WHAT IS THE EFFORTLESS DEFENSE ADVANCED THREAT DEFENSE PLATFORM?

The Effortless Defense Advanced Threat Platform is the software solution that:

- Continually monitors the network traffic to detect advanced threats.
- Assesses risk to an organization based on the threat severity and local context.
- Provides threat containment by leveraging existing enforcement infrastructure of Firewalls, Secure WEB Gateways and IPS.

What are the key benefits of the Effortless Defense Solution?

The Effortless Defense Advance Threat Defense Platform Delivers:

- Accurate detection for advanced and evasive threats across Windows, Mac, and Mobile platforms with integrated support for WEB and Email Protocols.
- Distributed Software Architecture for wide and deep visibility into the threat across the organization.
- Speedy resolution and containment of threats using risk based prioritization within existing enforcement devices.
- Flexible Deployment and integration with existing IT Infrastructure.

How is the Effortless Solution Deployed?

The Effortless Defense Solution is available as a software that can be deployed on bare-metal core servers or as a VM in virtualized environments. There are two major components within the solution- the core and collectors.

Collectors: are lightweight components that are deployed across the organization to collect potential Malware carrying objects and threats across the network and send information to The Core.

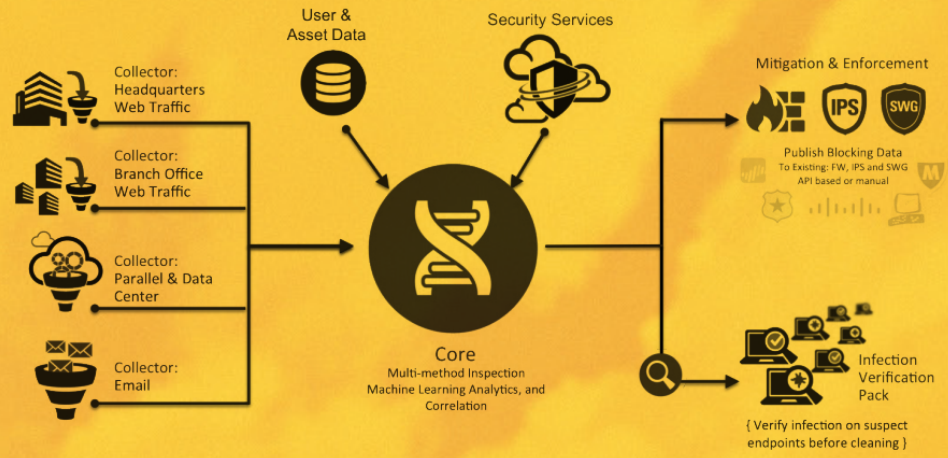
The Core: is deployed in centralized location and provides detection and mitigation functions.

How does Effortless Defense provide prioritization of threats?

Effortless risk-based prioritization is based on the following:

- Multiple related alerts are tied into threat incidents.
- Inherent severity of the threat, i.e. its capabilities, adversaries behind the threat intent
- Asset value of the targeted assets.
- Security posture of the devices e.g. OS version, anti-virus etc.
- Lifecycle stage of the threat e.g. Exploit, Download, Infection, Data Exfiltration.

The Effortless Defense Advanced Defense Platform



How does Effortless block or contain the threat activity?

The Effortless solution works with your existing Firewalls, Secure WEB Gateway, and IPS devices by pushing and blocking IP addresses, URL's and signatures to these devices programmatically or with manual intervention, if desired.

How is Effortless Defense different?

The Effortless Defense is a solution developed to detect advanced persistent threats, Zero Day Malware and targeted attacks specifically to address many of the shortcomings of the Firewall solution:

Deployment: Expensive appliances for every network location vs. distributed software Collectors, licensed by overall bandwidth for the site.

Detection: Selective Analysis of downloaded objects vs. analysis of every object.

Evasion: Other solutions are unable to detect threats that are sandbox aware of encryption and other types of obfuscation techniques.

Validation: Other solutions do not offer validation of endpoint infection resulting in malware investigations and unnecessary re-imaging of hosts.

Threat Prioritization: Other solutions can send hundreds of threat alerts without providing necessary context for risk based prioritization resulting in costly and lengthy remediation.

Containment and Mitigation: Other solutions provide limited blocking capabilities for known threats and require to be placed in line with no proactive protection. The Effortless solution by contrast uses existing environment devices for blocking threat activity across the organization, not just the location where the threat was detected.

	EFFORTLESS DEFENSE	MASERGY	FIREEYE	DAMBELLA	TREND MICRO	ANTIVIRUS + IDS/IPS
INBOUND: Analysis and prevention of inbound threats (Malware, infected objects)						
Known malware detection (signatures & heuristics)	✓	✓	✓	✓	✓	✓
Dynamic, on-demand analysis of malware, torjans and droppers (sandbox)	✓		✓	✓	✓	
Dynamic analysis of documents with embedded exploits (PDF, Office Docs,...)	✓	✓	✓		✓	
Detailed forensics for both malware binaries and web threats (exploits)	✓	✓	✓			
High resolution malware analysis (monitoring execution from the inside)	✓	✓				
Support for multiple OS (Windows, MAC OS, Mobile)	✓	✓		✓		
Collect live threats via customer crowdsourcing	✓	✓	✓	✓	✓	✓
Collect live threats via active threat discovery	✓	✓				
Flexible malware analysis in the Cloud	✓	✓		✓	✓	
Multi-method engine with machine learning	✓	✓				
Integrated web and email detection	✓	✓				
Workflow of mitigation and remediation	✓	✓				
Anti-evasion and anti-armoring technology	✓					
Behavioral Analysis based on Machine Learning as opposed to signature / rules based learning	✓					
Advanced Persistent Threat and Malware detection with Sandbox detonation to protect Customer Environment	✓					
INTERNAL: Outbound, Lateral, Network visibility, blocking of C&C connections and data leakage						
Content rules and signatures to block known, malicious traffic	✓	✓	✓	✓	✓	✓
Reputation analysis (URLs, Ips) to block traffic to known bad sites	✓	✓		✓	✓	✓
Identifies anomalous network activity (domain generation, fast flux)	✓	✓		✓		
Detect and block attack behavior (spam, DoS)	✓	✓		✓	✓	✓
Abstract malware communication pattern detection (network fingerprints)	✓	✓				
Multi Vector Inspection of Web Traffic, Email Traffic, and File Sharing Traffic within the most trusted zone of the network	✓					
Detects Lateral malware propagation that evades perimeter security controls	✓					
Rapid containment and remediation to reduce long term exposure	✓					
CONFIGURATION FLEXIBILITY						
Deployment Options	✓	✓	✓	✓	✓	✓
Proprietary hardware appliance	✓	✓			✓	
Virtual appliance (for specific environments)	✓	✓				
On-Premise: Customer facility or Colocation Data Center	✓	✓				
Platform is built on a restful API architecture and can easily integrate with existing security services	✓					
Agentless deployment without adding load to compute or latency to network	✓					
SUPPORTED NETWORK SPEED						
>20 Mbps egress	✓					
100 Mbps egress	✓	✓				
1 Gbps egress	✓	✓	✓	✓	✓	✓
10 Gbps egress	✓	✓		✓		