

SCORING RUBRIC

SERVICE	RISK			Score	Mitigation Factor	Mitigation Score
	HIGH (1)	MEDIUM (2)	LOW (3)	(1-3)		
ENDPOINT	Not all devices using endpoint	All devices have AV but using legacy, signature based protection	All devices have a next-gen endpoint protection that can detect file-less attacks	x	4	=
EMAIL PROTECTION	Using standard spam filter	Some use of advanced spam filter	Using advanced email protection	x	4	=
2FA/SSO	No 2FA Policy	Some apps using 2FA and SSO	Most apps using 2FA and SSO	x	4	=
FIREWALL/IDS	Not Using firewalls at every site	Advanced firewalls but no IDS system	Advanced firewall and IDS	x	4	=
SECURITY MONITORING	Not being monitored by SOC	Network monitoring OR log monitoring from a SOC, but not both	Full network and log monitoring by SOC	x	4	=
BACKUP	No image based backups	Semi-regular image based backups of critical data	Regular image based backups of all critical data	x	3	=
PATCH MANAGEMENT	Not doing patch management	Only doing patch management for some servers	Fully enrolled in patch management	x	3	=
TRAINING	No cybersecurity training for employees	Semi-annual cybersecurity training for all employees	Annual cybersecurity training for all employees	x	3	=
PASSWORD POLICY	No password Policies	Some apps using robust password policy	All apps using robust password policy	x	2	=
THREAT INTEL	Not receiving threat intelligence	Sourcing your own threat intelligence	Receiving vetted threat intelligence from cybersecurity experts	x	2	=

RECOMMENDATIONS FOR IMPROVEMENT

SCORE KEY

- Below 70** : Danger Zone
- 70 - 90** : At-risk
- Over 90** : Safe Zone

TOTAL SCORE: