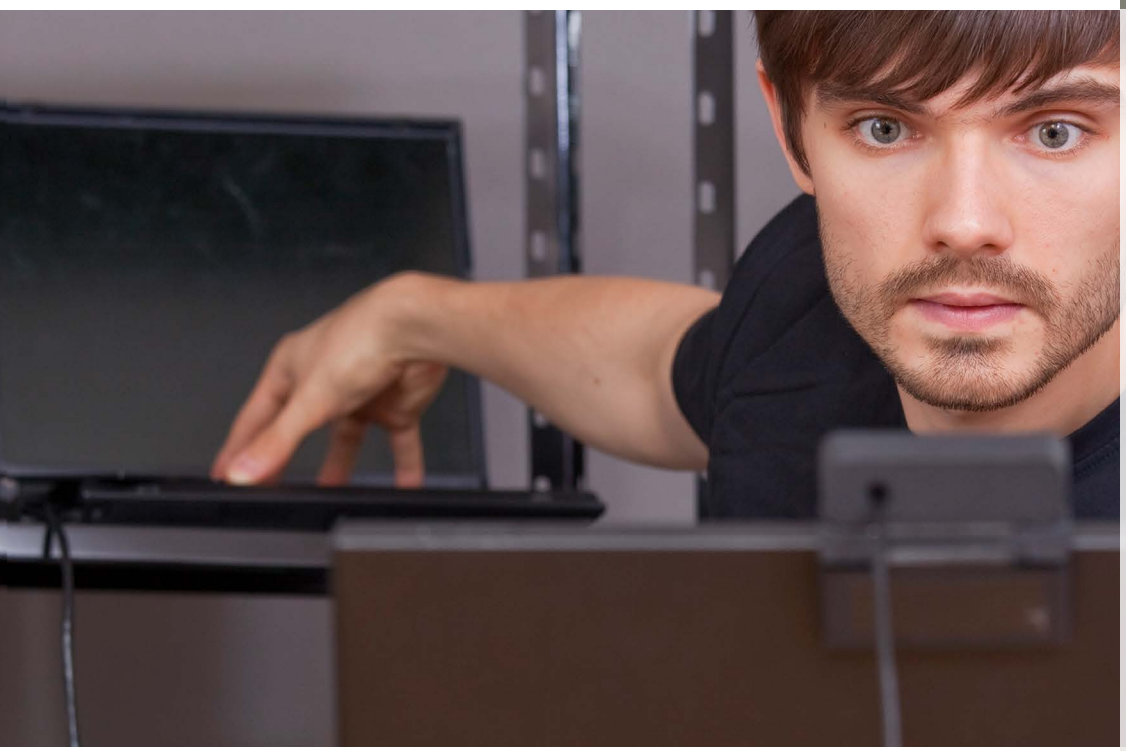


ADVANCED THREAT PROTECTION

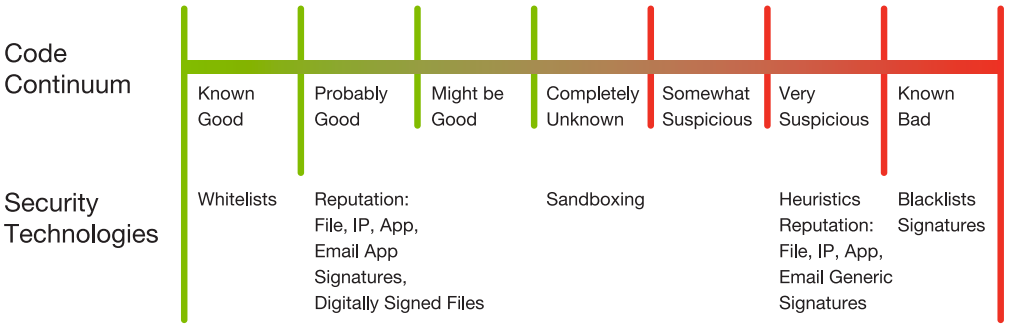
Protect your organizations against advanced attacks. Sandboxing is able to detect threats that other security may miss by coaxing those threats into exposing themselves.

Why Do You Need Sandboxing for Protection?

Organizations breached by Advanced Persistent Threats (APTs) are all over the news and sandboxing is the latest hot thing being touted to protect you from APTs. Why? Why sandboxing? What does a sandbox solution give you that you don't already get from your existing layers of security?

A Sandbox gives you a chance to see into the future, into the unknown.

We don't live in a black and white world, where everything is known to be good or bad. The code that runs over your network spans a continuum from known good code to known bad or that includes malicious code. A lot is simply unknown. You are likely already running a number of security technologies to help protect your organization from malicious code and you are probably running technologies that help you identify good code. However, like most organizations, you are still at risk from the unknown. And that unknown gap in the code continuum is a significant one.



Benefits

- Prevent data breaches caused by advanced attacks
- Detect advanced persistent threats
- Expose previously unknown malware
- Block more spearphishing attacks
- Increase effectiveness of your NGFW, or UTM or Secure Email Gateway solution

POWERED BY FORTIGUARD.

The 2014 Verizon Breach Report confirmed 1,367 security breaches and over 63,000 security incidents in 2013. Sandboxing finally gives you a method to close the gap, to identify previously unknown attacks that traditional security technologies may not detect.

How does sandboxing fit into the many layers of security I have already?

Consider the lifecycle of an attack and how security technologies play a part in protecting an organization.

- **Step 1:** An attacker starts with reconnaissance on the target. They then craft a clever email, often with a malicious link (or file) in it. And send the email to the target. This is where your antispam/antiphishing solution may block the email. But if it doesn't: the email goes to the target where the attacker hopes the target will click on the malicious link.

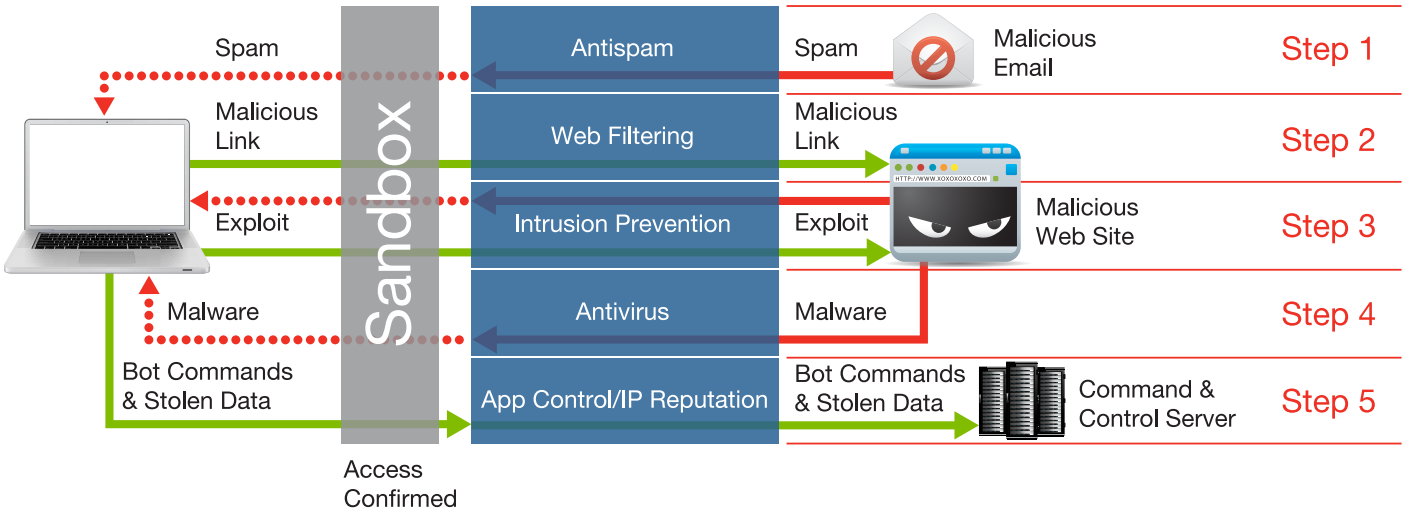
- **Step 2:** If the target clicks on the link, traffic will go out to a web site to establish communication. This is where your web filter may block the traffic but if it doesn't: that malicious web site starts attacking your organization.

- **Step 3:** The malicious web site will usually launch exploit attacks at the target to gain access to the system. This is where your intrusion prevention system (IPS) attempts to block the attack, but if it doesn't: a tunnel is opened up and the malicious site can launch malware into your organization.

- **Step 4:** With malware seeking entry, ideally your antimalware will protect you, but if it doesn't the attacker gets executable code into your system where it can run.

- **Step 5:** Once the malicious code is running, it usually looks to access credentials, move laterally in search of sensitive data and collect/stage it within your organization. But in order to complete its mission, it needs to exfiltrate that data out to a command & control server. This is where your application control, IP reputation, botnet and other protections come into play. But if these technologies don't block this traffic: You are breached.

Antispam, web filtering, IPS, antivirus, app control and IP reputation techniques are necessary protection but will not stop the most sophisticated attacks today. They rely on identifying known (even if broad-based) indicators of attack, whether through signatures, heuristics or reputation methods. The danger comes when an attack is brand new or is able to mask itself through tunneling, encryption or other evasion methods. If you add sandboxing to your security mix you add a layer of protection that can detect malicious code even if it is previously unknown by teasing it into exposing itself in the sandbox.



What is Sandbox?

A sandbox is a safe isolated environment that replicates an end user operating environment where you can run code, observe it and rate it based on activity rather than attributes. You can run executable files, allow contained network traffic and more that can contain hidden malware in a sandbox. The sandbox provides a safe environment in which to execute and observe malicious code such as file/disc operations, network connections, registry/system configuration changes, etc.

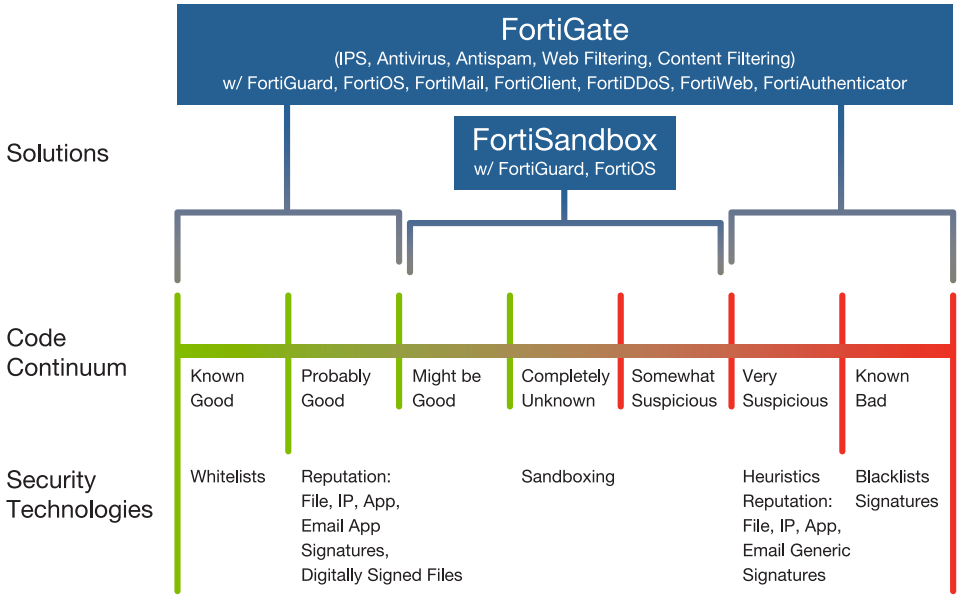
What makes the FortiSandbox so fast and effective?

FortiSandbox aims to replicate the behavior of real end user systems in order to execute and even accelerate malicious code as it is intended to run in order to detect it. In order to assess malware, sandboxes will run multiple code evaluation processes with different operating systems and technologies. FortiSandbox prioritizes code evaluation processes by how prevalent malware is in different configurations in order to speed up the identification of malicious code.

FortiSandbox is a detection tool that works best in conjunction with the enforcement capabilities of established threat prevention capabilities like a next generation firewall (NGFW) or unified threat management (UTM) system, as well as secure email gateway or endpoint protection platform. In Fortinet's case, such solutions cover the ingress, egress and internal inspection points and thus can proactively prefilter traffic to catch what it can (based on what's known or highly suspected) and prioritize the unknown or unsure traffic that should go to the FortiSandbox for additional inspection. This cooperative approach allows each product to specialize in what it does best. For example, the sandbox doesn't have to spend time working on traffic and threats that can be blocked first with other technologies.

While there are many proprietary technologies at play in the Fortinet solution, there is one particularly critical piece that plays a major role in proactively preventing advanced malware, Fortinet uses a patented Compact Pattern Recognition Language (CPRL) developed by FortiGuard Labs to perform deep-inspection on code. This language can identify 50,000 or more disguises used by known malicious code. If code is using a known evasion technique, CPRL can discover it and the FortiGate can identify the code without sending it to the sandbox. This valuable step boosts performance by reserving the sandbox resources to work on code that is unknown. This technology is a core component of our Flagship FortiGate as well as FortiMail and FortiClient offerings and is the reason these solutions routinely earn top marks in third party tests like those from Virus Bulletin, AV Comparatives and others.

For additional detection of the most sophisticated threats, Fortinet has packaged up the advanced analysis techniques from FortiGuard Labs in the FortiSandbox, which demonstrated 99% breach detection, identifying the majority of breaches in under a minute, in the NSS Labs 2014 Breach Detection Systems report.

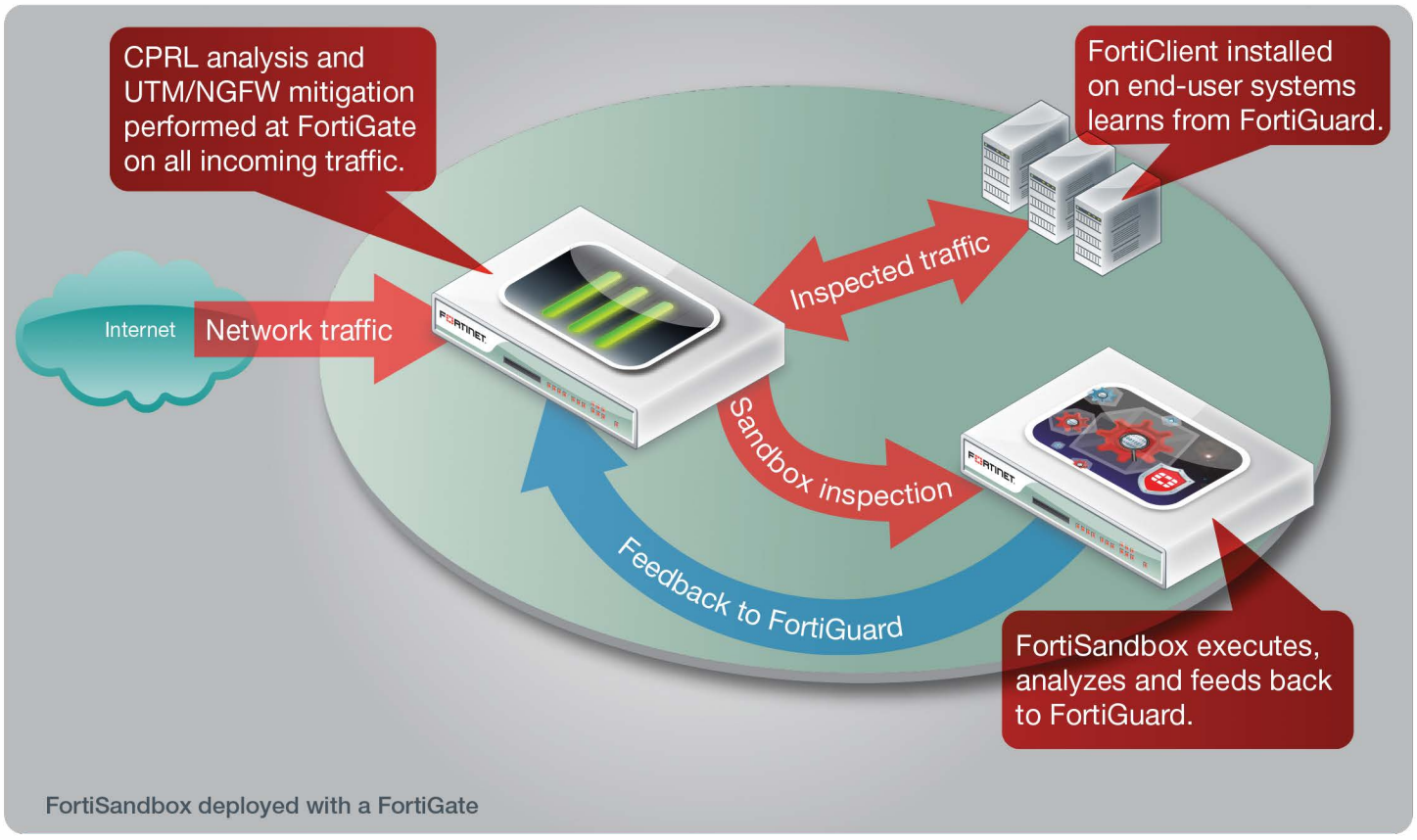


How do I choose the best sandbox for me?

You want a sandbox that effectively detects breaches and can detect them quickly. Make sure you choose a sandbox solution that's been independently tested and rated, don't just rely on vendor claims for effectiveness and performance. You also want your sandbox solution to work cooperatively with the rest of your network security technologies. Sandboxing doesn't replace your in placet antispam, IPS, antivirus, web filtering, IP reputation and application controls within next generation firewalls, secure email gateways and endpoint protection platforms. Your sandbox should work cooperatively with these technologies to provide an additional layer of protection that can be managed as part of a coordinated defense.

Finally, sandboxing is resource intensive and solutions from different vendors vary widely in cost. Make sure your sandbox solution delivers the security you need at a good value.

For more information on Fortinet sandboxing, please go to http://www.fortinet.com/products/fortisandbox/index.html.



FortiSandbox deployed with a FortiGate

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480