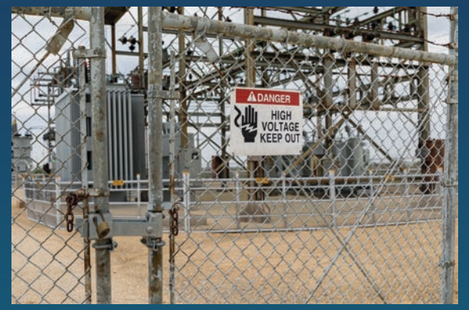
DYNAMIC AUDIT EVENTS

ENHANCED ACCOUNTABILITY FOR YOUR MOST IMPORTANT CYBERLOCK ACCESS POINTS

CyberLock®

8:14 AM

A trained maintenance technician for a local Power Utility needs to unlock a padlocked gate at a remote substation. From the intuitive user interface of CyberAudit-Web management software, the security manager at the Utility programs the technician's CyberKey smart key to access the CyberLock padlock securing the substation gate.



Due to the remote location, the unmanned substation does not have a cabled network connection. However, in response to a recent vandalism attack, the Utility has deployed surveillance cameras that use an onsite cellular router to transmit footage back to the Utility servers. One of the cameras is trained on the padlocked access gate. To further validate substation access, CyberLock's latest software enhancement module, Camera and NVR Integration, has been configured by the Utility's security manager to capture video footage of Access Granted events in CyberAudit-Web.

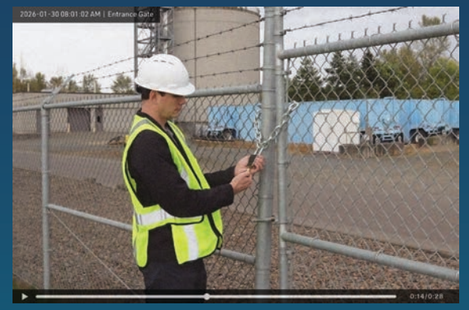
10:04 AM

At the substation, the technician uses the CyberKey smart key to unlock the padlocked gate, which stores a timestamped audit event record in both the CyberKey smart key and the CyberLock padlock. Meanwhile, the video data transmitted to the Utility servers from the gate camera includes the technician's access attempt.

8:08 AM

The following day, the technician's CyberKey has expired and must be synced with CyberAudit-Web to reactivate the key. During this reactivation process, the audit event record from the substation gate is uploaded to the CyberAudit-Web database. Since there was a camera associated with the substation gate, the Camera and NVR Integration module creates a Dynamic Audit Event that includes a snippet of the previous day's video footage when the substation gate was unlocked.

2:04 PM



During a security audit the following month, the auditor is reviewing access logs for the substation and asks the security manager how the Utility can be sure it was actually the trained technician that accessed the gate. Although the Utility's security protocols require all technicians to enter a unique PIN in order to activate their CyberKey, the security manager is able to quickly locate the Dynamic Audit Event in CyberAudit-Web and establish that the technician name listed in the audit trail is indeed the same technician visible in the Dynamic Audit Event video.