SENTIS
Managed Solutions

Hybrid work vulnerability Checklist

Although most professional services leaders want teams physically together at least three days a week (to maintain the culture and detail diligence so vital to the sector), work from home days are here to stay.

But, while we've all been adapting to flexible business and the huge productivity advantages of hybrid, security vulnerabilities have become deep-rooted. These weak points – unique to hybrid workplaces – must be addressed, or data integrity, continuity and finances are under serious threat.

Use our checklist to confirm whether your professional services organisation has a robust hybrid security posture, or if reinforcements would be of benefit.

Online Safety

- [ ] Zero-trust VPNs are used for remote connections
- [ ] Password Multifactor Authentication is used on VPNs
- [ ] Web content filtering is active for all internet users
- [ ] PDNS and DMARC anti-phishing technology is used
- [ ] Email filtering and inspection is active for every inbox
- [ ] Application workload-based network segmentation is used

Data Protection

- [ ] Least-privileged access permissions are standard
- [ ] Cloud backups are active and regularly checked
- [ ] Document and endpoint backups are run daily
- [ ] Multifactor authentication is active at every access point
- [ ] Bitlocker drive encryption is active for every endpoint
- [ ] Compliant email archiving and discovery is active

Hardware Management

- [ ] Compliance and policy management tools are active on every endpoint
- [ ] Mobile devices have the equivalent perimeter security applied
- [ ] Distinct BYOD policies are enforced for mobile devices
- [ ] Hardware can be wiped remotely in the event of loss or theft

Collaboration

- [ ] Internal calls, messages, and files are encrypted
- [ ] External calls, messages, and files are encrypted, including call recordings
- [ ] Access permissions balance security with productivity
- [ ] Third-party integrations are audited and held to internal compliance standards
- [ ] MFA and vulnerability scanning are applied to collaboration apps
- [ ] SIEM software is active to moderate and monitor platform use

User Compliance

- [ ] Regular security awareness training is delivered with a hybrid or remote focus
- [ ] Browser-based threat simulation testing is active on all endpoints
- [ ] Distinct hybrid or remote worker security policies and support are in place

Threat Containment

- [ ] Timely patching is undertaken to mitigate hybrid vulnerability exploitation
- [ ] Advanced Threat Protection (ATP) is active on every resource and endpoint
- [ ] Threat Detection and Response, including SIEM and EDR is active
- [ ] Next-Generation Firewall is configured for hybrid vulnerabilities
- [ ] Clear incident response plans, processes, and technology are in place

SENTIS
Managed Solutions

Have we mentioned any unfamiliar terms or processes? Read our cybersecurity glossary as part of our Ransomware Survival Guide.

For help securing your hybrid workforce, arrange a free, no-obligation consultation with Sentis Managed Solutions. We're dedicated to helping leaders make better sense of technology to maximise the value it brings back into business.