HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

365 4 TOTAL PROTECTION ET NIS2



Comment 365 Total Protection contribue-t-il à la conformité à NIS2 ?

Alors que les cybermenaces continuent d'évoluer, la directive NIS2 renforce les exigences en matière de gestion des risques de cybersécurité dans toute l'Union européenne. Elle met davantage l'accent sur la gouvernance, la résilience, la réponse aux incidents, la continuité des activités et la sensibilisation des collaborateurs. Pour répondre à ces exigences, les entreprises doivent adopter une approche globale combinant gouvernance, technologies, résilience et sensibilisation aux cyberrisques. **365 Total Protection peut accompagner les entreprises dans cette démarche en proposant des mesures de sécurité et des fonctionnalités liées à la conformité, en adéquation avec plusieurs exigences de la directive NIS2.**

HORNETSECURITY BY proofpoint.

INFOSHEET AI POWERED

DISPOSITION	CE QUE LE CLIENT DOIT METTRE EN PLACE	COMMENT LES PRODUITS PEUVENT AIDER	COMMENT 365 TOTAL PROTECTION CONTRIBUE	CORRESPONDANCE AVEC LES PILIERS DU NIST	DOMAINE NIS2
ARTICLE 20(1)	Les instances dirigeantes doivent approuver les mesures de gestion des risques de cybersécurité prises par l'entreprise afin de se conformer à l'article 21 et superviser leur mise en oeuvre.	Tableaux de bord de gouvernance, workflows d'approbation des contrôles, rapports destinés aux instances dirigeantes et dossiers de preuves.	Tableaux de bord du Control Panel	Gouvernance	Gestion risques de cybersécurité
			Tableaux de bord et vues d'audit de 365 Permission Manager		
			Historique des sauvegardes et restaurations de 365 Total Backup et approbation selon le principe des quatre yeux		
			État du Security Awareness Service et certificat de l'entreprise		
			Email live tracking		
			Journaux d'audit.		
ARTICLE 20(2)	Les instances dirigeantes doivent suivre une formation en cybersécurité, et les entreprises doivent proposer une formation similaire à leurs collaborateurs.	Plateformes de sensibilisation, suivi de la progression, attestations et formations adaptées aux rôles.	Modules d'e-learning du Security Awareness Service, simulations de spear phishing, courtes vidéos et quiz	Gouvernance	Gestion risques de cybersécurité
			Certificat annuel d'entreprise du Security Awareness Service		
ARTICLE 21(1)	Les entités concernées doivent mettre en place des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées afin de gérer les risques de cybersécurité.	Plateformes de contrôle centralisées, outils de gestion des risques, application des politiques et collecte de preuves.	Ensemble de contrôles combinés couvrant la sécurité des emails, le chiffrement, la continuité des activités, la sauvegarde, la gouvernance des autorisations et la sensibilisation : Spam & Malware Protection, Content control, Compliance filter, chiffrement global S/MIME/PGP, Websafe, Continuity Service, 365 Total Backup, 365 Permission Manager, Security Awareness Service, AI Recipient Validation et Teams Protection.	Gouvernance	Gestion risques de cybersécurité
ARTICLE 21(2)(A)	Politiques d'analyse des risques et de sécurité des systèmes d'information.	Outils de gestion des registres de risques, gestion du cycle de vie des politiques et mise en correspondance des contrôles de sécurité.	Règles personnalisées de Compliance filter	Gouvernance	Gestion risques de cybersécurité
			Politiques de conformité de 365 Permission Manager, réaudit récurrent automatique des accès précédemment approuvés et, prochainement, classification du niveau de gravité des risques		
			Email live tracking		
			Journaux d'audit		
			Vues du tableau de bord indiquant l'état de la conformité et des sauvegardes.		

DISPOSITION	CE QUE LE CLIENT DOIT METTRE EN PLACE	COMMENT LES PRODUITS PEUVENT AIDER	COMMENT 365 TOTAL PROTECTION CONTRIBUE	CORRESPONDANCE AVEC LES PILIERS DU NIST	DOMAINE NIS2
ARTICLE 21(2)(B)	Gestion des incidents.	SIEM/SOAR, gestion des incidents, playbooks et systèmes de ticketing.	Intégration avec les solutions SIEM et SOAR, soit de manière native, soit via des API Fonctionnalité native d'alertes et de surveillance dans le Control Panel.	Détecter / Réagir	Gestion risques de cybersécurité
ARTICLE 21(2)(C)	Continuité des activités, y compris la gestion des sauvegardes, la reprise après sinistre et la gestion de crise.	Orchestration des sauvegardes, tests de reprise après sinistre, planification de la continuité des activités et workflows de gestion de crise.	Email Continuity Service 365 Total Backup	Récupérer	Gestion risques de cybersécurité
ARTICLE 21(2)(D)	Sécurité de la chaîne d'approvisionnement, y compris les aspects de sécurité liés aux relations avec les fournisseurs directs et les prestataires de services.	Gestion des risques liés aux tiers, questionnaires destinés aux fournisseurs et surveillance continue des prestataires.	Contrôles du partage externe avec 365 Permission Manager, détection et correction des liens de partage, ainsi que détection des autorisations anormales AI Recipient Validation pour éviter toute perte accidentelle de données lors d'un envoi à un fournisseur ou à un prestataire de services Chiffrement des emails pour sécuriser les communications externes avec les fournisseurs et les prestataires de services.	Gouvernance	Gestion risques de cybersécurité
ARTICLE 21(2)(F)	Politiques et procédures visant à évaluer l'efficacité des mesures de gestion des risques de cybersécurité.	Tests des contrôles, conformité continue, preuves d'audit et tableaux de bord des KPI/KRI.	Tableaux de bord de conformité et journal d'activité de 365 Permission Manager État des sauvegardes, journal d'activité et historique des restaurations de 365 Total Backup Employee Security Index, statistiques et certificat annuel du Security Awareness Service Email live tracking et autres statistiques liées aux emails Journaux d'audit	Gouvernance	Gestion risques de cybersécurité
ARTICLE 21(2)(G)	Pratiques essentielles d'hygiène cyber et formation à la cybersécurité.	Sensibilisation à la cybersécurité, simulations de phishing, référentiels de bonnes pratiques d'hygiène cyber et contrôles de la posture de sécurité des terminaux.	Modules d'e-learning du Security Awareness Service, simulations de spear phishing, courtes vidéos et quiz Certificat annuel d'entreprise du Security Awareness Service.	Protéger	Gestion risques de cybersécurité
ARTICLE 21(2)(H)	Politiques et procédures relatives à la cryptographie et, le cas échéant, au chiffrement.	Gestion des clés, application des politiques de chiffrement et outils de gestion du cycle de vie des certificats.	Email encryption	Protéger	Gestion risques de cybersécurité

HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

DISPOSITION	CE QUE LE CLIENT DOIT METTRE EN PLACE	COMMENT LES PRODUITS PEUVENT AIDER	COMMENT 365 TOTAL PROTECTION CONTRIBUE	CORRESPONDANCE AVEC LES PILIERS DU NIST	DOMAINE NIS2
ARTICLE 21(2)(I)	Sécurité des ressources humaines, politiques de contrôle des accès et gestion des actifs.	IAM, workflows de gestion des arrivées, des changements de poste et des départs, inventaire des actifs et contrôle des accès à privilèges.	Rapports sur les autorisations de 365 Permission Manager, délégation aux propriétaires de sites, niveaux de partage externe, Auto-remediate et journal d'activité ; contrôles d'accès privé et d'accès test aux archives d'emails	Protéger	Gestion risques de cybersécurité
			Gestion groupée des utilisateurs avec 365 Total Backup.		
ARTICLE 21(2)(J)	MFA ou authentification continue, communications vocales, vidéo et textuelles sécurisées, ainsi que communications d'urgence sécurisées, le cas échéant.	MFA/SSO, accès conditionnel, communications sécurisées et communications d'urgence.	Email encryption	Protéger	Gestion risques de cybersécurité
			Websafe		
ARTICLE 23(2)	Notification sans retard injustifié, dans un délai de 24 ou 72 heures selon l'incident.	Alertes sous 24 heures, automatisation du triage, classification initiale et gestion des astreintes.	Alertes en temps réel et Auto-remediate avec Advanced Threat Protection	Réagir	Partage d'informa
			Email Live Tracking		
			AI Email Security Analyst aide à caractériser les incidents impliquant des emails		
			Corrections automatisées avec 365 Permission Manager.		

Renforcez votre stratégie de cybersécurité pour NIS2

La conformité à NIS2 nécessite une approche à l'échelle de l'entreprise, qui combine gouvernance, processus, collaborateurs et technologies. Aucun produit de sécurité ne peut, à lui seul, garantir la conformité.

365 Total Protection peut contribuer à cette stratégie globale en fournissant des fonctionnalités de sécurité, de résilience, de gouvernance et de sensibilisation qui aident les entreprises à mettre en oeuvre des mesures liées aux principales exigences de NIS2, de la sécurité des emails et du chiffrement à la sauvegarde, en passant par la gestion des autorisations, la visibilité sur les incidents et la sensibilisation à la cybersécurité.

Ensemble, ces fonctionnalités peuvent aider les entreprises à renforcer leur posture de cybersécurité et à soutenir leurs efforts continus de mise en conformité avec NIS2.

COMMENCEZ VOTRE ESSAI GRATUIT

Sources: European Commission policy page • European Commission NIS2 FAQ • Official NIS2 text on EUR-Lex