

Cyolo PRO (Privileged Remote Operations) Live Risk Detection

Detect Risk Before a Remote Session Becomes an Incident

As remote connectivity expands, more employees, vendors, and third parties need access to critical systems, increasing the volume of activity security and operations teams need to oversee. But manually monitoring every session and action simply isn't practical.

Live Risk Detection, an AI-powered capability of the Cyolo PRO access solution, adds intelligent, real-time supervision to **active user sessions**. Context-aware AI continuously evaluates activity as it unfolds, identifying cyber threats, operational risks, and unexpected behavior that warrant attention. When risk is detected, relevant teams are alerted immediately so they can investigate and intervene before critical systems or operations are impacted.

Understand Risk in Real Time

Identify suspicious, dangerous, or unexpected behavior as it happens.

Act When It Matters

Give teams the details they need to investigate and intervene while the session is still active.

Scale Session Oversight

Extend oversight across more sessions while helping teams prioritize where attention is needed.

Intelligent Oversight at Scale

The Benefits of Context-Aware Supervision

Add Context to Every Action

Evaluate each action in the context of the user, task, and session to identify behavior that may appear harmless on its own but signals risk in context.

Reduce Cyber and Operational Risk

Identify both security threats and unsafe actions that could put critical assets, processes, or operations at risk.

Pair AI Insight with Human Control

AI surfaces potential risk and provides context, while security and operations teams decide whether and how to intervene.

Enhance Protection for Third-Party Access

Apply an additional layer of supervision to vendor and third-party sessions involving critical assets.

Cyolo PRO Live Risk Detection

Live Risk Detection flags potentially risky activity in real time, including:



Risky Commands

Commands or configuration changes that could disrupt critical systems or operations.



Attempted Lateral Movement

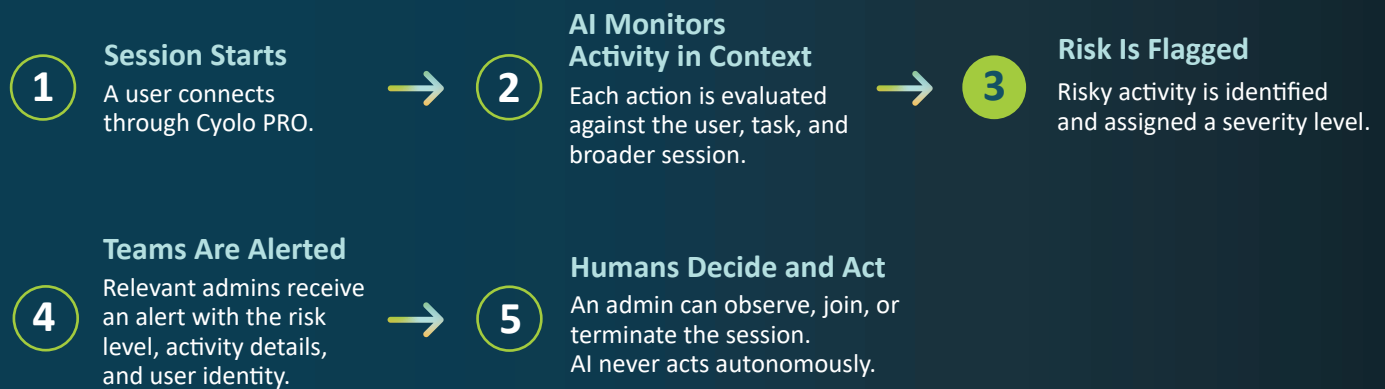
Attempts to reach systems or resources outside the user's approved scope.



Out-of-Context Actions

Activity that doesn't align with the user's expected task, role, or session.

How Live Risk Detection Works



Zero Trust Doesn't End at Login

Live Risk Detection brings the principles of Zero Trust into the active session. Identity verification and strong access controls provide the foundation for secure remote access. Live Risk Detection builds on these protections by monitoring what happens next, helping teams recognize and respond when risk emerges during the session.



Built for Real-World Use

Live Risk Detection combines flexible controls, existing security workflows, and privacy-conscious monitoring to fit the needs of operational environments.



Context-Aware Analysis

Evaluate actions based on the user's task and overall session, rather than in isolation.



Adjustable Risk Sensitivity

Evaluate actions based on the user's task and overall session, rather than in isolation.



SOC-Ready Alerts

Alert relevant teams to detected risk and stream activity logs to the SOC.



Privacy by Design

Monitor activity only within the working session, never on the user's endpoint or device.



Mask Sensitive Details

Remove sensitive information, such as passwords, from session records.



Broad Protocol Support

Support web RDP, native RDP, and VNC sessions.

Cyolo secures every connection across critical infrastructure and operational technology (OT) with a full-stack Secure Connectivity Platform that unifies remote privileged access and zero trust microsegmentation. Leading manufacturers, utilities, and data centers rely on Cyolo for surprisingly simple secure connectivity.