1. Motivation

- “God, root, what’s the difference?”
- IT can steal valuable data
  E.g., Edward Snowden

2. Contributions

- Strategy for protecting organizations from IT threats.
- WatchIT: A proof of concept implementation.
- Case study on the IBM Research IT Department.

3. Perforated Container

- We introduce **Perforated Linux Container**
  - Like Linux container
  - Punched isolation
  - Shares resources with the host

- Example: license issue
  - Isolated network, filesystem, processes
  - Access license server; home directory

4. WatchIT Work-Flow

5. P-Container as a Sandbox

6. Case Study

**IBM Research IT Department**
- ~16,000 trouble tickets
- Topic modeling – 10 classes