For example, direct integration with enforcement tools such as firewalls, might not be the best practice. Instead, it is typically more efficient to integrate with a central SOAR tool.

WHAT TO LOOK FOR

- You need to find a solution that integrates seamlessly with other tools to create a solution for your specific use-case.
- A strong open API that can provide maximum flexibility rather than implementing canned integrations that many times are not suitable for real-life use cases.
- The ability for 2-way integration. Meaning, it can send out information, as well as receive data. This should include process related actions as well (such as alert closing) and proliferation of updates through all solution components (such as from central component to distributed sensors).

Customer Service

You never want to purchase a product from a vendor that considers the sale to be the end of the relationship. Every OT network is unique and you will likely need some customizations down the road. Work with a company that you will feel comfortable building a long term relationship with.

WHAT TO LOOK FOR

A vendor that provides close support during the project, and eager willingness to cooperate on adding value and support of new technologies

Managed Services Another Option For OT Security

If your organization is one of the many who are too short-staffed or your team lacks the specific training required to oversee OT security, you aren't alone. A recent survey commissioned by our research team revealed that 83% of cyber security professionals believe there are not enough qualified OT security experts to meet the demands of the marketplace. (Get an ungated copy of the survey here)

To assist your organization stay protected, SCADAfence offers a program of managed services for OT. Our OT experts deliver the expertise and technology to effectively control OT networks with visibility, risk management, and vulnerability detection. Your team will receive weekly updates and monthly reports and your personal analyst discusses the ramifications of the findings with you during scheduled calls.

Conclusion

Selecting the right OT security is a major decision with ramifications that will affect your entire organization. It's important to get buy-in from all the major stakeholders, from the board room, to the factory floor. As this buyer's guide explained,

the factors you need to consider when choosing an OT security solution include cost of deployment, length of time to deployment, integration with existing technologies, and minimizing the number of false positives so that you can use your OT security resources effectively.

Finding the right solution that will satisfy all your major requirements requires getting to know the OT security marketplace and learning what each has to offer.

The SCADAfence Platform is the most highly-awarded OT security solution currently available, and offers the shortest time to value in today's market. SCADAfence was mentioned as an OT representative vendor by Gartner in their 2022 Market Guide For Operational Technology Security and our solution meets the majority of the requirements they list as necessary for OT security.

SCADAfence
www.scadafence.com

About us

SCADAfence is the global technology leader in OT & IoT cyber security.
The SCADAfence platform enables organizations with complex OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and governance with minimal false-positives.
SCADAfence delivers proactive security and visibility to some of the world›s most complex OT networks, including the largest manufacturing facility in Europe.
SCADAfence enables organizations in manufacturing, building management and critical infrastructure industries to operate securely, reliably and efficiently. To learn more, visit our website, check out our blog, or follow us on Linkedin.

New York
122 Grand Street
New York, NY 10013
USA
+1-646-475-2173

Tokyo
5th Floor Nishida Bldg.
2-14-6 Shibuya
Shibuya-ku Tokyo 150-2000
Japan
+81-3-4588-5432

Dach Region
+49-89-2206-1175

Ramat Gan
2 Shoham St.
Ramat Gan, 5251003
Israel
+972-3-763-0785