



empow

You have it in you.

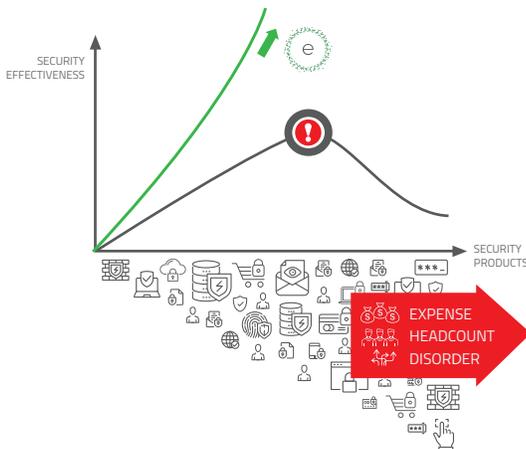
# empow's Security Platform

Turn What You Have Into What You Need



# Make More of What You Already Have

In their attempt to defend against the increasing volume of advanced attack campaigns, organizations are buying more and more security solutions, unwittingly creating a complex and cumbersome cybersecurity architecture. Enterprises are quickly reaching security inflection point, at which their security architecture becomes highly complex, rigid, and non-adaptive. Beyond this point, any further investment in security tools and staff ironically decreases overall effectiveness.



To overcome this, empow is up-ending the conventional approach that “more is better” by turning your existing security tools into an abstracted security language and layer. This layer responds to the unique nature of every attack - **understanding intent and making instant correlations** in order to deploy the right defense strategy.

empow’s Security Platform integrates with your existing network infrastructure and breaks your security tools down into their individual components - what we call Security Particles. These Security Particles represent your organization’s existing security controls and enables dynamic reassembly of these particles into optimized and targeted defense strategies aligned to counter attack missions and compliance-focused risk factors.

Sitting atop of your existing security configuration, the empow Security Platform executes these defense strategies by collecting each security event your security tools and services are generating, automatically deciphering its intent, correlating the events to identify real threats to the organization, prioritizing, assigning and executing the most optimized response.

Using your existing tools, empow’s security platform coordinates and automates optimal detection, investigation and response according to each defense strategy in place - giving you the confidence that your security is responding in the right way, every single time, and **turning what you have into what you need**.

## With empow you can:

Continuously reassemble your existing security tools’ capabilities to optimally handle any advanced attack campaign.

---

Identify advanced threats missed by single (siloeed) tools.

---

Direct, automate and accelerate optimal incident response based on attack intent.

---

Know which security tools are truly effective and what your security gaps are.

---

# Our Intent-based Security Language

empow provides a strategic, vendor agnostic, intent-based security language - which allows customizing, or using pre-built targeted defense strategies (Security Apps) per business needs. The intent-based security language mirrors the attack kill-chain model, the taxonomy of attackers' tactics, techniques and procedures; and is further extended through security community terms. The empow intent-based security language is made up of Security Particles, which are logical security functions that describe various detection, investigation and response controls, allowing you to develop adaptive advanced defense strategies in a simple and intuitive manner.

## Many tools, one tongue



**Detection Particles**



External reconnaissance  
"Call home"  
Privilege escalation  
Financial data scraping  
...



**Investigation Particles**



Network anomaly evidences  
Network intrusions evidences  
Sandbox evidences  
IOC hunting  
...



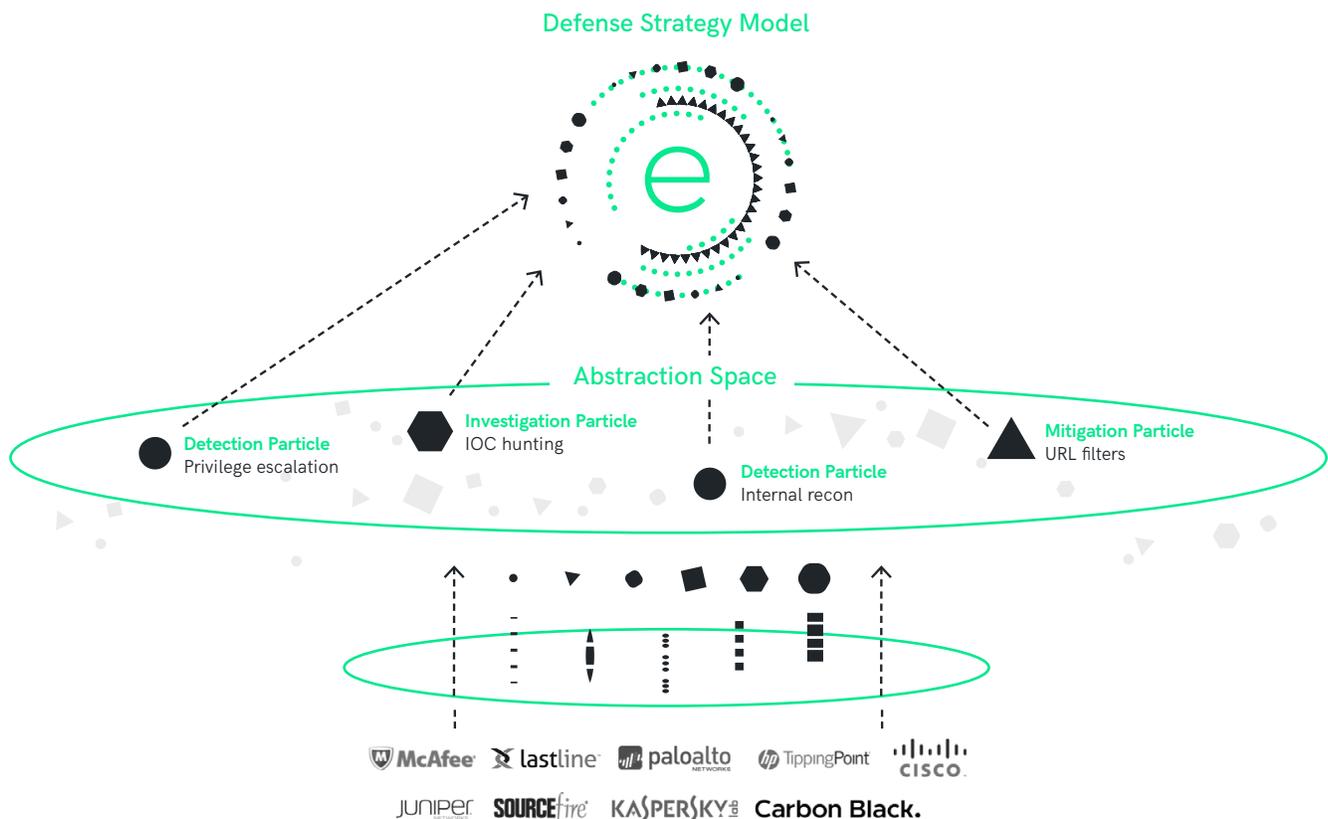
**Response Particles**



Kill process  
Uninstall application  
NG Firewall rules  
ACLs  
...

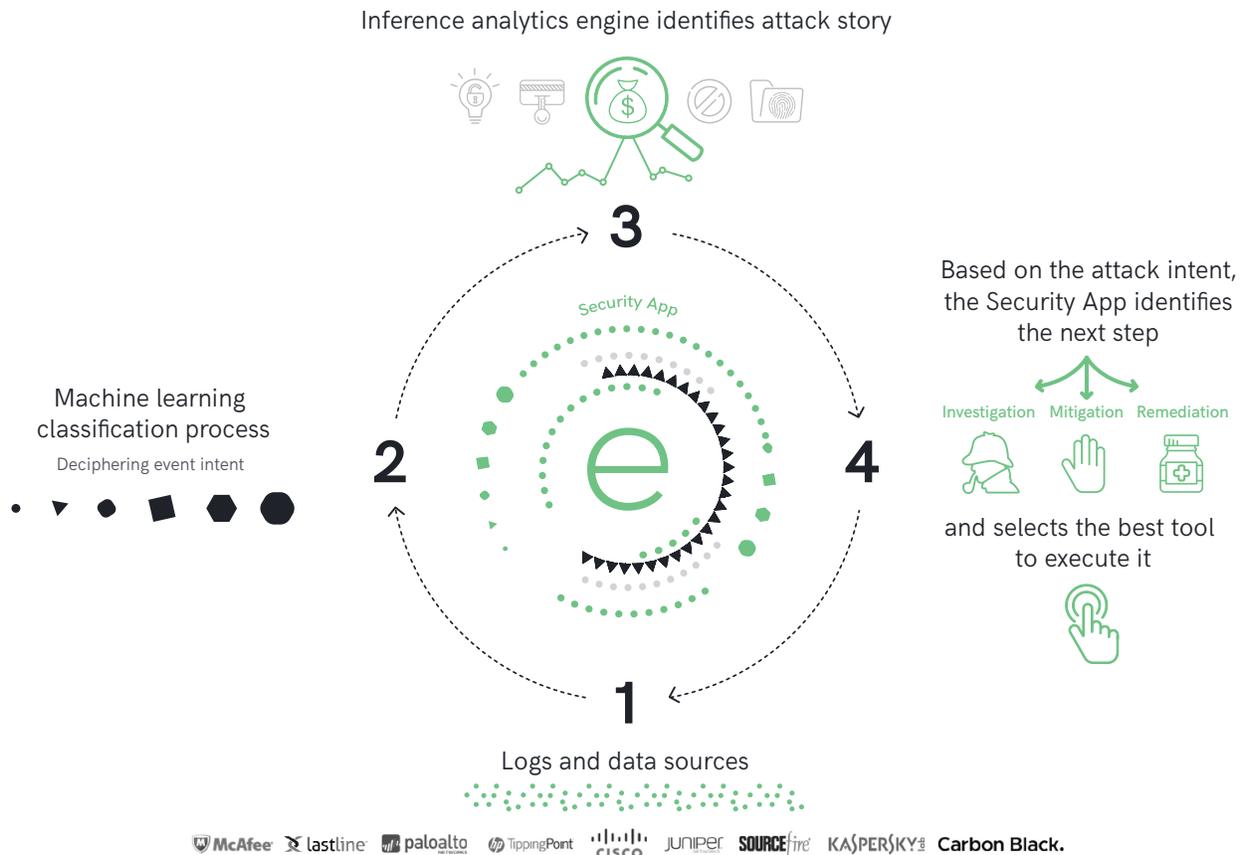
## Security Platform

empow's adaptive Security Platform sits on top of the network infrastructure and actualizes the intent-based security language by translating targeted defense strategies (Security Apps) into one holistic security system that detects, investigates and responds to advanced attacks. The Platform effectively implements and executes these throughout the organization's existing security tools and network infrastructure, while continuously measuring the security system's effectiveness, and the effectiveness of its tools in executing your defense strategies.



# The Process Behind the Promise

empow's solution is made possible by proprietary AI technologies, which are strategically integrated into the following process:



## 1/ Logs and data sources

The empow Platform collects and analyzes logs, data and intelligence feeds from existing security products, using a range of plugins for third-party network and endpoint solutions. If needed, new plugins specific to the customer's needs can be developed by empow's Professional Services team within days, and easily-configured custom data sources may be added.

## 2/ Machine Learning Classification Process

empow's Security Platform deciphers the intent of each collected log, using machine learning and Natural Language Processing (NLP) algorithms. The algorithms emulate the actions done today by the Security Analyst: read the logs, seeking out relevant information from the log itself and from third party data sources outside the organization, and identifying the attack intent. This process runs continuously and automatically, with virtually zero human involvement.

## 3/ Inference Analytics Engine

The security analytics engine identifies cause-and-effect relationships between the collection of deciphered intents, grouping them together and creating a visual attack story. This engine also emulates human security expert processes, decides in real-time, according to the attack intent, which investigation policies are required, and according to the system's risk assessment capabilities, decides which proactive response policies to employ.

## 4/ Identify Next Step and Act

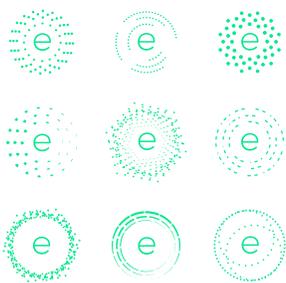
empow's Contextual Orchestration Engine dynamically identifies and selects the best available products and network tools to execute the investigation and response actions. This translates into fast and optimal incident response, while at the same time simplifying security operations and eliminating maintenance overhead.

# Security Apps – Optimal Reassembly of Targeted Defense Strategies

Our Security Platform includes predefined security applications, designed to optimally coordinate your tools to protect against different types of advanced attack campaigns, all of which are customizable. Downloading pre-built applications from empow's Security Apps Store lets you stay up to date and respond quickly to new advanced attack campaigns.

An intuitive drag-and-drop user interface allows security teams to create DIY Security Apps where they select the security particles, as well as workflows that will integrate detection, investigation and response behaviors. Once built by your team, these apps become part of the tool-set that empow's platform abstracts and orchestrates. Vendor-neutral, all security applications utilized by the empow Security Platform are not affected by changes to underlying security products.

## Security Applications



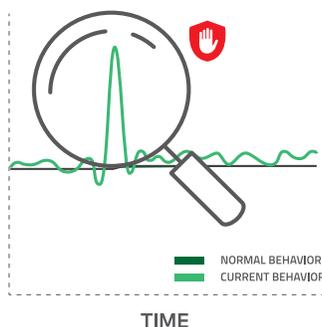
### Compliance based apps

HIPAA  
 PCI DSS  
 EU GDPR  
 NYCRR 500

### Threats based apps

Advanced Ransomware      Financial Data Leak  
 Insider Threat              PII Data Leak  
 Intelligence Gathering      Data Manipulation  
 Service Disruption

# empow Network Traffic Behavioral Analysis Service



empow's solution comes with an out-of-the-box network behavioral analysis service that adds visibility to internal network traffic and detects anomalies in it. empow's NTA consists of a set of DPI software engines that are connected to tap devices or copy ports in the underlying network infrastructure, and monitor east-west traffic flows.

Based on empow's network DPI software engines, the network traffic analytics service learns and profiles the normal patterns of behavior of users and servers inside the network, and identifies behavior anomalies that can be associated with various threat categories.

# Security Ecosystem

A range of plugins for 3rd party networking, servers and security vendors are included in empow's offering, such as intrusion detection systems (IDS), network anti-malware, security reputation services, endpoint security tools, network behavior analysis, firewalls, and many others. If needed, new plugins can be developed by empow's professional services team, according to the customer's needs and within days.



## Threat Analytics Reporting and Security Diagnostics

The empow Security Platform provides advanced threat analytics and security diagnostics. These include both analytics into the different threats targeting the organization - injecting threat management visibility into the organization's security posture as well as detailed diagnostics covering security tools' performance and effectiveness.



The empow Security Diagnostics Service measures the effectiveness of your security architecture against different threats and regulatory standards, providing you (CISOs and Security Managers) with in-depth analysis of your security systems' effectiveness.

empow's Security Diagnostics Service also allows organizations to test various "what-if" scenarios, such as assessing the success of the architecture when a certain product is disabled, and providing a score for each product within the context of various risks. For more information, please refer to our Security Diagnostics Service Brief.

# The Power of empow

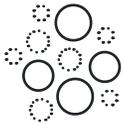
Gives you the confidence of knowing your security organization is responding in the right way, every single time.



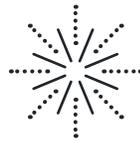
Provides **proactive real-time mitigation** of advanced attack campaigns.



**Automates detection and root-cause investigation** of advanced attack campaigns.



Offers **insight** into which tools are performing at the highest level, and which aren't doing their job.



Unlocks the untapped power of your security apparatus... while **saving** on SOC and security engineering headcount.

“empow’s platform is unique in the security arena... instead of offering an additional protection or functionality, it makes all the tools in our arsenal work optimally and in a synchronized way so that our level of security is effectively improved. With empow, I have the **confidence** of knowing that my security organization is responding in the right way, every single time. //”

Director of National Security at a major U.S. company

## Recognition & Awards

“... Replacing the security Tower of Babel of existing point solutions...”

“empow's unique approach listed among RSA 2017's four disruptive cyber trends.”

**Forbes**

“Breaking through the cybersecurity bubble”

**NETWORKWORLD**  
FROM IDG

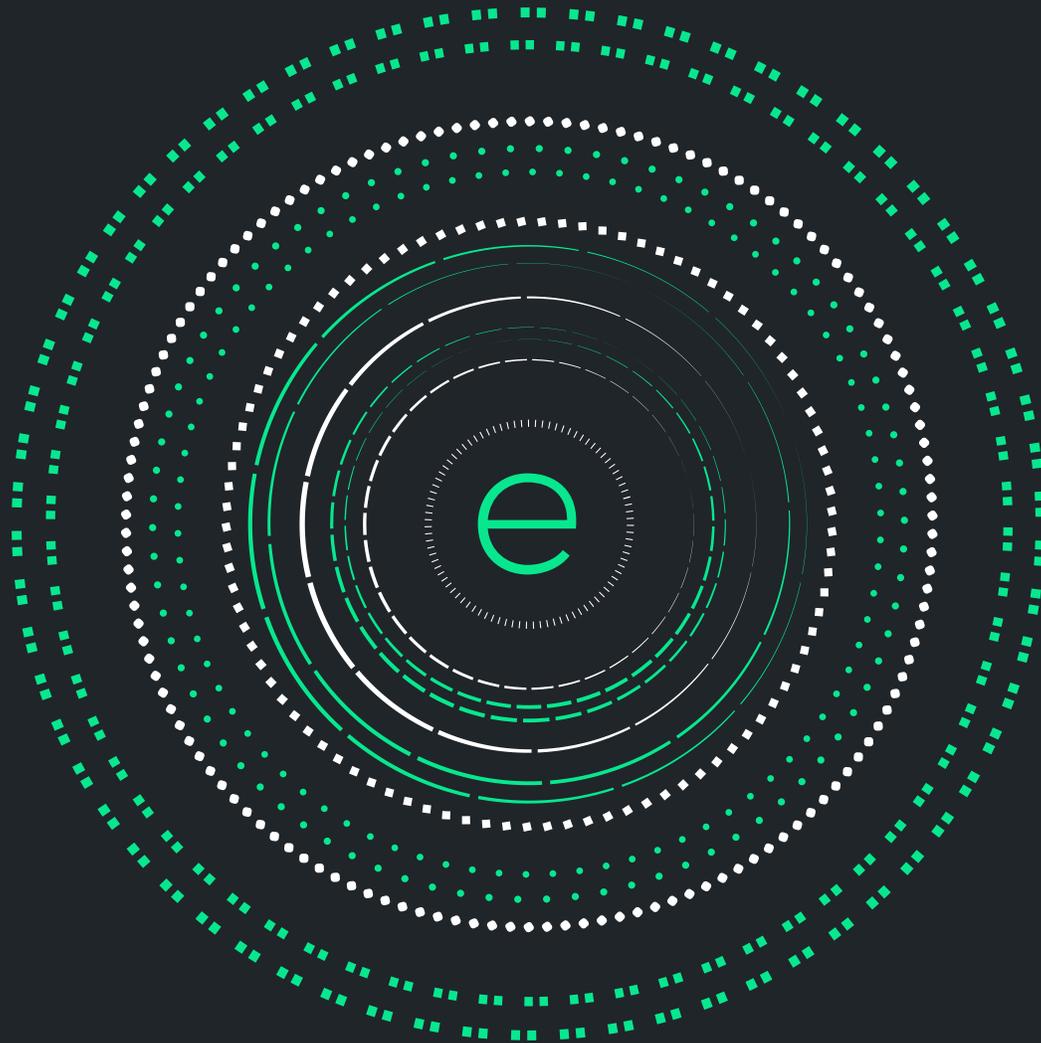


**Gartner**

**Cool Vendor 2017**

“empow’s models generate a small set of strategic rules, as opposed to the hundreds or thousands that are present in most Security Information and Event Management (SIEM) systems.

It goes one step further than most products do by deciphering the intent of bad actors, and then selects optimized investigation, and prescribes mitigation action accordingly – combined these methods reduce the noise and false positive in security systems...”



Turning What You Have  
Into What You Need.



empow  
You have it in you.

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

[www.empownetworks.com](http://www.empownetworks.com)

