Attackers don't break in. They log in.

Most modern cyberattacks don't start with malware.
They start with stolen or misused credentials.

THE NEW REALITY

Adversaries don't need to break your defenses when they can use your identities.

Trusted access is the new attack vector.

HOW IDENTITY ATTACKS HAPPEN

1. **Someone gets access**
   A password, token, or account is stolen.
2. **They look legitimate**
   Attackers log in using valid credentials.
3. **They gain more access**
   Permissions allow them to move deeper into systems.
4. **Damage happens**
   Data is stolen, systems are disrupted, and costs rise.

WHY THESE ATTACKS ARE HARD TO DETECT

- They use real accounts
- Activity often looks normal
- Traditional tools miss identity threats
- Damage may happen before alerts appear

WHAT ORGANIZATIONS NEED TO DO

- **Verify** — Know who has access.
- **Monitor** — Watch for unusual behavior.
- **Limit** — Remove unnecessary permissions.
- **Respond** — Act quickly when risk appears.

Every identity matters

The sooner you find risky access, the sooner you can stop an attack before it spreads.