How to supplement Microsoft

Stronger together with HumanAI™ for zero-hour protection

- Microsoft provides basic email hygiene capabilities, including:
  - Blocking emails from known bad senders
  - Scanning attachments with AV and Safe Attachment sandboxing
  - Block emails with known bad URLs
  - Prevent access to known websites with Safe Links URL rewriting
  - Content analysis to identify spam
- Good base level email security but poor at advanced threat protection
- Recommends supplementing E3/E5 with email security solutions with relationship graphs, natural language processing, and computer vision ML capabilities to combat zero-hour threats

Stronger Together with SlashNext ICES

Zero-hour Protection With HumanAI™

Microsoft

- Sender blocklist contains known bad IPs and domains
- Email authentication reviews DMARC, SPF & DKIM auth results
- Safe Links rewritten URLs against known URL threat DB at time-of-click
- Safe Attachments sandbox files for malicious codes

- ✓ Cloud native & purpose built for Microsoft
- ✓ Zero-hour BEC protection
- ✓ Zero-hour credential phishing & link protection
- ✓ Zero-hour ransomware and file protection
- ✓ Spam and newsletter detection
- ✓ Comprehensive defense in depth protection with MS API integration
- ✓ 48-hour detection advantage
- ✓ Explainable threat insight for seamless investigation and response
- ✓ Security analytics integration w/ Microsoft Sentinel
- ✓ 360º protection across email, SMS/Mobile and browser

SLASHNEXT

- **Relationship and contextual analysis** detect unusual communication cadence and conversation style
- **Natural language process** detects topic, tone, emotion, intent, and manipulation triggers associated with BEC
- **BEC Generative AI** clones latest threats for ML training and detection
- **Live Scan™ Computer Vision** inspect webpages for visual deviations
- **Live Scan™ file inspection** scans for social engineering traits and malicious codes