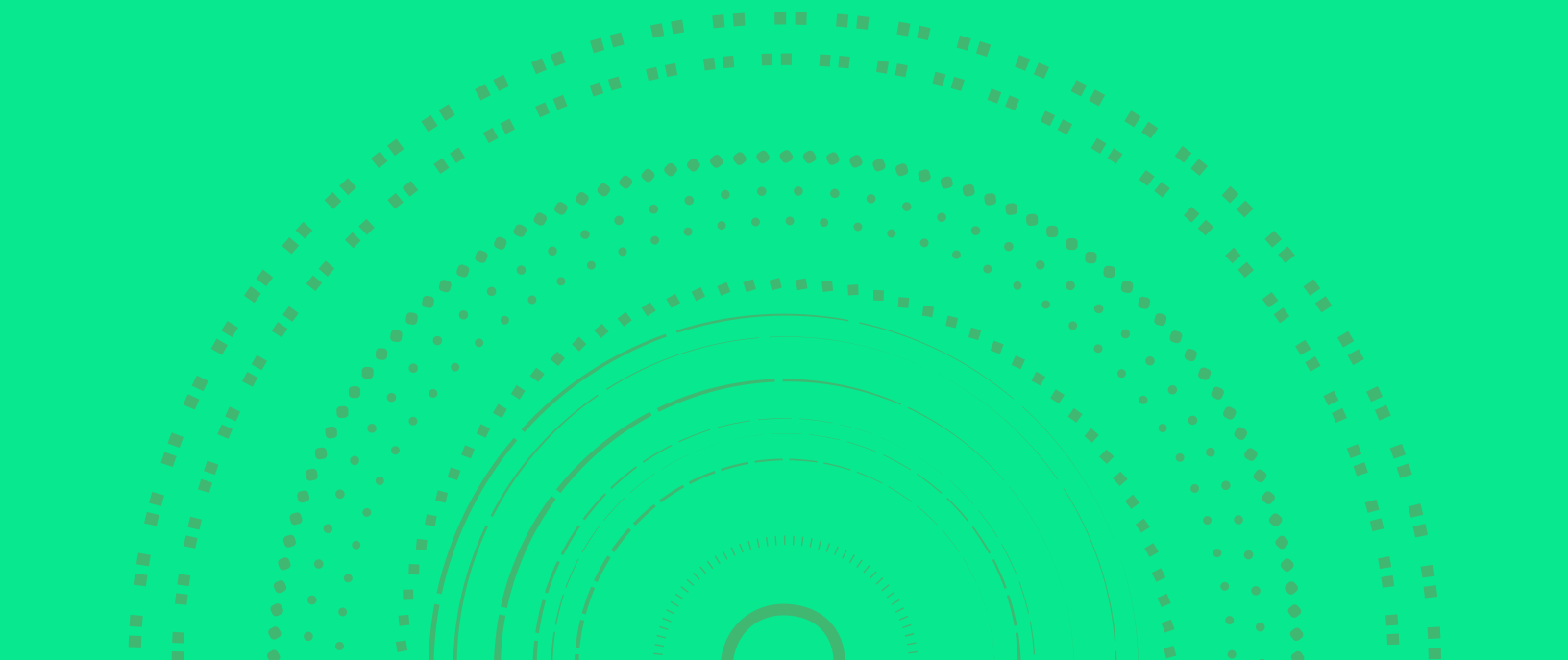
empow

You have it in you.

empow's Security Platform

The SIEM that Gives SIEM a Good Name



Donnelley Financial Solutions

"empow's platform is unique in the security arena... 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."

Dannie Combs, SVP and
Chief Information Security Officer

MIT Media Lab

"As a university, we need to share things, to be open, but still protect our users privacy - this makes us a big juicy target for cyber attackers.

empow's Security Platform allowed us to optimize our security coverage, while ensuring privacy and extending visibility of what is happening in our network"

Michail Bletsas, Director of Network
and Computing Systems

Recognition & Awards

"... Replacing the security Tower of Babel of existing point solutions..."

"empow's unique approach listed among RSA 2017's four distruptive cyber trends."

Forbes

"Breaking through the cybersecurity bubble"

NETWORKWORLD FROM IDG

2017 EDITOR'S CHOICE SECURITY ABSTRACTION SOLUTION CDM

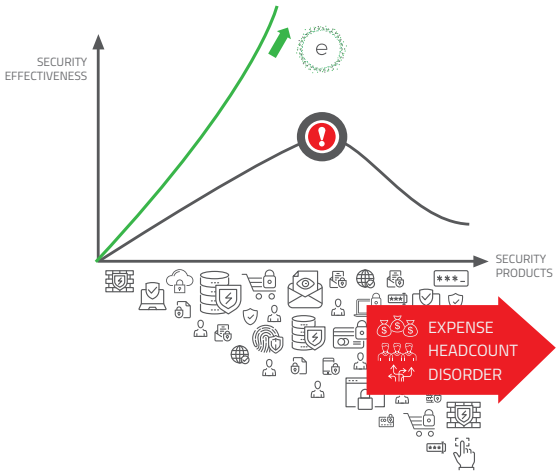
Gartner Cool Vendor 2017

"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..."

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.

SIEM systems were supposed to be the industry's solution to this problem, but they have failed miserably. Today's SIEM systems create more problems than they solve, are very expensive, and ultimately ineffective.

empow's Security Platform is "The SIEM That Gives SIEM a Good Name", and is up-ending the conventional approach that "more is better" by turning your existing security tools into an abstracted security language and layer.

The Platform integrates with your existing network infrastructure and breaks your security tools down into their individual components – what we call **Security Particles**™. This creates a taxonomy of security functions that mirrors advanced attack kill-chain models, and enables modeling targeted defense strategies. Sitting atop of your existing security configuration, empow's Platform – powered by proprietary AI algorithms - then executes these defense strategies throughout the network, automatically deciphering attack intent, and investigating and responding optimally, according to each defense strategy in place. Now you will know that your security is tackling attacks in the right way, every single time, and **turning what you have into what you need.**

The SIEM That Gives SIEM a Good Name

Here's where old SIEM systems have failed, and how empow's Security Platform measures up:

Today's SIEM Solutions	empow's Security Platform
Limited out of the box security coverage	Wide coverage – automatically correlates security logs (no rules required)
Reactive, limited to known attack patterns	Proactive – powerful AI enables constant identification of new attack patterns
No automatic incident response functions	Automated decision-making investigation and mitigation processes
Flood the system with false positives	Reduces noise and false positive rates by an average of at least 90%
High TCO – massive expert involvement, expensive and slow to implement	High ROI thanks to seamless integration and virtually no maintenance costs

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

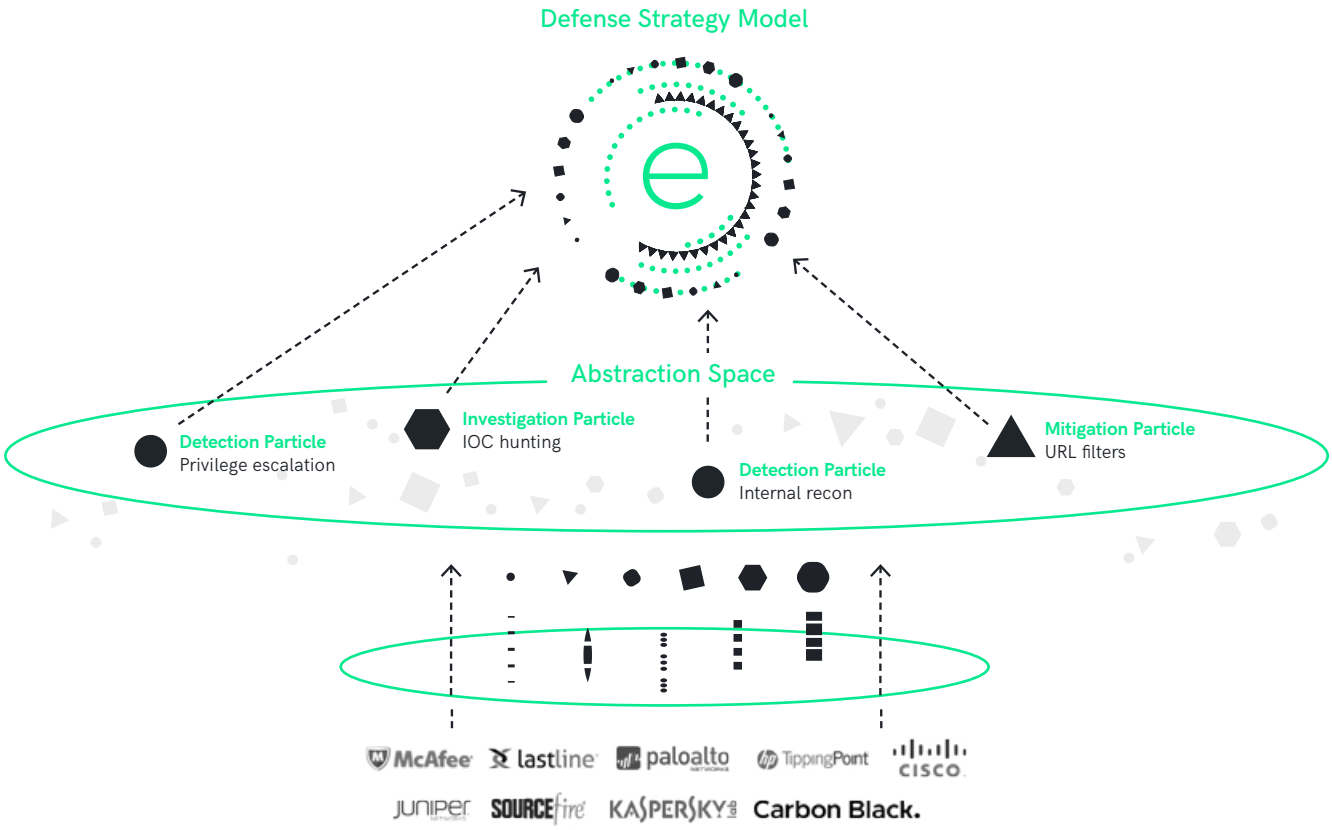
Detection Particles
External reconnaissance
"Call home"
Privilege escalation
Financial data scraping
...

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

Response Particles
Kill process
Uninstall application
NG Firewall rules
ACLs
...

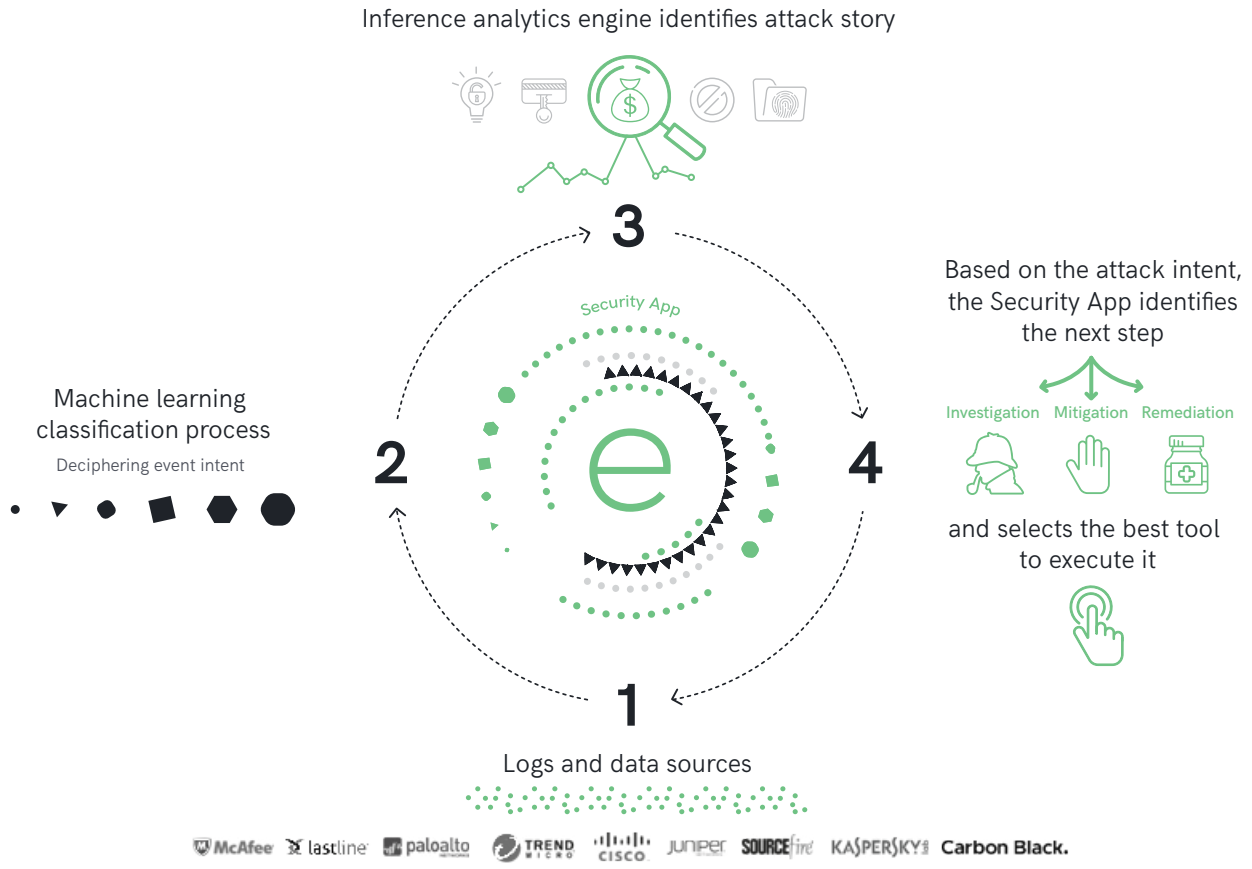
Security Platform

empow's 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: reads the logs, seeks out relevant information from the log itself and from third party data sources outside the organization, and identifies 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

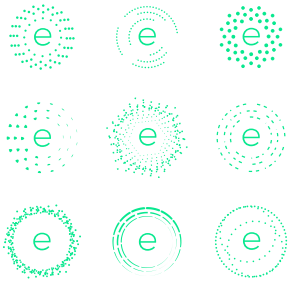
empow's Contextual Orchestration Engine dynamically identifies and selects the best available products and network tools (security particles) to execute the investigation and response actions. This translates into fast and optimal incident response, while at the same time simplifying security operations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

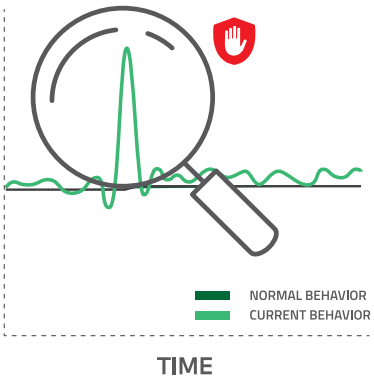


Compliance based apps	Threats based apps	
HIPAA	Advanced Ransomware	Financial Data Leak
PCI DSS	Insider Threat	PII Data Leak
EU GDPR	Intelligence Gathering	Data Manipulation
NYCRR 500	Service Disruption	

empow Network Traffic Behavioral Analysis Engine

empow's solution comes with an out-of-the-box network behavioral analysis engine 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.

McAfee lastline paloalto TREND MICRO CISCO JUNIPER SOURCEfire KASPERSKY Carbon Black.

Threat Analytics Reporting and Security Diagnostics

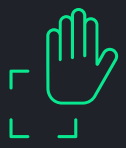
The empow Security Platform provides advanced threat analytics and security diagnostics. These include both analytics into the different threats targeting the organization – injecting threat management visibility into the organization's security posture as well as detailed diagnostics covering security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

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

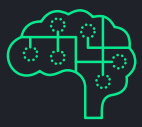
empow's Security Diagnostics Service also allows organizations to test various "what-if" scenarios, such as assessing the success of the architecture when a certain product is disabled, and providing a score for each product within the context of various risks. For more information, please refer to our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



Identifies and mitigates advanced threats missed by single (siloed) tools.



Directs, automates and accelerates optimal incident response based on attack intent.

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.

Turning What You Have Into What You Need.

empow
You have it in you.

Tel: +1-630-362-7231
NGIN Workplace, suite 201, 210 Broadway
Cambridge, MA 02139

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

www.empownetworks.com