

Soluții de Securitate

Tehnologie Fortinet
implementată de inginerii
Dendrio



Cuprins

3

Fortinet Threat Landscape Index

4

Studii recente

5

Atacuri rapide și sofisticate

6

Fortinet Next-Generation Firewall (NGFW)

7

Securitate la viteza afacerii

8

Implementare Dendrio: Consolidarea și securizarea rețelei cu FortiGate 200E

9

Implementare Dendrio: Securizarea infrastructurii critice de rețea cu NGFW la unul dintre cele mai mari spitale din România

10

Dendrio, partener Fortinet



Fortinet Threat Landscape Index:

Volatilitatea ridicată și tendința ascendentă a amenințărilor cibernetice

Rezumat

Mulți dintre experții CISO (Chief Information Security Officer), împreună cu echipele lor, sunt copleșiți de volumul de muncă pe care îl implică peisajul amenințărilor cibernetice actuale. De multe ori sunt nevoiți să adopte o poziție reactivă în timp ce încearcă să identifice și să corecteze breșele de securitate fără să oprească business-ul.

Multe astfel de echipe sunt depășite de evoluția rapidă a ecosistemului criminalității informatice și de tehnologiile care se diversifică permanent în acest segment. În plus, atacurile sunt din ce în ce mai automatizate și au o viteză de propagare atât de rapidă încât răspunsul manual devine inadecvat. În acest context, anxietatea pe care o simt mulți CISO este naturală și justificată.

Sunt necesare răspunsuri automatizate și cât mai predictibile, pentru impredictibilitatea oferită de contextul amintit mai sus. În acest sens a fost dezvoltat în 2019 Indicele Fortinet Threat Landscape, pentru a oferi o perspectivă asupra dimensiunii și direcțiilor amenințărilor cibernetice. Acest indice ne oferă o posibilă soluție asupra volatilității ridicate și a tendinței ascendențe a amenințărilor cibernetice: prevenție prin automatizare.



FortiGuard Labs - concluzii



Un studiu realizat de către SANS Institute în 2018 a arătat că centrul de operațiuni de securitate dintr-o organizație medie, primește peste 10.000 de alerte pe zi, însă un analist nu poate să investigheze empiric decât 20-25 dintre ele.



John Oltkis, în "Dealing with Overwhelming Volumes of Security Alerts", 2017, constată că 47% dintre specialiștii în securitate nu cred că echipele lor colectează adecvat informații despre atacuri pentru a acționa proactiv. 42% dintre aceștia spun că organizația ignoră un număr semnificativ de alerte, deoarece resursa umană nu poate ține pasul cu volumul lor.



Malware-ul targetat și polimorfic atinge în acest moment cote alarmante, ceea ce determină creșterea semnificativă a numărului zilnic de atacuri necunoscute (Zero Day).

O analiză realizată recent de FortiGuard Labs arată că până la 40% din malware-urile detectate într-o singură zi sunt de tip Zero Day, nefiind cunoscute anterior. Când apar atacuri de tip Zero Day, echipa de cybersecurity este copleșită și acționează reactiv, pentru remedierea manuală a problemelor, însă acest mod de lucru nu este sustenabil pe termen lung.

În plus, Malware-as-a-Service (MaaS) este o resursă din ce în ce mai disponibilă pentru criminalii cibernetici care nu au abilitatea tehnică de a-l dezvolta de la 0. Devine posibil astfel accesul unui număr mai mare de infractori cibernetici, ceea ce determină o creștere semnificativă a volumului de atacuri. Un raport recent Fortinet Threat a identificat vânzarea malware-ului Emomet banking Trojan sub formă de licență – îl poți folosi și ai acces la update-urile acestuia, cât timp îl folosești.

Viteza crescută:

**impune
implementarea unui
răspuns automat**



Nu cu mult timp în urmă, detectarea și prevenirea amenințărilor cibernetice erau definite mult mai clar, iar strategiile de analiză și răspuns erau tactice. Dar odată cu creșterea tipurilor de riscuri și atacuri cibernetice, protecția împotriva acestora se poate dovedi dificilă chiar și pentru un CISO cu experiență.

Totodată, atacatorii se folosesc de un grad ridicat de automatizare prin Inteligența Artificială, ceea ce le permite să depășească viteza manuală de răspuns.

**Grad de sofisticare sporit:
păstrarea ritmului prin
tactici avansate**

97% dintre viruși își schimbă în mod automat caracteristicile, folosindu-se de polimorfism, ceea ce înseamnă că semnătura unui virus descoperită în urmă cu câteva minute se poate schimba la un interval regulat.

Fortinet Next-Generation Firewall (NGFW)

Performanță ridicată și protecție împotriva amenințărilor, cu vizibilitate automatizată

Fortinet Next-Generation Firewall (NGFW) filtrează traficul din rețea, organizațiile fiind astfel protejate de amenințări externe. Prin păstrarea caracteristicilor unui firewall clasic precum filtrarea pachetelor de date, suportul VPN, monitorizarea rețelei și funcțiile de mapare IP, Next Generation Firewalls dețin, în plus, funcții de inspecție avansate și au astfel o capacitate superioară de a identifica atacuri, malware și alte forme de amenințări cibernetice.

Next Generation Firewalls pun la dispoziția organizațiilor controlul aplicațiilor, prevenirea intruziunilor și vizibilitate avansată în rețea. Pe măsură ce peisajul amenințărilor continuă să se dezvolte rapid, firewall-urile tradiționale sunt depășite, punând în pericol o organizație. NGFWs nu numai că blochează programele malware, dar, oferă flexibilitatea de a evolua odată cu mediul extern și de a menține siguranța rețelei pe măsură ce apar noi amenințări.

Fortinet este singurul producător care se află de 10 ani în categoria "Lideri în segmentul Network Firewalls" – raport elaborat de entitatea independentă Gartner.





NGFW

Securitate la viteza de business

Protecție inegalabilă

NGFW-urile FortiGate oferă cea mai bună protecție împotriva amenințărilor cibernetice existente, într-o formă compactă și printr-o formă de utilizare facilă.

Bazat pe Inteligență Artificială și pe învățare automată (Machine Learning), NGFW-urile FortiGate oferă o gamă largă de servicii de securitate integrate:

- ✓ Protecția împotriva amenințărilor cibernetice;
- ✓ Inspecție SSL / TLS;
- ✓ Sistem de prevenire a intruziunilor (IPS);
- ✓ Filtrare URL;
- ✓ Rating de Securitate;
- ✓ Segmentarea bazată pe intenție;
- ✓ IPsec / SSL VPN;
- ✓ Identificarea utilizatorului / dispozitivului și a tentativelor de autentificare;
- ✓ Sandboxing;
- ✓ Rețea (LAN, WAN, Wi-Fi);
- ✓ Management și raportare.

Studiu de Caz 1 Implementarea unei soluții Fortinet

Companie de construcții



Consolidarea și securizarea rețelei cu FortiGate 200E

Soluție implementată de inginerii Dendrio

OBIECTIV: consolidarea operațiunilor de rețea și securitate cu vizibilitate deplină pentru a proteja o locație în Județul Galați.

CERINȚE CHEIE: acces wireless securizat, prevenirea intruziunilor, antivirus, segmentare internă

SOLUȚIE: Next Generation Firewall - Fortigate 200E.

BENEFICIILE CLIENTULUI:

- ✓ vizibilitate completă a întregii arhitecturi, dintr-un singur ecran
- ✓ flexibilitate pentru a consolida în viitor elemente specifice de securitate cu soluție integrate
- ✓ scalabilitate pentru a satisface nevoile viitoare de Securitate
- ✓ soluția a fost neutră din punct de vedere al costurilor în comparație cu soluția anterioară, oferind în același timp un nivel de performanță și securitate superior.



Studiu de Caz 2 Implementarea unei soluții Fortinet

Unul dintre cele mai mari spitale din România

Securizarea infrastructurii critice de rețea cu Fortinet Next Generation Firewall

Soluție implementată de inginerii Dendrio

OBIECTIV: securizarea infrastructurii critice de rețea, vizibilitate deplină pentru a proteja o locație, consolidarea și securizarea operațiunilor de rețea. Spitalul trebuie să protejeze datele celor peste 100.000 de persoane care se internează anual și celor peste 300.000 de pacienți care se prezintă pentru consultații anual.

CERINȚE CHEIE: acces wireless securizat, prevenirea intruziunilor, antivirus, segmentare internă.

SOLUȚIE: Next Generation Firewall - Fortigate 100E + Switch + Wi-Fi securizat.

BENEFICIILE CLIENTULUI:

- ✓ vizibilitate completă a întregii arhitecturi dintr-un singur ecran;
- ✓ flexibilitate pentru a consolida în viitor elemente specifice de securitate cu soluție integrate;
- ✓ scalabilitate pentru a satisface nevoile viitoare de Securitate cibernetică.

Dendrio

Secured Hybrid Multi- Cloud Integrator



Partener Fortinet

Dendrio este ghidul inteligent care fructifică tehnologiile existente și identifică noi tehnologii pentru a oferi avantaj competitiv clienților săi: preț, viteză de reacție, siguranță și optimizare. În acest fel le înlesnește călătoria în business.

Fiecare zi de business este o călătorie în lumea tehnologiei. Dendrio este alături de tine. Livrăm servicii integrate bazate pe cloud, securitate, rețelistică și soluții complete de mobilitate, aplicații software cu diverse opțiuni de licențiere. Totul pentru ca drumul pe care îl parcurge compania ta să fie cel mai scurt și mai sigur:

Dendrio. Your Journey. Upgraded!

www.dendrio.com
askformore@dendrio.com

(+4021) 303 20 70

**Bld. Timișoara, Nr. 26, Etaj 1, Clădirea
„Plaza Romania Offices”, Sector 6,
061331, București, România**