Cyolo

At a Glance

Empowering the Energy & Utilities Industry with Safe and Secure Access

Cyolo PRO for Energy & Utilities

Energy and electricity are essential services that we rely on to power our homes and businesses, fuel our transportation systems, provide crucial medical services, and much more. Unfortunately, an increasing number of adversaries also recognize the value of the Energy & Utilities sector. These threat actors are acclerating their attacks on operational technology (OT) in order to disrupt operations, commit cyber-terrorism, and generally wreak havoc.

Protecting the industry from cyberattacks is crucial for several key reasons:

Energy Infrastructure is Critical Infrastructure: Energy infrastructure is considered critical infrastructure because the economy, as well as the safety and health of citizens, depends on the reliable delivery of power and energy. Cyberattacks can lead to extremely serious power and energy supply disruptions, and the consequences can be dire – with the potential for severe economic losses, damage to infrastructure, and even loss of life. Power and energy are so essential that infrastructure vulnerabilities can be considered a matter of national security.

Extreme Financial Risk: Successful cyberattacks are very expensive, and costs are only rising. The average cost of a data breach in the Energy & Utilities industry climbed to $4.78M in 2023, according to IBM. The financial fallout following a security incident includes not just the cost of resolving the attack but also losses due downtime, regulatory fines, and reputational damage.

70%

of energy & utilities organizations are currently pursuing some level of IT/OT convergence.

Ponemon Institute, 2024

Regulatory Pressures: The Energy & Utilities sector is one of the most heavily regulated industries in the world. As a result, organizations are under intense scrutiny, and failure to comply with industry, regional, and national regulations can result in heavy fines and penalties. NERC CIP in North America and the NIS2 Directive in the European Union are just two examples of relevant regulations.

Rising Complexity: The cyberthreat landscape is growing in complexity. Organizations in the Energy & Utilities space must contend with increasingly sophisticated threats as well as geopolitical uncertainties that can send risk skyrocketing. These same organizations also bear the brunt of the responsibility for decarbonizing and enabling a successful energy transition. This means accommodating more complex connections to the power grid and energy infrastructure, all while navigating a dynamic regulatory and policy landscape and minimizing risks to safety and security.

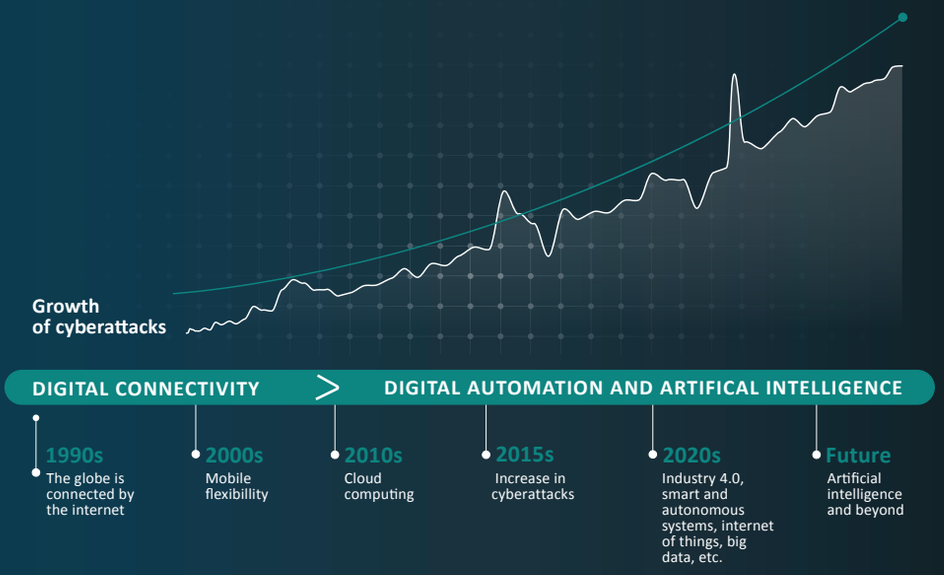
Against this backdrop, remote work, automation, progress toward Industry 4.0, and rising connectivity between OT and information technology (IT) are creating new opportunities as well as new vulnerabilities across the Energy & Utilities industry. Remote connectivity, as one example, reduces costs, improves operational agility, and lowers safety risks by enabling maintenance on power lines or the electrical grid to be conducted without traveling to distant or potentially dangerous locations. However, remote access creates its own security and safety risks that must be contained with the proper access, connectivity, and supervisory controls.

Cyolo PRO (Privileged Remote Operations) is an advanced Secure Remote Access solution designed to enable organizations in the Energy & Utilities industry to safely connect remote workers, third-party vendors, and privileged employees to even the most sensitive assets and environments.

Energy & Utilities Security Risks

The Energy & Utilities industry is deeply dependent on systems that are becoming more digitally connected. Connectivity lowers costs, increases efficiency, and decarbonizes the sector, but it also introduces new risks.

Robust cybersecurity will enable companies to fully enjoy the benefits of digital transformation and IT/OT convergence. But there is work to do, as 48% of of power and utilities CEOs said they believe a cyberattack is "inevitable."



Source: World Economic Forum

Energy Cybersecurity by the Numbers

42% of energy professionals think their organization's current level of investment in cybersecurity is sufficient to ensure the resilience of their operational assets and infrastructure.

78% of energy professionals report that geopolitical uncertainty has increased their awareness of potential OT vulnerabilities.

89% of energy professionals believe cybersecurity to be a pre-requisite for digital transformation.

38% of energy professionals identify the lack of in-house cybersecurity skills as the most intractable barrier to maturity in the industry.

Source: DNV, 2023

Case Study: How a Leading Energy Provider Ensures Secure Access to OT and SCADA Systems

The Need: Remotely connect global partners and third-party suppliers to critical systems

Top Challenges

- Required a single solution to enable secure access for global support teams, third-party suppliers, and customers
- Needed to meet strict internal and external security regulations
- Sought to reduce friction and improve user experience for frustrated employees and support teams

Business Outcomes

- Fastest deployment in company history
- Fast, secure, and seamless access for all users to IT, OT, and SCADA systems
- Months of work reduced to hours
- Hundreds of thosands of dollars saved, plus significantly reduced travel costs
- Improved productivity and user satisfaction

"No solution gives me as much conrol and security as Cyolo. It's everything I need in one solution."

Shlomo Kamilyan
CIO, Rapac Energy

Multiple Needs, 3 Security Layers , 1 Unified Solution

PRIVILEGED ACCESS

- Safeguard Credentials → Vault
- Establish Audit Trail → Session Audit & Recording
- Track Privileged Activities → Intelligent Supervised Access

IDENTITY MODERNIZATION

- Protect the Last Mile → Zero Trust for Devices
- OpEx Reduction → End User Self-operation Tools
- Device Security → Internal IDP/MFA/SSO for Legacy Systems

ZERO TRUST SECURITY

- Mitigate Asset Vulnerabilities → Application Security
- Mitigate Risk of Phishing Attacks & Ransomware → Zero Trust for Users
- Implement Robust Access Controls → Access & Action Management

THE OUTCOMES

- Advanced Security
- Improved User Experience
- Operational and Power Grid Safety
- Reduction of Compliance Headaches
- Increased Production Reduced Cost & Complexity
- Enterprise-ready Deployment

Managing Access and Risk in Energy & Utilities Companies

48% **Failure to prioritize OT security.** Less than half (48%) of energy & utilities companies identify securing access to OT environments as a high priority.

74% **No accurate asset inventory. 74%** of energy & utilities companies do not maintain an accurate, up-to-date inventory of the industrial assets in their OT environments.

43% **Underprotected. 43%** of energy & utilities companies lack confidence that they're effectively protecting their OT environments.

60% **Insecure OEM Vendor and Third-Party Access. 60%** of energy & utilities companies grant OT systems access to more than 50 different vendors, and 21% give such access to more than 100 vendors.

Source: Ponemon Institute, 2024

Key Remote Privileged Access Use Cases

Facilitate Third-Party Remote Access

Safely connect third parties to your OT environments for enhanced productivity.

Provide OEM Access For Fast, Secure Support

Ensure rapid, secure, and safe support and maintenance for your factory floor and OT environments.

Manage Critical and Risky Access

Secure all access points to your mission-critical assets, whether on-prem or remote.

Achieve Regulatory Compliance

Implement segmentation, supervision and other requirements of industry and regional compliance mandates.

5 Critical Controls

For World-class OT Cybersecurity

- **ICS Incident Response**
- **Defensible Architecture**
- **ICS Network Visibility Monitoring**
- **Remote Access Security**
- **Risk-based Vulnerability Management**

Source: SANS Institute

The Cyolo Ecosystem Addresses All 5 Critical Cybersecurity Controls

Case Study: The Cyolo/Dragos Partnership

Together, Cyolo and Dragos deliver a comprehensive ICS/OT security framework based on the five critical controls of effective ICS/OT security:

ICS Incident Response - which integrates operational insights into incident handling, enhancing system integrity and recovery (Dragos)

Defensible Architecture - ensuring robust visibility, segmentation, and enforcement mechanisms to bridge technological and human aspects of security (Dragos and Cyolo PRO)

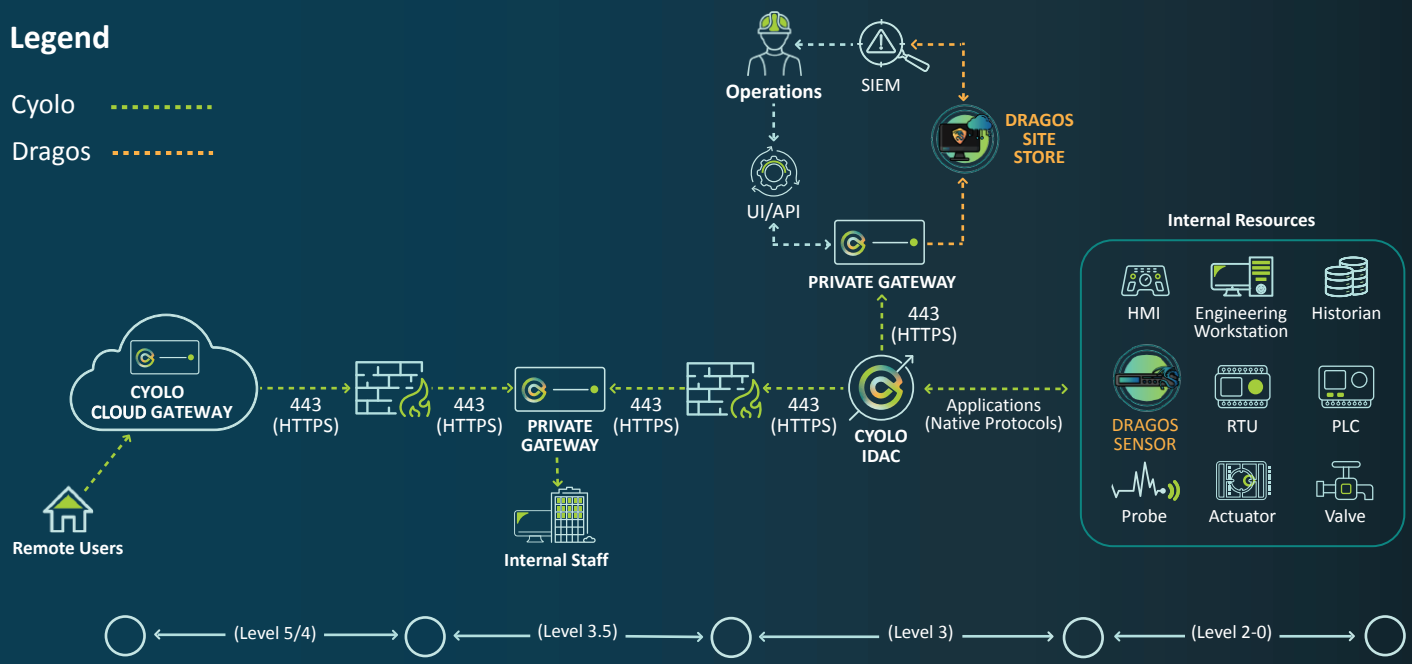
ICS Network Visibility Monitoring - employing continuous monitoring and protocol-aware tools to detect and address potential vulnerabilities (Dragos)

Remote Access Security - ensuring safe and secure stringent access control in the face of evolving hybrid work environments (Cyolo PRO)

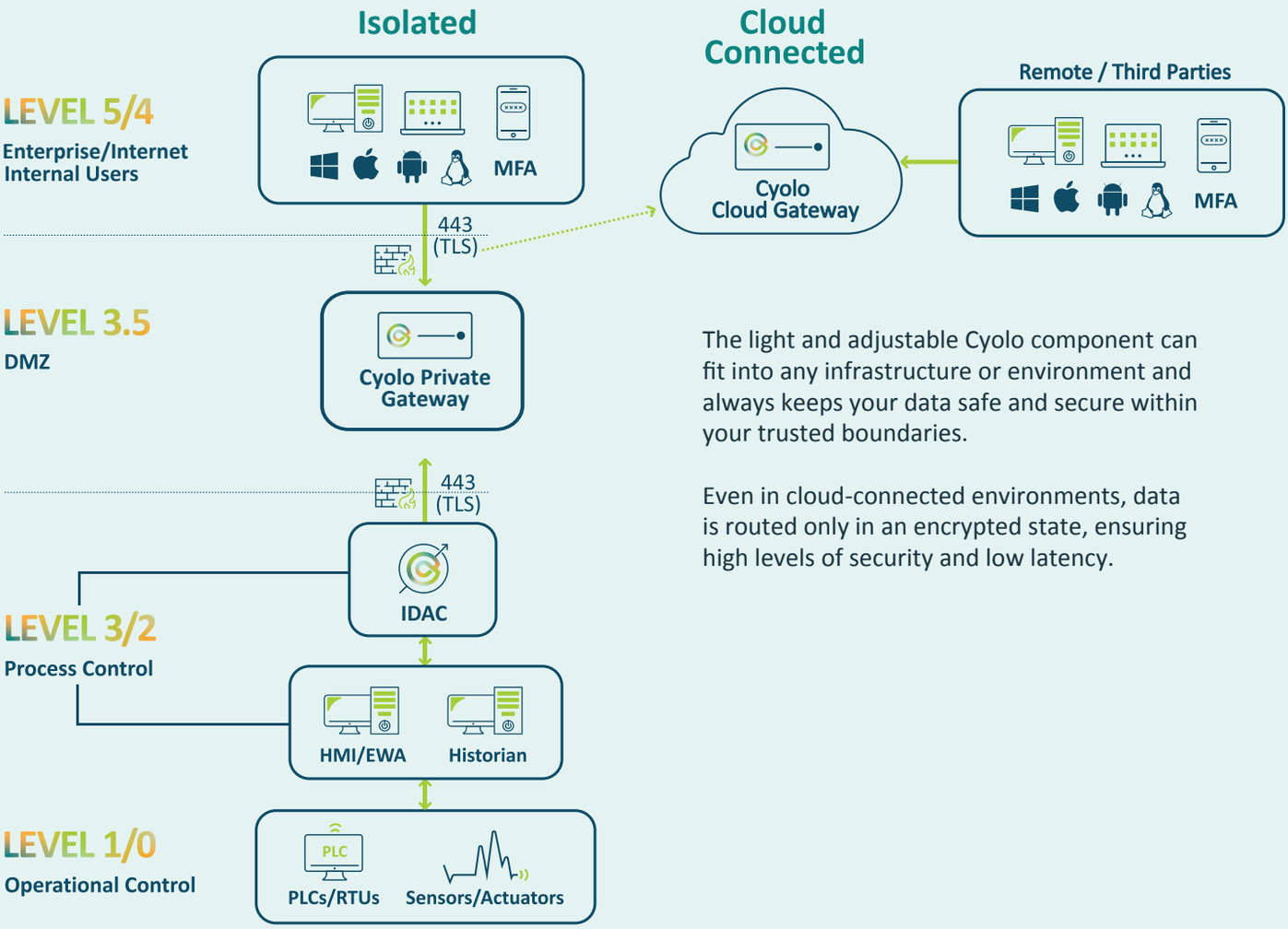
Risk-based Vulnerability Management - prioritizing and addressing vulnerabilities based on their potential to pose significant operational risks, thereby ensuring proactive prevention, response, and recovery actions (Dragos and Cyolo PRO)

UNIFIED INDUSTRIAL CYBERSECURITY CONTROL

HOW IT WORKS



Cyolo PRO's Unique Architecture Enables a Flexible Solution to Fit Any Environment



The light and adjustable Cyolo component can fit into any infrastructure or environment and always keeps your data safe and secure within your trusted boundaries.

Even in cloud-connected environments, data is routed only in an encrypted state, ensuring high levels of security and low latency.

Cyolo PRO Benefits

Secure

- Keep your data inside your trusted boundaries
- Granular identity-based controls & supervision
- Full activity/audit trails

Flexible

- Deploy on-prem, on-cloud & hybrid—simultaneously
- Extend identity authentication and security to legacy applications
- Centralized governance & site-based administration

Fast and Easy

- Agentless deployment
- Consolidated access controls with modularity
- Low-latency/High-availability
- Intelligent supervision eases operational burden

Cyolo is a leading cybersecurity innovator dedicated to simplifying secure remote access for critical industries. With a focus on security, agility, and user experience, Cyolo enables safe operations, uninterrupted productivity, and compliance-readiness.

www.cyolo.io

Cyolo