but it's no silver bullet. For example, many times the ransomware attack vector involves the employee's own machine, which holds the decryption keys for seamless day-to-day access. Furthermore, even if you happen to be attacked in a way other than through the machine that holds the keys, data encryption really only helps with the threat of exfiltration. It doesn't keep the bad guys from locking you out of your own data.

Even though there are no silver bullets, there is an arsenal. Along with the usual measures of user education and patching, we really need to talk about DAG (and related technology such as NetIQ Privileged Access Management (PAM) by OpenText for correcting the real problem of over exposure. Use of these technologies can significantly mitigate

As you move forward, you'll have a "building" with a data footprint like this: