Cybersecurity
Progress. Protected.

Sustabdykite sudėtingas grėsmes debesijos darbo aplinkoje

ESET Cloud Application Protection

Problema

El. paštas išlieka pagrindiniu kibernetinių atakų kanalu. Integruotos Microsoft 365 ir Google Workspace apsaugos priemonės dažnai nesustabdo pažangių el. pašto grėsmių, todėl organizacijos išlieka pažeidžiamos fišingo, tapatybės klastojimo (spoofing) ir nulinės dienos (zero-day) atakoms.

Pagrindiniai verslo iššūkiai

- DI pagrįstos atakos, kenkėjiški QR kodai ir tapatybės klastojimo atakos apeina standartinius filtrus, sukeldamos grėsmę duomenims, finansams ir organizacijos reputacijai.
- Nulinės dienos pažeidžiamumai apeina įprastas apsaugos priemones, sukeldami paslaugų sutrikimus, išpirkos reikalaujančių programų incidentus ir didindami veiklos kaštus.
- Darbuotojų klaidos gali lemti duomenų saugumo pažeidimus, atitikties reikalavimų nesilaikymą ir papildomas rizikas.

$50,000

Vidutinis verslo el. pašto kompromitavimo (Business Email Compromise, BEC) incidento nuostolis

87%

Socialinės inžinerijos pagrindu įvykdomų saugumo pažeidimų susiję su fišingu arba apsimetinėjimu

1.5%

Vidutiniškai tiek darbuotojų kiekvienos fišingo kampanijos metu tampa jos aukomis

Šaltinis: Verizon Data Breach Investigations Report 2025

Sprendimas

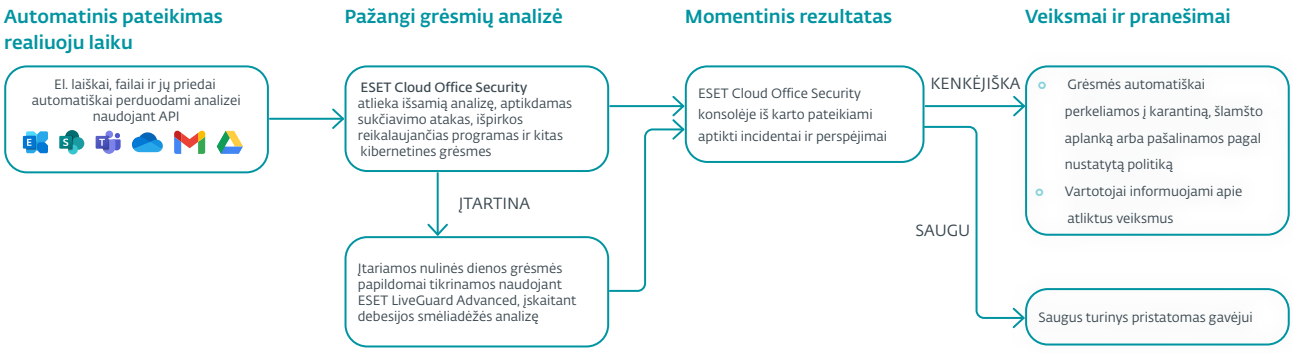
ESET CLOUD OFFICE SECURITY

ESET Cloud Office Security užtikrina pažangią, dirbtiniu intelektu paremtą Microsoft 365 (**Exchange Online, OneDrive, SharePoint Online, Teams**) ir Google Workspace (**Gmail, Google Drive**) apsaugą. Sprendimas sustabdo grėsmes, kurios apeina standartines apsaugos priemones, naudodamas:

- apsaugą nuo sukčiavimo (Anti-Phishing);
- apsaugą nuo kenkėjiškos programinės įrangos;
- brukalo filtravimą;
- apsaugą nuo tapatybės klastojimo (Anti-Spoofing);
- homoglifų domenų apsaugą.

Remdamasis pažangia ESET grėsmių žvalgyba, sprendimas realiuoju laiku aptinka ir blokuoja nulinės dienos grėsmes bei leidžia patogiai valdyti saugumą per intuityvią debesijos valdymo konsolę.

KAIP TAI VEIKIA



PAGRINDINIAI PRIVALUMAI

Proaktyvus grėsmių aptikimas naudojant unikalias ESET technologijas

Naudojama pažangi apsauga nuo grėsmių ESET LiveGuard Advanced ir ESET grėsmių žvalgyba leidžia realiuoju laiku aptikti ir blokuoti nulinės dienos grėsmes.

Maksimalus veiklos tęstinumas

Grėsmės sustabdomos dar prieš vartotojui jas pasiekiant, todėl pašto dėžutės išlieka švarios, o darbas – nepertraukiamas. Naudodami Email Clawback administratoriai gali greitai pašalinti įtartinus el. laiškus, laikinai sustabdyti kompromituotas vartotojų paskyras, priverstinai atjungti prisijungusius naudotojus.

Apsauga nuo pažangių el. pašto grėsmių

Sprendimas aptinka ir blokuoja tapatybės klastojimo atakas, homoglifų domenus, kenkėjiškus QR kodus, suklastotus kalendoriaus kvietimus.

Išmanus automatizavimas paprastam saugumo valdymui

Sumažina administratorių darbo krūvį, užtikrindama automatinę vartotojų apsaugą, įspėjimus realiuoju laiku ir individualiai pritaikomi valdymo skydą. Automatizavimas veikia iš karto ir leidžia nustatyti individualias taisykles.

ĮSIGIJIMO GALIMYBĖS

- Galima pasirinktuose ESET PROTECT prenumeratos planuose.
- Galima įsigyti kaip atskirą sprendimą. Lengvai įdiegiamas ir sklandžiai integruojasi su bet kuria esama įrenginių apsaugos platforma arba XDR sprendimu.

SUSISIEKIME

ESET Lietuva
Tel.: +370 5 233 9992
El. paštas: info@eset.lt
www.eset.lt