Why Our Proven OT Security Expertise Matters

Executive Summary

Technological tools and network systems developments often change more rapidly than a company's strategic approach to operating technology (OT) security. Remote work environments and bad actors that are becoming more and more sophisticated, and they're bringing high-risk elements to the OT protection table. Many organizations face daunting challenges in choosing the right solutions. OT connections to Information Technology (IT) systems create new environments with varying degrees of vulnerability. Security of the highest order and efficiency are of paramount importance, and the the critical component to all of this is breach prevention. Savvy leaders are becoming more proactive in protecting critical assets, and the right expertise can make all the difference. Gartner©conducts deep analyses to identify the most qualified and efficient professionals and products, and Blue Ridge Networks in numbered among them.

Cyber attacks on the ISP/MSP sector increased by 67% in 2021.[1]

The OT Security Decision Journey

Agency and corporate leaders juggle competing urgent priorities at blinding speeds, often struggling with the debate among business units and teams within their organizations around critical budget dollars. Weighing the financial impacts of the bottom line doesn't come easy, and the allotment of finances requires deep exploration and justification of the Return on Investment (ROI).

It is critical for these leaders to understand that a proactive approach to breach prevention on the front end will help them to avoid huge recovery costs on the back end in response to a breach event. But what company or service should they select and why? Gartner©, the leading trusted industry research firm is considered by many organizations to be the gold standard "Go To" resource for finding and choosing the best solutions for a wide variety of industrial, regulated, and commercial entities. Gartner©has recognized Blue Ridge Networks as a representative vendor for OT security.
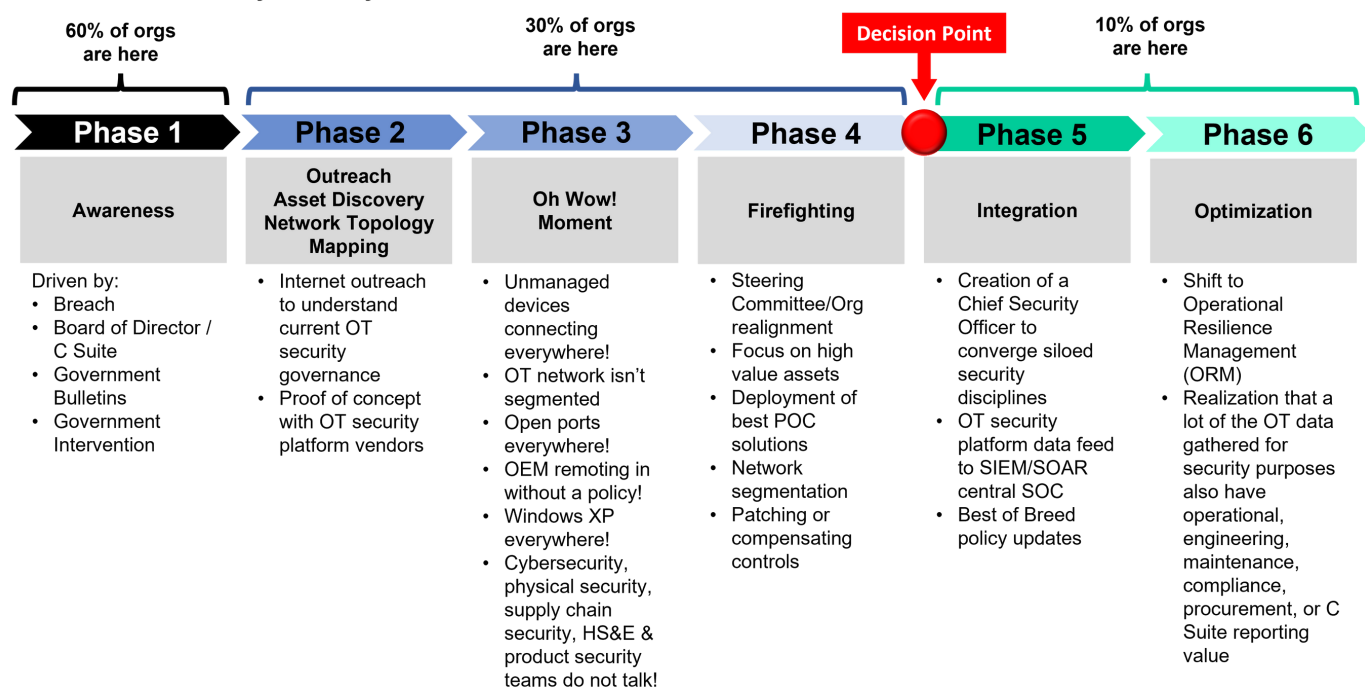
Where Are You in the OT Security Decision Journey?

The good news is that a vast majority of organizations are progressing past the initial Awareness phase, and are actively researching their OT security options while considering how to match them to their respective network infrastructures and financial resources. The bad news is that the inspiration to move forward in this journey most likely originated with and attack, or a breach event, or pressure from a leadership body.

The next steps involve deep dives into vendor viability and experience, which can reveal new problems and challenges that the organization never knew existed. As reflected in the image below, each phase of the journey leads to considerations that require resources and time.

The OT/CPS Security Journey [2]

60% of orgs are here	**30% of orgs are here**		**Decision Point**	**10% of orgs are here**	
Phase 1	**Phase 2**	**Phase 3**	**Phase 4**	**Phase 5**	**Phase 6**
Awareness	**Outreach Asset Discovery Network Topology Mapping**	**Oh Wow! Moment**	**Firefighting**	**Integration**	**Optimization**
Driven by: • Breach • Board of Director / C Suite • Government Bulletins • Government Intervention	• Internet outreach to understand current OT security governance • Proof of concept with OT security platform vendors	• Unmanaged devices connecting everywhere! • OT network isn't segmented • Open ports everywhere! • OEM remoting in without a policy! • Windows XP everywhere! • Cybersecurity, physical security, supply chain security, HS&E & product security teams do not talk!	• Steering Committee/Org realignment • Focus on high value assets • Deployment of best POC solutions • Network segmentation • Patching or compensating controls	• Creation of a Chief Security Officer to converge siloed security disciplines • OT security platform data feed to SIEM/SOAR central SOC • Best of Breed policy updates	• Shift to Operational Resilience Management (ORM) • Realization that a lot of the OT data gathered for security purposes also have operational, engineering, maintenance, compliance, procurement, or C Suite reporting value

We're Here to Help

Trust Blue Ridge Networks as an expert in the OT security space. Our guidance will ensure the comprehensive protection of your critical network operations and infrastructure. Benefit from results such as continuous cost savings while protecting sensitive information, securing critical assets, and ultimately improving operational efficiency upon eliminating the risk of disruptions.

1. "Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats," Forbes, January 21, 2022
2. "Market Guide for Operational Technology Security," Gartner, Inc., August 4, 2022

BLUERIDGE®

N E T W O R K S

Connect with Blue Ridge

📞 800-722-1168

✉️ sales@blueridgenetworks.com

🌐 www.blueridgenetworks.com

About Us

Blue Ridge Networks is a proven and trusted provider of cybersecurity breach prevention solutions. Our mission is to provide proactive protection of critical infrastructure that eliminates the adverse impacts associated with reactive responses to compromises. Our unique CyberCloak capabilities secure critical assets and operations in zero-trust IT/OT network architectures. Regulated, Commercial, and Industrial organizations have trusted Blue Ridge Networks for over 20 years to prevent exploits and receive continuous returns on their investments while achieving uninterrupted operational efficiency.