anubisnetworks™
a BITSIGHT® company

DYNAMIC MALWARE ANALYSIS
integration with
MAIL PROTECTION SERVICE (MPS)

Email security solutions leverage techniques and tools such as antispam, antivirus, IP reputation, and many other security filters to protect your organization. However, these won't stop today's new breed of attacks, which are sophisticated enough to mask themselves through tunneling or encryption. Our Dynamic Malware Analysis will work cooperatively with the email security technologies, as a strengthened layer of defense.

At **AnubisNetworks**, we've partnered with Check Point Software Technologies to bring you their sandbox technology, **SandBlast Threat Emulation**. SandBlast boasts the most accurate sandboxing engine available to protect your organization from attackers before they enter your network. SandBlast Threat Emulation prevents infections from new malware and targeted attacks using innovative zero-day threat emulation capabilities to deliver the best possible catch rate for threats, being virtually immune to attackers' evasion techniques.

By adding Email **Dynamic Malware Analysis** to your security, you will be obtaining an extra layer of protection with the ability to detect very recent malicious code, by exposing its intentions in a computer sandbox - equipped with all the latest anti-sandbox/anti-vm counter measures.

The problem with traditional sandbox solutions is that they only detect malware behavior at the OS level. In some cases, this will mean the exploitation has already occurred and the malicious code is already running. With SandBlast Threat Emulation, the detection takes place at the CPU level, monitoring the instruction flow to detect exploits attempting to bypass OS security controls.
Therefore, **attacks are stopped before they have a chance to launch**.

Dynamic Malware Analysis

This technology allows AnubisNetworks to provide a new Dynamic Malware Analysis filtering module within AnubisNetworks' Email Security Gateway.

SandBlast capabilities in our Mail Protection Service (MPS) defense layer are:

Sandblast Zero-Day Protection
The SandBlast Threat Emulation technology employs the fastest and most accurate sandboxing engine available to clean active content in files, protecting your organization from attackers before they enter your network. Moreover, simulate session context to detect malicious Flash objects.

Evasion Resistant Detection:
Traditional sandbox solutions detect malware behavior at the OS level – after the exploitation has occurred and the hacker code is running. They are therefore susceptible to evasion. SandBlast Threat Emulation capability utilizes a unique CPU level inspection engine which monitors the instruction flow at the CPU-level to detect exploits attempting to bypass OS security controls, effectively stopping attacks before they have a chance to launch.

Artificial Intelligence (Machine Learning Engines):
Look at the full context of the inspected element, extract parameters from the environment. Check Point Software was named a Leader in Endpoint Security Suites by Independent Research Firm (Forrester Research). SandBlast received the highest possible scores in the Malware Prevention.

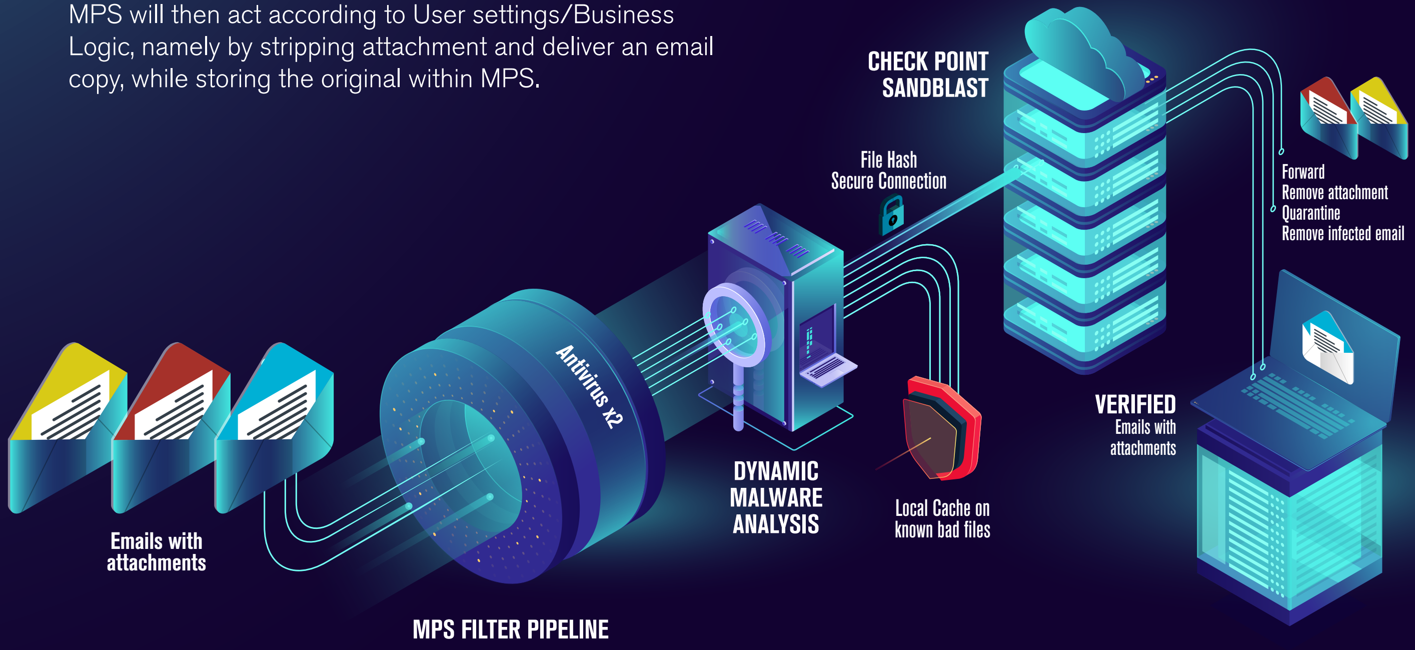
anubisnetworks™
a BITSIGHT® company

MPS' Dynamic Malware Analysis

Dynamic Malware Analysis is the ultimate MPS filter for last resort verification on infected attachments.

MPS will use local awareness on such files or resort to Check Point's secure cloud for inline (<10 minutes) assessment.

MPS will then act according to User settings/Business Logic, namely by stripping attachment and deliver an email copy, while storing the original within MPS.



FOLLOW US

- facebook.com/anubisnetworks
- twitter.com/anubisnetworks
- linkedin.com/company/anubisnetworks
- youtube.com/anubisnetworks

LISBON

Address
Centro Empresarial e Comercial Espaço 7 Rios
Escritório 50 (0.04), Piso -1
Rua de Campolide, Nº 351
1070-034 Lisbon, Portugal
Phone: +351 217 252 110

BOSTON

Address
111 Huntington Ave
Suite 2010
Boston, MA 02199
USA
Phone: +1 617 245 0469

www.anubisnetworks.com
info@anubisnetworks.com