CASE STUDY

Securing Critical Glass Manufacturing Operations with the Dragos Platform

Protecting Industrial Glass Production Through Advanced OT Cybersecurity

Guardian Glass transformed their operational technology (OT) security posture with the Dragos Platform, gaining visibility into their complex manufacturing environment while maintaining the operational stability critical to their business success. This case study illustrates the critical importance of OT-native cybersecurity solutions that understand the unique requirements of industrial environments where safety, stability, and continuous operation are paramount.

Guardian Glass is a leading manufacturer of glass products, operating float glass plants where glass is continuously formed in one of the most complex industrial environments imaginable. Consider a massive sheet of glass continuously formed on the surface of a swimming pool-sized vessel filled with molten metal, heated to thousands of degrees, transported on a layer of tin down a cooling line until it solidifies enough to be cut and transported.

GUARDIAN® GLASS

1932
Founded in 1932, Guardian Glass is one of the largest glass manufacturers in the world

160
countries served across 5 continents

500KM
of float glass produced each day

24
float glass lines worldwide

700
different Guardian Glass products

While safety is Guardian's top priority, operational resiliency and uptime are also critical to business success. In this environment, starting and stopping production is not only time-consuming but incredibly costly. Considering this, Guardian Glass recognized the opportunity to improve their OT cybersecurity.

The Challenge: Securing Complex OT Environments

Guardian Glass, like many industrial manufacturers, operates in two distinct technological worlds:

Information Technology (IT)

- Prioritizes confidentiality, agility, and user experience
- Uses well-known protocols (HTTP, SSH, RDP)
- Exposed to many actors across various networks
- Experiences frequent but typically low-impact cyber incidents

Operational Technology (OT)

- Above all, prioritizes safety, stability, and availability
- Uses specialized industrial protocols (Modbus, Profinet, etc.)
- Limited to essential personnel and tightly controlled networks
- Fewer incidents, but with potentially catastrophic consequences

For Guardian Glass, any disruption to their OT environment could result in production shutdowns, safety hazards, and significant financial losses.

The Challenge: Securing Complex OT Environments

Guardian Glass chose the Dragos Platform to gain comprehensive visibility into their OT network assets and threat activity. Improved visibility into their OT environments would significantly reduce risk by enabling faster, more informed responses to cybersecurity events.

Key Platform Capabilities That Appealed to Guardian Glass

- **Passive Monitoring Designed for OT.** "Prior to using Dragos, Guardian had no tooling that helped us find assets without impacting the environment." — Mark Smillie, Guardian CISO

  The Dragos Platform's passive monitoring approach was crucial for this sensitive production environment, allowing Guardian Glass complete network visibility without risking operational disruption.

- **OT Watch Threat Hunting Service.** Dragos's specialized OT Watch service provides industry-specific threat hunting and continuous monitoring, delivered by experts who understand the unique challenges of industrial control systems.

- **Expert Onboarding and Support.** Dragos was highly engaged throughout the implementation process, providing valuable feedback based on their unique expertise and experience in OT environments.

Measurable Business Outcomes

Improved Capital Investment Planning

By gaining visibility into sub-assets on the network, Guardian Glass is able to quickly assess the age and firmware of manufacturing devices, which drives a faster turnaround time and enables better capital investment decisions.

Discovery of Unknown Security Risks

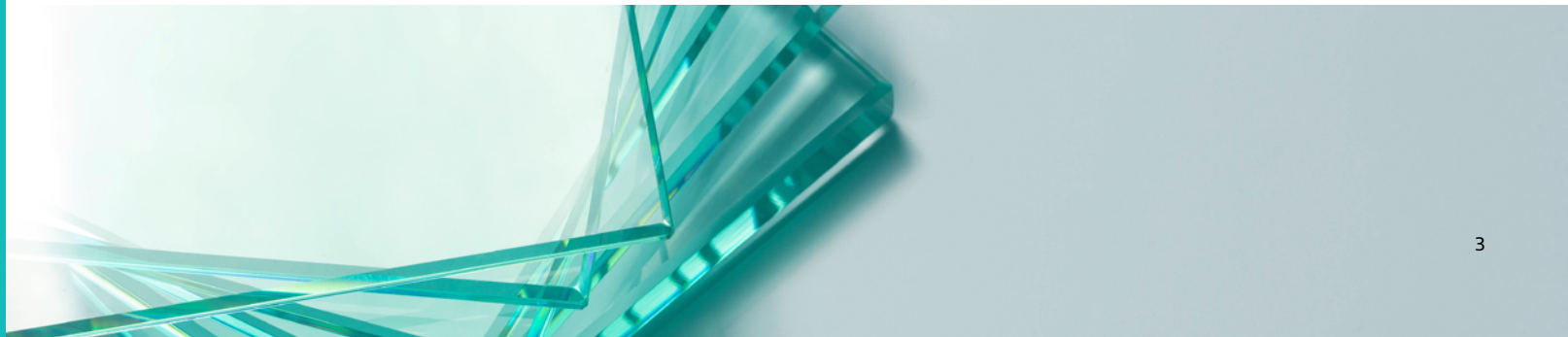
The Dragos Platform revealed critical security gaps that Guardian Glass didn't know existed:

> Dragos provided visibility to high-risk devices, devices we didn't expect to see, 4G remote access devices we didn't realize our suppliers had put on our network.
>
> **Mark Smillie • Guardian CISO**

Enhanced Security Posture

The Dragos Platform identified multiple areas for improvement:

- Gaps in system documentation
- Protocols that were enabled that shouldn't have been
- Devices where access credentials were unknown or outdated



Why This Matters

The success Guardian Glass has seen with the Dragos Platform demonstrates how proper OT cybersecurity can deliver both security and operational benefits with returns observed across the organization. By gaining complete visibility into their network without disrupting critical processes, they've not only reduced cybersecurity risk but also optimized their maintenance strategies and discovered cost-saving opportunities.

Ready to Transform Your OT Security?

Discover how the Dragos Platform can provide the visibility and protection your infrastructure needs without compromising operational stability. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us.**

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.