Call Centers: Beware of These 17 Employee Behavior Red Flags

Call centers are, from a security standpoint, one of the riskiest areas of the enterprise. Like any branch of an organization, call centers are susceptible to malware, APT, and other security threats. But there's one security concern that call centers need to pay extra special attention to: the insider threat.

There are two keys to defeating the insider threat: knowledge and visibility. By keeping an eye on your employee behavior, you can stop the insider threat before it begins. Here's 17 red flags to watch out for in your employees' behavior.

- ❑ **Unusual rate of copying/moving files to a local machine**
- ❑ **Unusual rate of copying/moving files between servers**
- ❑ **Unusual rate of copying/moving files to USB drives**
- ❑ **Unusual rate of writing files to CD/DVD drives**
- ❑ **Printing sensitive data to networked printers**
- ❑ **Printing sensitive data to a local printer**
- ❑ **Upload to cloud services from the corporate network**
- ❑ **Upload to personal webmail from the corporae network**
- ❑ **Copy and past sensitive data to a website**
- ❑ **Access The Onion Router (TOR)**
- ❑ **Unusual use of Incognito/Private Browsing mode**
- ❑ **Researching, installing, & using proxy bypass/VPN/tunneling**
- ❑ **Researching, installing, and using peer-to-peer applications**
- ❑ **Use of password-cracking applications to retrieve data**
- ❑ **Attempting to disable/tamper with controls (e.g. DLP)**
- ❑ **Unusual local admin activity (e.g. scripts, file activity)**
- ❑ **Machine performing local activity during ususual hours**