Precisely + Illumio

Strengthen IBM i security with visibility, segmentation, and breach containment

Overview

Organizations running IBM i systems face a rapidly evolving cyber threat landscape. These platforms rarely operate in isolation — they're deeply connected to applications, users, and networks across hybrid and multi-cloud environments. Every connection point is a potential pathway for attackers.

Traditional perimeter defenses can't stop lateral movement once a threat gains entry. That's why microsegmentation is critical. Together, Precisely Assure Security and Illumio give you the visibility and policy enforcement needed to contain breaches before they spread — protecting critical IBM i data and ensuring cyber resilience.

Integration Highlights

- Support for Precisely Assure Security – System Access Manager module with Illumio provides network visibility and enforcement.
- Enforce allow/deny policies directly on IBM i to stop unauthorized traffic from communicating. Pre-built dashboards to identify risks and provide insight into IBM i communications.
- Automate segmentation across hybrid and multi-cloud environments, reducing reliance on specialized IBM i expertise.
- Strengthen compliance posture by applying consistent policies aligned with Zero Trust principles.

How Precisely + Illumio Help You Stay Secure

Spot breaches before they spread

With real-time visibility into IBM i communications, you can quickly identify unusual or unauthorized activity. Pre-built dashboards make it easy to spot risks early and act before they escalate.

Reduce insider risk

Whether malicious or accidental, insider activity is one of the hardest threats to defend against. By applying precise segmentation policies, you reduce exposure to misconfigurations, data exfiltration, or misuse.

Enforce granular access policies

Only the right traffic gets through. Illumio-driven rules let you approve or deny lateral communications with precision, ensuring critical workloads and sensitive data stay locked down.

Contain attacks with segmentation

Even if a breach occurs, microsegmentation limits attackers from moving laterally. Services and systems are isolated unless communication is explicitly allowed — minimizing impact and preserving business continuity.

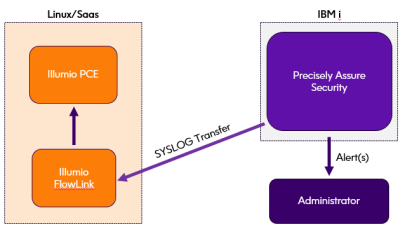
Benefits

- Enhanced Transparency – Gain a clear view of how systems are communicating across environments, quickly spot unusual or unauthorized activity, and address risks early.
- Stronger Lateral Security – Limit the spread of threats by applying precise, enforceable network policies to IBM i traffic.
- Fortified Access Control – Ensure only authorized traffic reaches critical systems and sensitive data.
- Centralized Policy Management – Define and enforce segmentation policies across all IBM i systems from one centralized solution.
- Faster Containment – Reduce dwell time by detecting and containing threats before they escalate into business disruptions.

Keep your IBM i secure and resilient

With Precisely and Illumio, you can extend Zero Trust principles to IBM i, contain lateral threats, and protect your most critical systems from modern threats — without adding complexity or sacrificing performance.

How it works: Traffic flow from IBM i to Illumio



How it works: Illumio ACL File Import