Lastline and empow - Joint Solution

Automate Detection, Investigation and Response.

empow
You have it in you.

Benefits at a glance

- Upgrade attack detection and visibility by utilizing the industry's leading advanced malware detection technology
- Automate investigation and attack prioritization
- Automate incident response throughout the network
- Reduce workload
- Integrate with existing security infrastructure to make tools more effective

lastline™

The Challenge

Although organizations are adopting multiple technologies to detect and protect against advanced threats, attackers have engineered malware to bypass security mechanisms. As a result, organizations face the following challenges:

- Lack of detection - partial visibility, resulting in advanced attacks going undetected, or too slow to detect, by point solutions.
- Long time to investigate - triage and investigations lacking context and done manually within siloed products.
- Long time to respond - containment and remediation processes are slow and inaccurate, where customers require these to be fast, pervasive and surgical.

Together, empow and Lastline provide customers with unparalleled threat visibility and detection, and optimized response against advanced attacks.

Lastline and empow Security Platform Joint Solution

Lastline provides unmatched malware detection and visibility into every malicious behavior engineered into a piece of malware, enhanced by a global threat intelligence network. The empow Security Platform provides prescriptive security analytics across threat scenarios and security tools, dynamically automated security orchestration – all based on a unique insight into attacker intent.

With Lastline and empow integrated, customers not only benefit from early malware detection and malware intelligence, but can maximize the value of this information and put it to action - to understand the entire attack story, optimize investigation and automate response. With the joint solution in place, security architects can define defense strategies against prioritized risks intents, maximizing security tools' capabilities; Organizations can focus on prioritized threats, benefiting from seamless integration and full automation with their entire existing security infrastructure.

Optimize Detection and Response with empow and Lastline Enterprise

Threat Scenario

An employee receives a spear phishing email and clicks on a malicious link, resulting in a malware download attempt. The attacker is using a new malware variant, lateral movement and C&C infrastructure for a broader attack campaign against the target company. Additional endpoints are infected as they contain the sensitive information the attacker is after, with the intent of exfiltrating that information.

Integration in Action

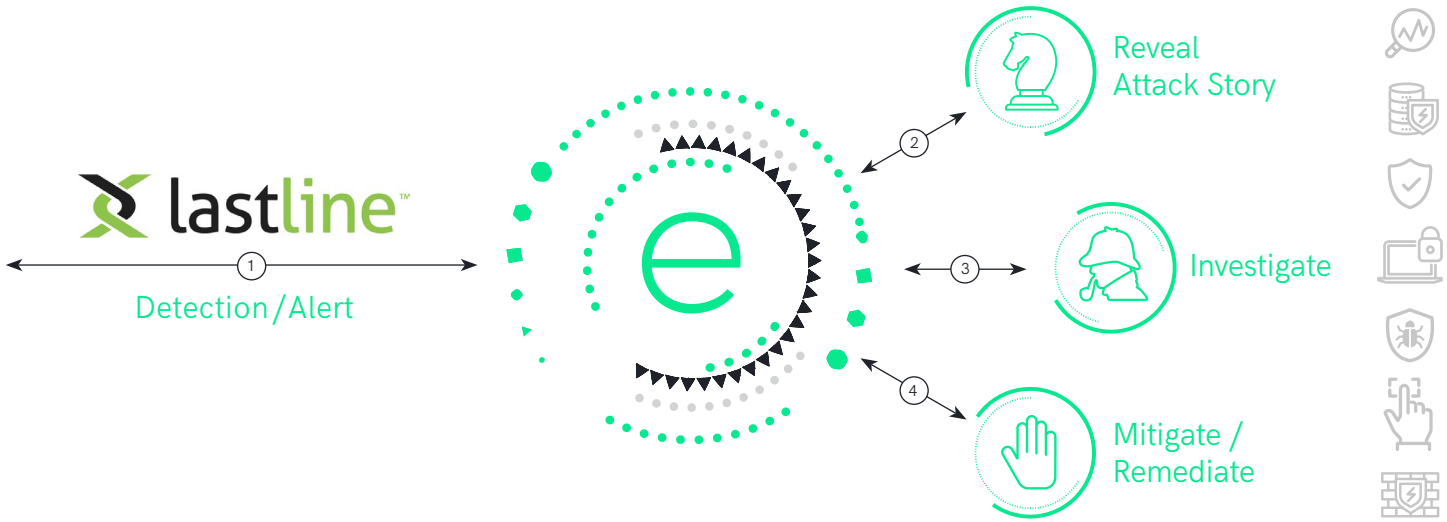

Figure 1 - Detection and Response Optimization

1/ Detection and Alert

Lastline analyzes the file download and reports a zero-day malware alert to empow, including all malicious behaviors engineered into the malware, and actionable IOCs.

2/ Reveal Attack Story

empow analyzes the Lastline alert, and collects security events from the other security tools and services in the network, automatically deciphering each event intent and correlating the events to reveal the attack story and mission.

3/ Investigate

empow automatically investigates, by extracting IOCs from the Lastline alerts, and uses this threat intelligence to hunt for compromised hosts throughout the entire network.

4/ Mitigate / Remediate

After mapping the attack intent, stages and scope of infection, empow orchestrates a surgical response using network tools to contain the attack throughout the entire network, including stopping malicious processes on endpoints and blocking exfiltration of data at gateways.

Summary

empow's Security Abstraction approach allows companies to understand and act on attack intent through advanced prescriptive analytics and dynamic automation – easily connecting, correlating and orchestrating security tools. This allows customers to unleash the power of Lastline's advanced malware detection, visibility and intelligence capabilities in a broader set of threat scenarios and use cases, maximizing investment to mitigate risks and accelerate time from detection to response.

Joint solution customers benefit from full automation of advanced attack detection, investigation and response, by seamlessly integrating with any existing security tools.

About empow

empow is a cybersecurity startup founded in October 2014 in Tel Aviv with the mission of helping organizations "make more of what they already have."

empow's Security Platform integrates with your existing security tools, analyzes them, and breaks them down into their individual components (what we call "security particles"). This creates an abstracted new layer (one unified language), which continuously modifies security capabilities, uncovers attacker intent and optimizes response.

Gartner recently recognized empow as a 2017 Cool Vendor in the Monitoring and Management of Threats category for its intent-based approach, and Forbes singled out empow's technology as one of the few disruptive technologies at RSA in the "software-defined cybersecurity" arena. empow's solution is successfully deployed at large companies in Europe and the U.S.

To learn more, visit www.empownetworks.com

About Lastline

Enterprise security professionals use Lastline to defend their organizations against advanced malware-based attacks that result in damaging and costly data breaches. Our solutions deliver the visibility, context and integration security teams need to rapidly detect and respond to network breaches. Guided by a dynamic blueprint of the breach unfolding within their organization, our customers achieve exceptional enterprise security using fewer resources and at a low total cost of ownership. Lastline solutions are sold directly, through an extensive channel of global partners, and are integrated into the solutions of leading security technology vendors worldwide. Lastline is privately held with headquarters in Silicon Valley.

To learn more, visit www.lastline.com

empow
You have it in you.

Tel: +972-77-4502326
info@empownetworks.com
Hayetzira 29, Ramat Gan, Israel 5252171

www.empownetworks.com