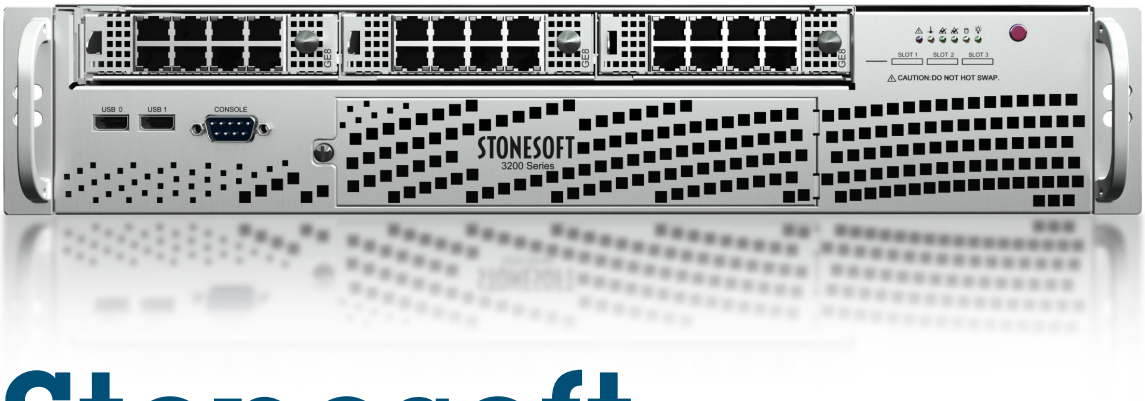


Stonesoft Evasion Prevention System 5.6

Datasheet

- The purpose-built network security product that provides real-world protection against Advanced Evasion Techniques.
- Unique and thorough data stream based normalization and inspection across all protocols and network layers.
- Successfully tested against over 800 million Advanced Evasion Techniques.
- Affordable, easy and fast deployment with no migration process or infrastructure changes required.
- "Infrastructure patch" without compromising network performance.

STONESOFT
A McAfee Group Company

Stonesoft Evasion Prevention System (EPS)

Advanced Evasion Techniques – why worry?

The number of closely targeted and sophisticated cyber-attacks is getting higher. Attacks made by highly motivated (APT) hackers and cyber criminals are in the news every day. Those hackers and cyber criminals are using Advanced Evasion Techniques (AET) to protect their investments, lower the possibility of failure and to maximize success rates and gains. Advanced Evasion Techniques are playing a bigger and bigger role in hacking strategies. If an attacker knows the target host is protected by state-of-the-art security devices and 24/7 security processes, they need to use AETs in order to avoid detection. Simple exploits will fail. By definition, AETs are methods of delivering an exploit or malicious content into a vulnerable target so that the traffic looks normal and security devices will pass it through. It falls into the very same category as Social Engineering, Phishing, Day Zero Exploits, backdoors, etc. All are meant to make the implementation of the cyber attack successful. And the delivery and hacking strategies will not harm per se, but combined with the exploits, they can infiltrate a vulnerable target easily.

What is the Problem? A fundamental design flaw

Currently, a majority of the Network Security products that are supposed to do network traffic inspection and detect/block malicious content and exploits are ineffective and blind to detect, stop and report Advanced Evasion Techniques. The easiest way to self-assess if your network infrastructure is vulnerable (or not) to AETs is to download the free Evader evasion testing software (evader.stonesoft.com) and test in your own environment with your own configurations and security policies.

Many next generation firewalls and intrusion prevention systems are still doing (1) packet-based inspection without doing proper, full-stack traffic normalization before the inspection. Either because they have limited memory or performance capacity or the inspection process is designed incorrectly. (2) Detection and blocking of exploits/malicious content directly from the non-normalized traffic with pattern match processing and signatures leads easily to false positives. In order to avoid that many products do (3) as limited inspection as possible (horizontal snapshots of the traffic). They also try to do the very same with evasions. This will never work as the number of possible evasions is virtually limitless. In many cases these products are also designed to provide high throughput performance. (4) Processes are accelerated with hardware (ASIC) and security processes optimized and streamlined to minimum levels. This leads to static security with high throughput performance and, at the same time, the product becomes incapable of processing data properly and its anti-evasion capabilities are sacrificed.

Due to these fundamental design flaws most current (and leading) security appliances do not provide protection if AETs are used against them. In other words, enterprises and organizations with high-value network infrastructure that rely on next generation firewalls (NGFW), intrusion detection/ prevention systems (IPS) or unified threat management (UTM) systems are left vulnerable.

If your organization has something valuable in digital form, such as data or systems, that are connected to networks, AETs can make them an easy target for hackers. Taking the threat seriously and acting upon the latest AET research and knowledge can be a smart decision for any organization.

How to mitigate the risk? Stonesoft's three steps approach

Stonesoft's new Evasion Prevention System (EPS) is designed to protect valuable digital assets and information against advanced cyber-attacks that use AETs to deliver malicious exploits. The EPS acts as a physical patch to vulnerable infrastructure.

As a modular add-on product, the Stonesoft EPS is fast and easy to deploy to any network infrastructure and does not require any infrastructural change or migration project. It is also highly affordable due to a customer friendly Service Provider License Agreement (SPLA) pricing model. Based on customer preferences it can be a CAPEX investment or OPEX cost. In Phase Two, the Stonesoft EPS can be upgraded to act as a full-blown Stonesoft Security Engine, including next generation firewall, intrusion prevention and evasion prevention capabilities or standalone Next Generation IPS or FW licences. This lengthens the product life-cycle and improves ROI. The outcome is a simplified network security infrastructure and better security at a lower total cost.

High AET protection without a performance trade-off

The Stonesoft Evasion Prevention System is a layer-2 network security deployment which logs and reports evasions through the Security Management Center. It is uniquely based on a data stream based normalization and inspection process across all protocols and network layers (full stack). The vulnerability-based detection/blocking is done after normalization and evasion removal. The EPS has an intelligent DFA, 64-bit memory system that enables a highly effective data stream normalization process that doesn't have significant effects on network throughput performance.

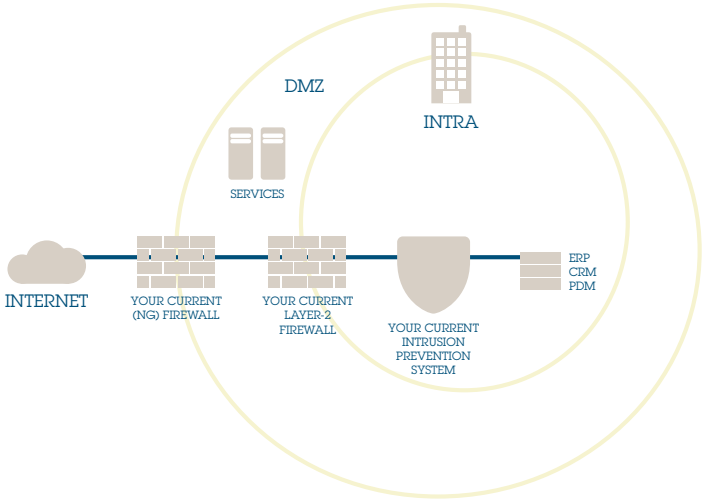
The Stonesoft EPS has been successfully tested against over 800 million Advanced Evasion Techniques and combinations. Stonesoft runs almost two million evasion test runs on a daily basis.

The EPS comes with an enterprise-grade management system license. And being a 100% software-based security appliance, the Stonesoft EPS is capable of receiving new updates and upgrades automatically and dynamically as new advanced evasion techniques are found and new cyber threats occur.

Deployment Scenarios

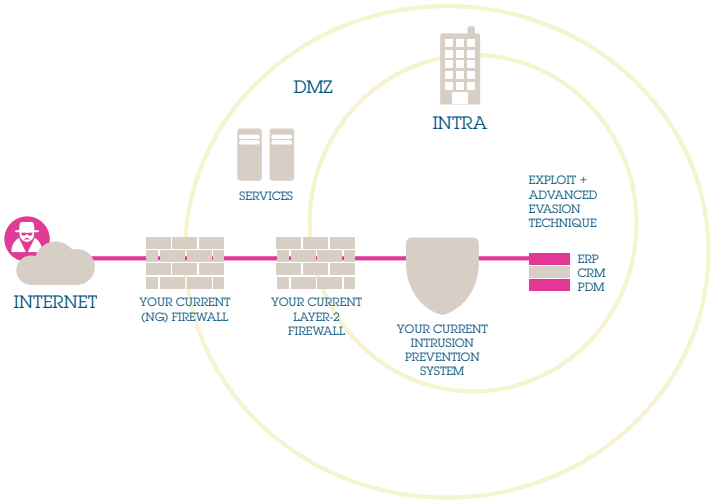
Current Deployment

Non-Stonesoft environment



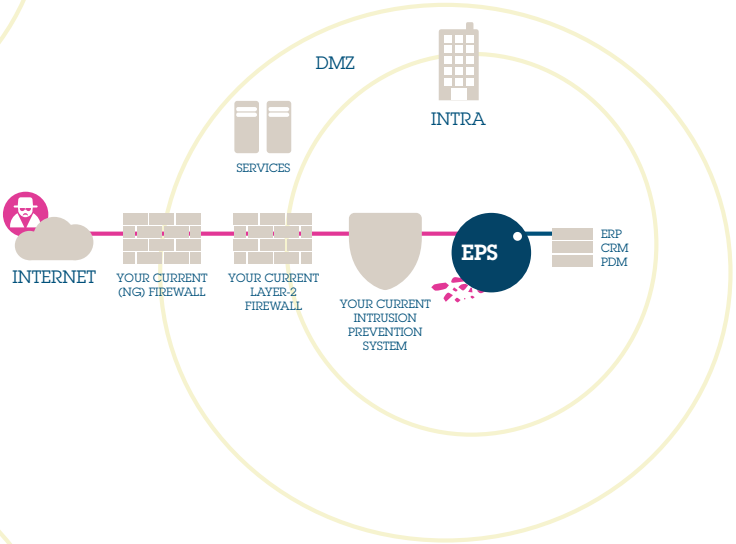
AET Cyber Attack

AET + exploit bypassing security products without leaving traces



Phase 1: AET risk mitigation and management

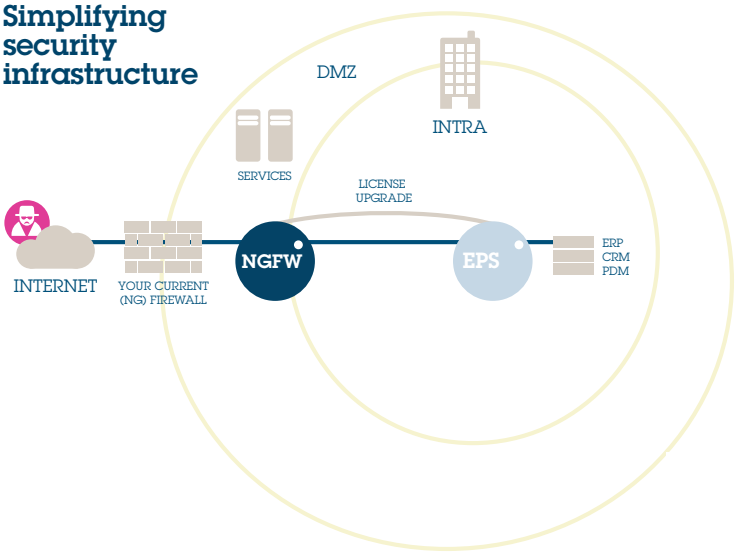
Outcome: Evasion-Proof Infrastructure



Phase 2: AET risk mitigation and management

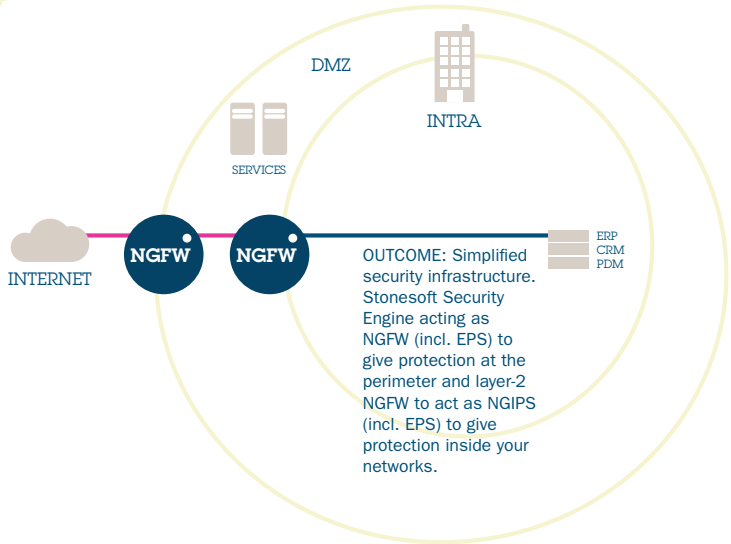
Migration to gain Savings

Simplifying security infrastructure



Phase 3: AET risk mitigation and management

Network Security Simplified & AET Risk Managed



EPS 5.6 Specifications

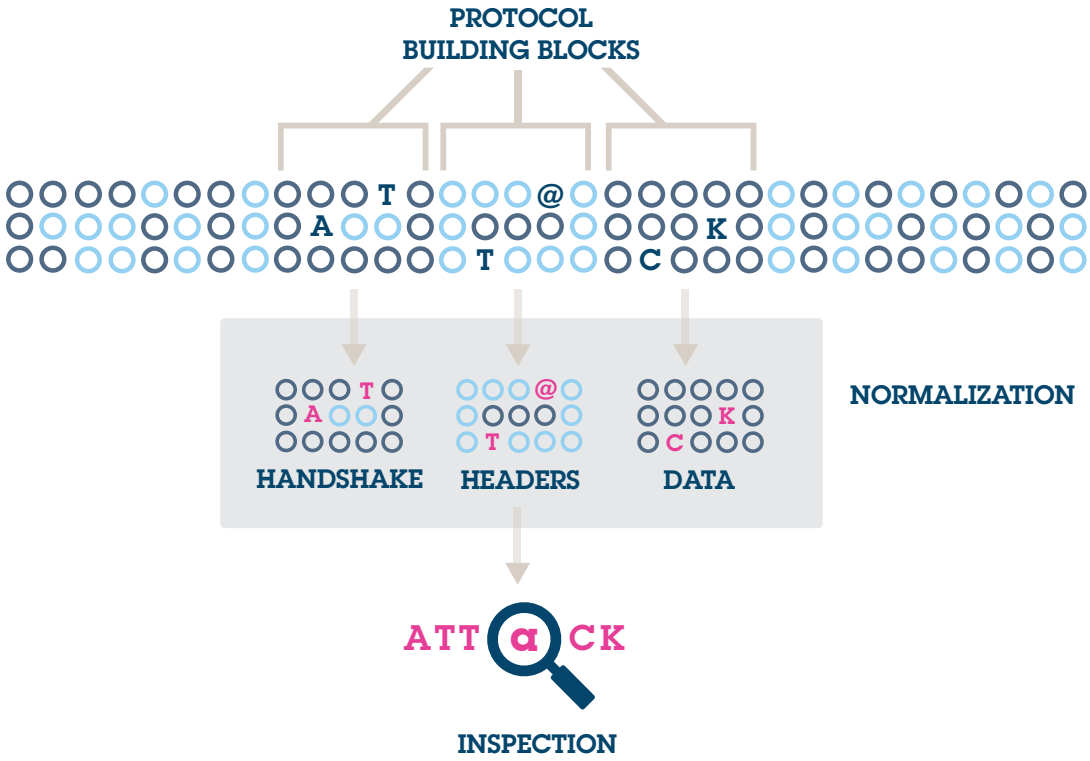
GENERAL	
Supported Platforms	
Stonesoft Appliances	1302, 3206 appliances
Operating modes	Layer 2 Evasion Prevention System

LAYER 2 SPECIFIC FUNCTIONALITY	
General	Advanced Evasion Techniques protection / Data stream normalization Logical interface matching for VLANs and physical interfaces
High availability	Serial clustering (active-active) Link-redundancy (active-passive) Fail-open interface support (IPS) Dynamic inspection overload handling

GENERAL FUNCTIONALITY (ALL OPERATING MODES)	
Encapsulation	Ethernet (Dix / IEEE), 802.1q VLAN
Policy matching	Interface zones Time TLS information Domain names Applications
Traffic management and QoS	Policy-based traffic shaping Guaranteed / maximum / bandwidth prioritization Differentiated Services Code Point (DSCP) matching / marking Concurrent session limiting
Inspection	
Dynamic context detection	Protocol Application File type (Flash, GIF, JPEG, MPEG, OLE, PDF, PNG, RIFF, RTF, text file, binary file)
Protocol normalization	Full protocol normalization for Ethernet, IPv4, IPv6, ICMP, UDP, TCP, DNS, FTP, HTTP, IMAP, IMAPS, SMTP, SSH, NBT, SMB, SMB2, MSRPC, POP3, POP3S, SIP, TFTP, HTTPS, GRE, IP-in-IP, IPv6 encapsulation
Protocol specific fingerprint inspection	DNS, FTP, HTTP, HTTPS, IMAP, SMTP, SSH, NBT, SMB, SMB2, MSRPC, IMAP, IMAPS, POP3, POP3S, SIP, TFTP
Protocol independent fingerprint inspection	Any TCP / UDP protocol
Evasion and anomaly detection	Multi-layer traffic normalization Vulnerability-based fingerprints Exploit-based fingerprints Fully upgradable software based inspection engine Evasion and anomaly detection Tested against over 800 million advanced evasion techniques
Custom fingerprint inspection	Protocol independent fingerprint matching Regular expression-based fingerprint language Snort ® signature converter Custom application fingerprinting
TLS inspection	HTTPS client and server stream decryption and inspection TLS certificate validity checks Certificate domain name based exempt list
Correlation	Local correlation, log server correlation
DoS/DDoS protection	SYN/UDP flood detection Concurrent connection limiting, interface-based log compression RTSP under Firewall protocol agents
Reconnaissance	TCP/UDP/ICMP scan, stealth and slow scan detection in IPv4 and IPv6
Blocking methods	Direct blocking, connection reset, blacklisting (local and distributed), HTML response, HTTP redirect
Traffic recording	Policy based traffic recordings, automatic excerpts from misuse situations

Updates & upgrades	Automatic dynamic updates through Security Management Center (SMC). Current coverage over 3000 protected vulnerabilities.
Web filtering (subscription required)	
Protocols	HTTP, HTTPS
Engine	Category based URL filtering, Blacklist / exempt list
Database	Over 280 million top level domains and sub pages (total billions URLs) Support over 43 languages 82 Categories
Management and Monitoring	
Centralized Management	Enterprise level centralized management, logging and reporting system. See more details from Security Management Center datasheet
SNMP monitoring	SNMPv1, SNMPv2c and SNMPv3
Traffic capturing	Console tcpdump, remote capturing through SMC
High security management communication	256-bit security strength in engine – management communication

PLATFORM CERTIFICATIONS	
ICSA Labs	Network IPS enterprise certified
NSS Labs Tested	Network Intrusion Prevention, Next Generation Firewall, Firewall
VMware	Virtual appliance VMware ready certified
RSA	Secured by RSA certified with RSA SecureID and RSA envision
Arcsight	Common Event Log format (CEF) certified
Q1Labs	Log Event Enhanced Format (LEEF) certified



Stonesoft Corporation International Headquarters
Itälahdenkatu 22A FI-00210 Helsinki, Finland
tel. +358 9 4767 11 | fax. +358 9 4767 1349
www.stonesoft.com

STONESOFT
A McAfee Group Company

Stonesoft Inc Americas Headquarters
1050 Crown Pointe Parkway, Suite 900
Atlanta, GA 30338, USA
tel. +1 866 869 4075 | fax. +1 770 668 1131