Seguretat del Lloc de Treball (Endpoint Security)

El lloc de treball (ordinador o servidor) és la primera línia de defensa i, sovint, la més feble de la cadena de seguretat. Aquest servei és fonamental i indispensable per a qualsevol client.

És un servei gestionat que protegeix els dispositius de l'empresa (endpoints) contra tot tipus d'amenaces, incloent-hi malware, ransomware, virus i atacs complexos.

El servei s'ofereix en dos nivells per adaptar-se a la sensibilitat de les dades i al perfil de risc de cada client:

Nivells de servei:

Nivell 1: NGAV (Next-Generation Antivirus)	Nivell 2: EDR (Endpoint Detection and Response)
La protecció fonamental. Va més enllà de l'antivirus tradicional basat en signatures, utilitzant tècniques de machine learning i anàlisi de comportament per bloquejar amenaces conegudes i desconegudes, amb un focus especial en la prevenció del ransomware.	La protecció avançada. Inclou totes les capacitats del NGAV i afegeix una capa de visibilitat i resposta. L'agent EDR actua com una "caixa negra" a l'endpoint, registrant tota l'activitat rellevant. Això permet als nostres analistes del SOC investigar atacs sofisticats, entendre com es va produir l'atac, aïllar dispositius i respondre de forma contundent.

Per a qui és ideal?:

- **NGAV:** Absolutament totes les empreses. És la capa de seguretat mínima i indispensable.
- **EDR:** Empreses que gestionen dades sensibles (personals, propietat intel·lectual, financeres), subjectes a normatives infinites, o que són un objectiu atractiu per als ciberdelinqüents.

Preus: 5 €/mes x usuari (NGAV + EDR).

Beneficis clau:

- Prevé infeccions per virus i malware.
- Bloqueja el ransomware.
- Proporciona visibilitat sobre amenaces silencioses (amb EDR).
- Centralitza la gestió i resposta a incidents en mans dels experts d'Eports Tech.
- Amb Heimdal, s'afegeix una capa de prevenció proactiva i la possibilitat de consolidar múltiples eines de seguretat en una sola.

Protecció de Correu Electrònic

El correu electrònic continua sent el vector d'atac número u. Més del 90% dels ciberatacs amb èxit comencen amb un simple correu de phishing, cosa que converteix aquest servei en una capa de protecció indispensable.

Un servei de seguretat al núvol (gateway de correu) que se situa entre Internet i el servidor de correu del client (Microsoft 365 o Google Workspace). Analitza i filtra el 100% del correu entrant i sortint per neutralitzar amenaces abans que arribin a la bústia de l'usuari.

Per a qui és ideal?: Totes les empreses, sense excepció. És una mesura de seguretat fonamental.

Característiques tècniques i què inclou:

- Filtre multicapa anti-spam i anti-phishing.
- Anàlisi de fitxers adjunts en sandbox per detectar malware de dia zero.
- Protecció contra la suplantació d'identitat (Business Email Compromise - BEC) i el frau al CEO.
- Validació de remitents (DMARC, DKIM, SPF).
- Continuïtat de correu (en cas de caiguda del servidor principal).
- Mòduls **Email Security** i **Email Fraud Prevention.** El primer ofereix una protecció avançada contra malware, correu escombraria i phishing, mentre que el segon s'especialitza a detectar i bloquejar atacs d'enginyeria social, suplantació de domini i BEC, utilitzant més de 125 vectors d'anàlisi.

Beneficis clau:

- ✓ Reducció dràstica del correu escombraria i maliciós.
- ✓ Protecció avançada contra frau i robatori de credencials.
- ✓ Prevenció de ransomware i malware distribuït per correu electrònic.

Preu: El servei es comercialitza sota un model de subscripció mensual per bústia de correu protegida: **4 €/bústia/mes**.

eports
tech

Ctra. Aldea-Tortosa, Km 2.4
43500 Tortosa (Tarragona)

CONTACTA'NS

977 50 30 70

comercial@eportstech.com

eportstech.com

eportsinternet.com

Empresa del grupo eacom