An effective CPS ecosystem requires vendor products that naturally interoperate. Choose vendors with pre-existing integrations to save time and resources. This enables asset owners to focus on core business activities instead of perpetual integration maintenance.

With a robust CPS Security Ecosystem, asset owners and operators can achieve:

- Higher ROI on past projects
- Less technical debt through vendor cooperation
- Efficient tool integration across the enterprise
- Improved IT and OT tool utilization

Key Requirements for A Complete CPS Security Ecosystem

For risk mitigation, ensure your chosen ecosystem addresses these vital capabilities:

- **Comprehensive XIoT Asset Discovery and Visibility**
  
  CPS security ecosystems must start with identifying what XIoT assets are in the environment. This foundational step should be comprehensive and use a variety of discovery methods to really gain a complete and comprehensive inventory. The discovery tool should use passive discovery, use safe/active queries and be capable of parsing ICS app databases. Finally, the visibility vendor must be able to deeply parse a wide diversity of industrial protocols to be valuable to most asset owners whose production processes typically include a wide variety of automation vendors.

- **Native to your Digital Transformation SaaS Platform**
  
  Digital Transformation is driving IT and OT convergence and is leading to more and more connectivity between industrial equipment and the cloud. As asset owners reduce costs and increase productivity in their production environments, further synergy can be found by leveraging CPS ecosystems that include integrations between the CPS platform and the Digital Transformation platform.

- **Bidirectional Endpoint Protection Integration**
  
  CPS Security should integrate with endpoint protection covering both IT and OT. Asset owners must extend existing endpoint protection to production areas, as many OT devices are vulnerable to
ransomware near network perimeters. A compromise can halt production, so look for an endpoint security player that specifically deploys to production environments. Opt for a system allowing bi-directional data sharing between endpoint and CPS platforms to optimize ROI.

✅ **Next Generation Firewall Integration**

Network segmentation is a key use case to apply protection and lock-down how data flows across the XIoT landscape. Look for an ecosystem that includes the ability to integrate with a next-generation firewall to share group and device attribute data that can simplify the generation of important network policies to limit inappropriate data access.

✅ **Network Access Control Integration**

Access Control Lists on switches are another important way that data and production processes can be protected. Seek ecosystems which include NAC policy generation capabilities between the CPS platform and the NAC tools as these will be able to directly impact the ability for devices to appropriately communicate in a controlled fashion.

✅ **System Information and Event Management Integration**

For an effective CPS security ecosystem, SIEM integration is crucial. SIEMs aggregate log data for real-time threat analysis. By linking CPS with SIEM, asset owners unify security monitoring across IT and OT, enhancing existing SOC investments. This integration swiftly detects and mitigates threats, minimizing disruptions. Choose a SIEM capable of ingesting data from your CPS security platform for precise, tailored alerting in complex production settings.

✅ **Workflow Management Integration**

Most asset owners have already invested in important workflow management systems to optimize and improve process efficiencies. By finding ecosystems that integrate with workflow management tools, asset owners can leverage those existing capabilities and extend their usage across IT and XIoT domains. Additionally, vulnerabilities can be managed across the entire enterprise in one place when the data integrations already exist.

**The Bottom Line: Save Money, Improve ROI**

By selecting an ecosystem with full asset discovery, SaaS integrations, next-gen firewall and NAC integrations, SIEM and workflow management integrations, asset owners can manage risks more effectively across the entire IT and XIoT landscape. These integrations enable a more complete Security Operations Center to manage risk across the enterprise.

**About Claroty**

Claroty empowers industrial, healthcare, commercial, and public sector organizations to secure all cyber-physical systems in their environments: the Extended Internet of Things (XIoT). The company’s unified platform integrates with customers’ existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, network protection, threat detection, and secure remote access.

Backed by the world’s largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

For more information, visit claroty.com or email contact@claroty.com.