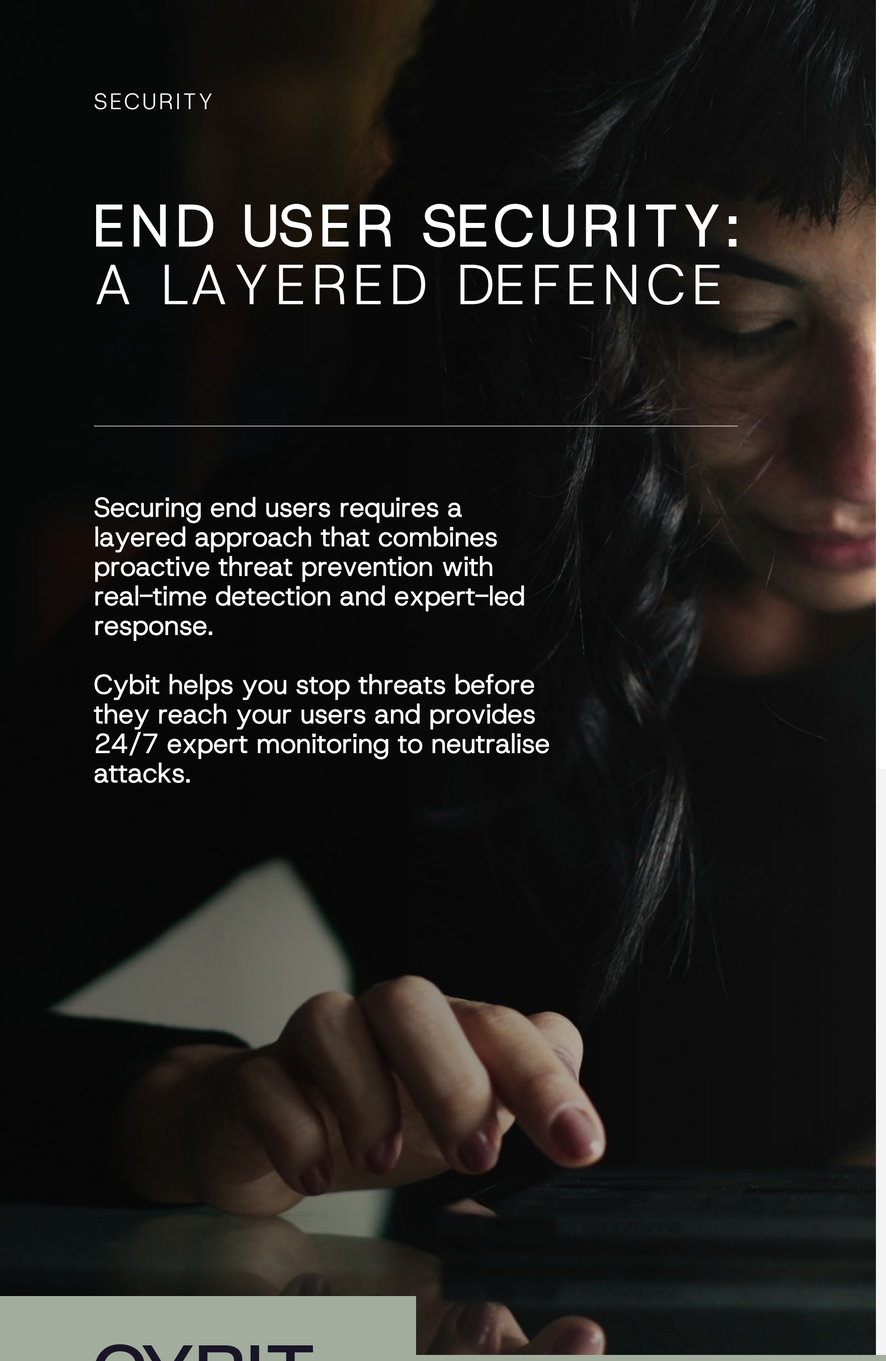

SECURITY

END USER SECURITY: A LAYERED DEFENCE

Securing end users requires a layered approach that combines proactive threat prevention with real-time detection and expert-led response.

Cybit helps you stop threats before they reach your users and provides 24/7 expert monitoring to neutralise attacks.

WHAT'S CHANGING & WHY IT MATTERS NOW

1. **Advanced Threat Landscape**
   Modern threats bypass traditional defences using sophisticated techniques like business email compromise and zero-day exploits.
2. **User-Targeted Attacks**
   Cybercriminals increasingly target end users through phishing, malware, and social engineering campaigns.
3. **Compliance Requirements**
   Regulatory frameworks demand robust email security and incident response capabilities.
4. **Remote Work Challenges**
   Distributed workforces require consistent protection regardless of location or device.

THE RISKS OF DOING NOTHING

! Successful phishing attacks leading to credential theft
! Malware infections spreading across networks
! Business email compromise causing financial losses
! Extended threat dwell time allowing attack escalation
! Regulatory non-compliance and associated penaltiesusing

LET'S MAKE YOUR SECURITY WORK SMARTER

Are you sure your security is protecting you from all angles? Cybit helps you:

Prevent email threats – with advanced filtering, sandboxing, and impersonation protection.

Gain 24/7 threat monitoring – from our Security Operations Centre (SOC).

Enable human-led threat hunting – to proactively find hidden indicators of compromise.

Integrate email and endpoint security – for a correlated, user-centric response.

WHY CYBIT?

- ✓ Layered Security E pertise across email protection and managed detection & response
- ✓ 24/7 SOC Operations with human-led threat hunting and incident response.
- ✓ An Integrated Approach combining email filtering with endpoint detection for a holistic view.
- ✓ Strategic, Proactive, and Compliance-Led supporting GDPR, HIPAA, & ISO 27001.

CYBIT