# Lastline Enterprise: Advanced Malware Protection

## Lastline Enterprise: Efektivní ochrana proti pokročilému malwaru

*I společnosti, které pravidelně investují do nových technologií a svědomitě budují svojí bezpečnostní infrastrukturu mohou být neustále zranitelné vůči pokročilým malwarovým útokům. Nejen nejnovější firewally a Intrusion Prevention Sondy, ale ani sandboxingové technologie nejsou schopny zachytit nejnovější tzv. Evasive malware, který je navržen způsobem umožňujícím spolehlivě identifikovat vaše bezpečnostní nástroje a vyhnout se jim.*

### Ochrana před Evasive technikami malwaru

Lastline Enterprise je kompaktní řešení zaměřené na Breach Detection. Poskytuje svým uživatelům bezkonkurenční ochranu proti pokročilému malwaru, a to i přesto, že je daný malware navržen tak, aby prošel skrze všechny bezpečnostní prvky nasazené ve vaší infrastruktuře a kompromitoval ji. K tomuto účelu využívá svou unikátní technologii analýzy - FUSE (Full System Emulation), která dokáže detekovat malware určený pro obcházení tradičních i pokročilých ochranných prvků. Díky této unikátní technologii FUSE je Lastline pro malware takřka nedetekovatelný tzv. Sandbox detektory (např. PAFISH). Lastline koreluje informace síťových incidentů do srozumitelných APT informací – **poskytuje pouze relevantní informace.**

**Lastline Sensor** **SHROMAŽĎUJE**

**Lastline Engine** **ANALYZUJE**

**Lastline Manager** **REAGUJE**

**LastLine Enterprise** přiřazuje úrovně závažnosti k jednotlivým hrozbám, díky čemuž se bezpečností administrátoři dokáží jednodušeji zorientovat. Zaručuje tak úsporu času pro váš security tým, který bude schopný reagovat na skutečné hrozby a nebude věnovat svůj drahocenný čas false-positive eventům.

### Možnosti nasazení:

**On-Premise Data Sharing -** Správce ukládá všechny informace týkající se detekce infikovaných stanic a analýzy softwarových artefaktů on premise.

**On-Premise Private –** Správce ukládá informace on-premise, avšak nesdílí žádná data týkající se škodlivých spustitelných souborů s Lastline.

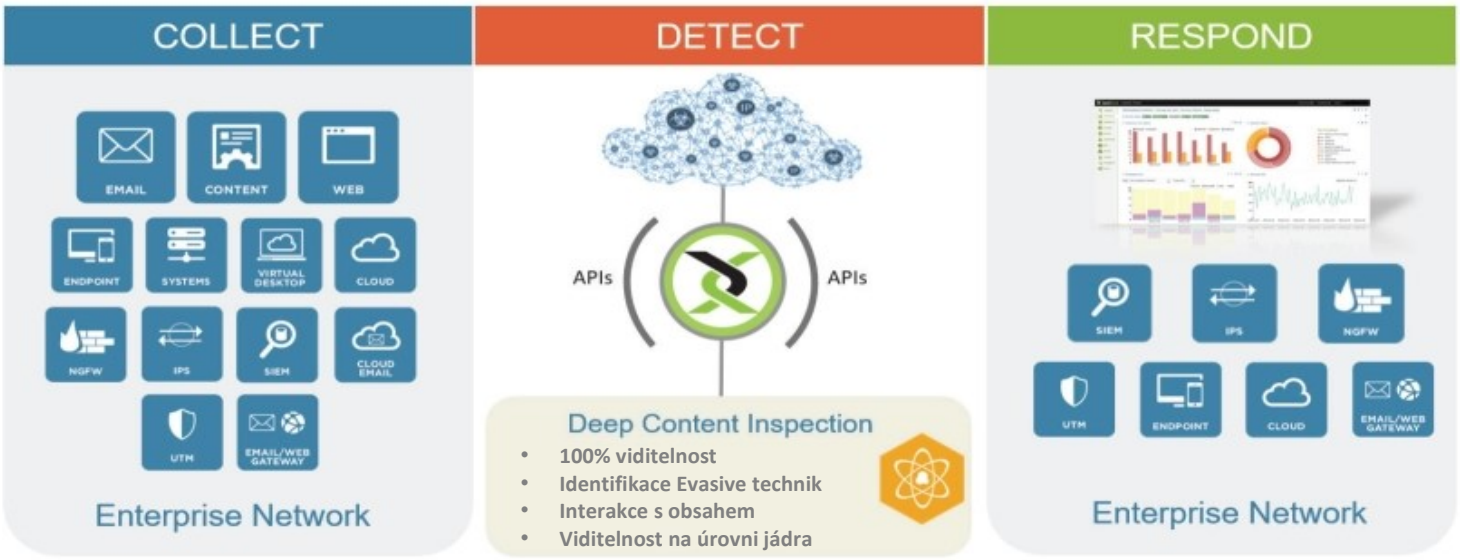
**Hosted Full –** Správce a Engine jsou umístěny v datovém centru společnosti Lastline.

### Klíčové vlastnosti

- ✓ Vysoká účinnost detekce (Nejlépe hodnocená detekční technologie dle **NSS LABS)**
- ✓ Velmi malé procento **False positives / False negatives incidentů**
- ✓ Možnost napojení globální reputační databáze, která se proaktivně zdokonaluje a využívá **machine learning techniky**
- ✓ **Korelace hrozeb** dle závažnosti pro vaši síť
- ✓ Detailní náhled do průběhu útoku na vaši síť
- ✓ Otevřená API integrace s obsáhlou dokumentací
- ✓ Jednoduchá integrace s dalšími technologickými vendory
- ✓ Podpora instalace na vlastní, běžně dostupný hardware (DELL, HP) – čímž snižuje náklady (TCO)

NSS LABS RECOMMENDED

**100%**
Breach Detection Score
**0%**
False positive
ve všech kategoriích




COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

# Lastline Enterprise: Advanced Malware Protection

## Lastline Enterprise: COLLECT – DETECT - RESPOND

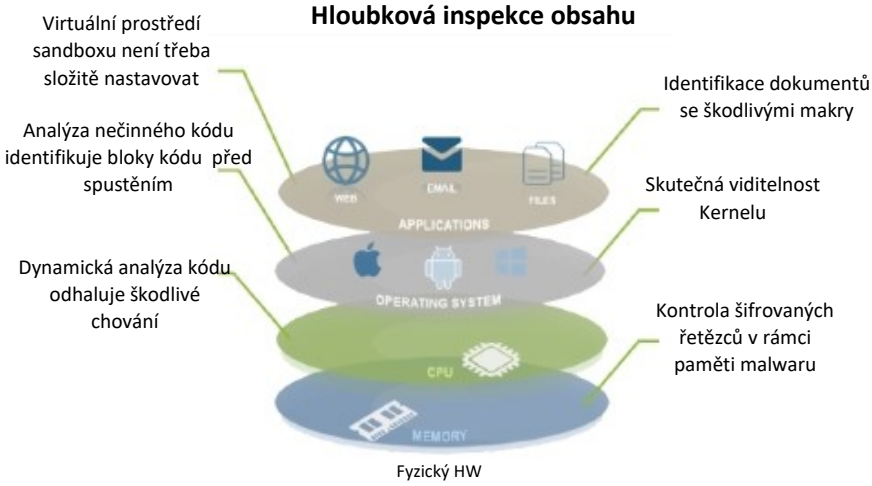
Lastline Enterprise je schopen detekovat nejenom existující malware uvnitř vaší organizace, ale i malware, který se snaží infiltrovat do vaší sítě prostřednictvím e-mailu, škodlivých webových stránek, infikovaných mobilních zařízení a notebooků atp. Celý proces funguje na ve třech krocích:

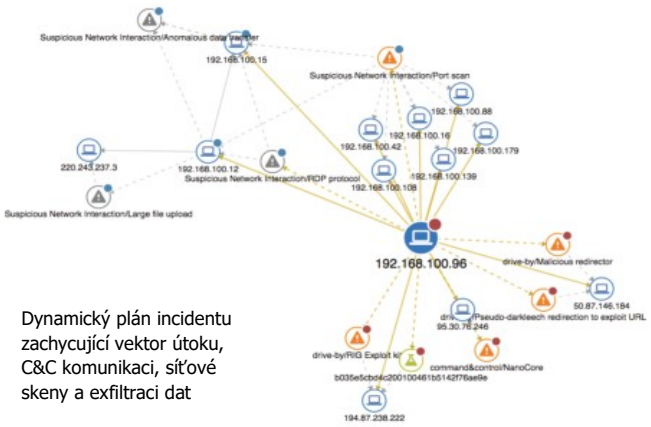
- **COLLECT:** Senzor umístěný v podnikové infrastruktuře shromažďuje neznámé soubory, e-maily a webový obsah za účelem analýzy. Informace v celém perimetru, v rámci datových center a síťové infrastruktury lze shromažďovat také pomocí produktů technologických partnerů s integrovanou funkcionalitou Lastline Collection, nebo využitím Lastline API.
- **DETECT:** Jedinečná technologie Deep Content Inspection zajišťuje detailní vhled do chování pokročilého malware a to díky vyspělému emulačnímu enginu FUSE, který poskytuje detailní simulace prostředí hosta (simuluje např. také CPU, systémovou paměť a připojená zařízení).
- **RESPOND:** Lastline Breach Defender analyzuje informace, které shromažďují senzory a na základě této analýzy generuje dynamický plán vniknutí a aktivity malwaru ve vašem systému. Tato vizualizace umožní vašemu bezpečnostnímu teamu rychle identifikovat a blokovat škodlivou aktivitu.

## Hloubková inspekce obsahu

Tradiční sandboxingové technologie pracují pouze na úrovni operačního systému, proto mají výrazně vyšší procento tzv. false pozitive alertů, nebo je dokáže pokročilý malware obejít. V případě Deep Content Inspection se jedná o jedinečné prostředí, které je izolované a probíhá v něm celková inspekce malwaru.

Lastline Enterprise dokáže díky Deep Content Inspection sledovat všechny možné akce, které se pokusí škodlivý objekt provést. Full System Emulation (FUSE) nabízí kompletní simulaci prostředí počítače, které umožňuje analyzování i nejpokročilejšího malwaru.




Dynamický plán incidentu zachycující vektor útoku, C&C komunikaci, síťové skeny a exfiltraci dat

## Global Threat Intelligence Network

Global Threat Inteligence Network je globální reputační databáze, která automaticky sdílí charakteristiky, chování malwaru a IoC (inverze chování). Tyto informace si zaznamená u každé hrozby, která prošla analýzou a detekcí jakéhokoliv řešení Lastline po celém světě. Díky informacím z GTI je vaše infrastruktura okamžitě chráněna proti nejnovějším hrozbám, které byly zaznamenány. Databáze GTI se proaktivně zdokonaluje pomocí machine learning technologií.

**Breach defender** je unikátní technologie, která poskytuje dynamický plán incidentu vniknutí přímo v jeho průběhu.

Každý incident (Breach) se skládá z mnoha eventů a právě Breach Defender je dokáže složit dohromady a dát jim potřebný kontext tak, aby mu porozuměli bezpečnostní administrátoři a dokázali na hrozbu včas a efektivně zareagovat. Breach Defender analyzuje podezřelé objekty a síťový provoz v reálném čase – poskytuje tak bezpečnostnímu teamu ty nejlepší podmínky pro rychlou reakci na aktuální hrozby. Navíc umožňuje využít **Lastline senzory pro zablokování nežádoucí síťové aktivity.**

## Integrace s dalšími bezpečnostními prvky

Lastline Enterprise lze snadno integrovat s dalšími bezpečnostními prvky předních bezpečnostních výrobců (Barracuda, Check Point, Symantec, HP ArcSight, IBM QRadar, TREND MICRO atd.), kdy může spolupracovat oboustranně a umožňuje rychlou detekci nejnovějších hrozeb a jejich nápravu.

Další výhoda je využití Latline API, díky němuž můžete sbírat důležitá data z již nasazených bezpečnostních řešení, kdy integrací Lasline Enterprise jednoduše upravíte sady pravidel a vytvoříte nové workflow. Tímto Lastline Enterprise výrazně vylepší detekci hrozeb u stávajících bezpečnostních prvků ve vaší síti.


COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz