

# Fortinet Advanced Threat Protection (ATP) Talking Points

## Overview

- With data breaches from advanced malware continuing to make headlines, businesses are seeking ways to improve security/reduce risk.
- Sandboxing is the “hot” (and essential) technology that should be added to existing security infrastructure.
- However, Fortinet actually recommends that a sandbox extend traditional security components, so there can be “hand-offs” between Prevention, Detection and Mitigation- this is our ATP Framework.
- Further, it should add local intelligence to a broader Security Fabric that is scalable, aware, secure, actionable and open.

## Did you know?

- For the 3<sup>rd</sup> year in a row (2014, 2015 and now 2016!), preventing/detecting APTs is the top IT security priority...and higher than ever before.
- According to the 2016 Verizon Data Breach Investigations Report (DBIR), only 20,000 of 3,000,000 pieces of malware investigated (<1%) were seen by more than 1 organization. And 99% of malware is seen for 58 secs or less.
- Detecting these unique pieces of malware requires local sandboxing, as they are often finished running before global analysis and preventive signatures.
- FortiSandbox detected more than 99%+ of unknown malware during independent, real-world testing by ICSA and NSS Labs respectively (2016).
- FortiSandbox Cloud demonstrated the fastest average detection time in the 2016 NSS BDS Testing at 4.1 minutes.
- In a recent survey, Forrester found that sandbox users would like integration with 6 other security products and a high degree of automation.
- FortiSandbox deploys as an integrated extension of FortiGate, FortiWeb, FortiMail and FortiClient for easier deployment and automated mitigation as well as updated protection.
- Fortinet is the only ATP solution NSS Recommended from Edge to Endpoint (NGFW, WAF, EPP and Sandbox) for both cloud and appliance deployment.
- The Fortinet Cyber Threat Assessment Program now includes FortiSandbox analysis to identify the most sophisticated attacks.

**FORTINET**®

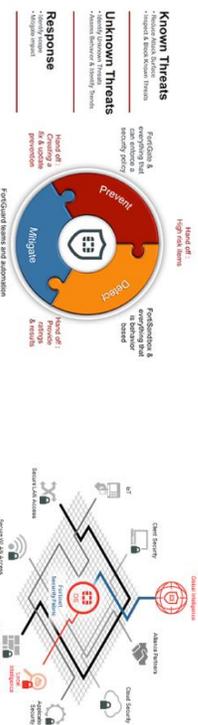
## The Highlights

- ICSA Certified and NSS Labs Recommended Sandbox.
- Integrated, top rated prevention components- NSS Recommended NGFW, DCIPS, WAF and EPP, VBSpan + SEG
- True prevention of the unknown (ie. FortiMail/FortiClient hold for FSA rating)
- Most flexible form factor choice (physical and virtual, cloud and MSS)
- A cohesive Security Fabric to deal with APTs extends sandbox coverage, simplifies administration and speeds response
  - Scales from the smallest device through the largest public or private cloud
  - Combines global and local intelligence/protection
  - Encompasses Fortinet and 3<sup>rd</sup> party security components

## Fortinet Advanced Threat Protection Framework

### Advanced Threat Protection Framework

Turn the unknown into the known for prevention



## Target customers

- Existing FortiGate customers looking for added defense against advanced threats/data breaches. **This is the low-hanging fruit!**
  - Larger Organization with FortiGate 600D and above or VM: Generally recommend FortiSandbox physical or virtual appliance
  - Smaller Organization with FortiGate 500D and below: Generally recommend FortiSandbox Cloud
- Organizations with legacy Email Security (especially Microsoft, McAfee and Cisco), struggling with targeted attacks.
- Organizations selecting their new (usually next generation) firewall platform.
- Organizations unhappy with existing (expensive/ineffective) endpoint security.

# Fortinet Advanced Threat Protection (ATP) Talking Points

## Qualification questions to ask your customers and prospects

- Have you been tracking the latest data breaches making the headlines? If so, what measures are you taking or considering to reduce the risk of it happening to you?

A: Listen for any of the following (and consider these items):

- Firewall/NGFW Project
- FortiGate/ NSS Recommended NGFW, DCIPS, Top VB RAP AV)
- New Secure Email Gateway Replacement or Supplement
- FortiMail (Top VBSpam+, AV Comparatives Advanced+ Antiphishing)
- New Sandbox Project
- FortiSandbox (NSS Recommended Breach Detection, ICSA Advanced Threat Defense)
- Endpoint Replacement or Endpoint Detection and Response Project
- FortiClient (NSS Recommended EPP, Top VBRAP)
- FortiClient + FortiSandbox

- Do you have a Sandbox project planned, in progress or recently completed?

A: This is the most common response to the current threat. Even if the customer has already bought FireEye, it is generally for a subset of the network or protocols (due to high price) so still worth a conversation about FortiSandbox.

- Would you like to increase your security posture by adding the latest security technology (sandboxing) to your existing security infrastructure?

A: There is a constant stream of new “best of breed” point products in security. A few years ago it was “NGFW,” now it is “Sandbox,” in a few years it will be something else. Rather than continuing to stack on point products, Fortinet offers customers the ability to simply enhance in-place security- this is a more effective (no silos) and easy to manage (looks and acts the same) approach.

- What is your most sensitive data, what would be the impact if it were stolen?

A: Everyone thinks “it won’t happen to me”...until it does. Consider CTAP with Sandbox to see what’s really happening in your network.

**FORTINET**®

## FortiSandbox Family

Performance & Scalability		FortiSandbox VM	FortiSandbox 1000D	FortiSandbox 3000D	FortiSandbox 3500D	FortiSandbox Cloud
VMs		2*	8	28	64	
Sandboxing (Packets)	Dependencies	160	160	500	1200*	Attached
AV Scanning (tasks)	Dependencies	6,000	6,000	15,000	48,000*	Attached
	Hardware					Attached

## Fortinet ATP vs. the Competition

**ATP Framework protects more threat vectors and is *industry certified***

Vendor	Signature Appliance	Platform	Cloud	Firewall	ThreatVector Integrated	Email	WAF	Client	NSS	Certification	ICSA
<b>FORTINET</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
TREND	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓
Check Point	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗
Symantec	✗	✓	✓	✗	✓	✓	✗	✓	✗	✓	✓
paloalto	✓	✓	✓	✓	✓	✗	✗	✓	✗	✓	✓
FireEye	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗	✗

## Key Resources

- Education: Kill Chain Video and Why You Need Sandboxing Solution Brief
- Education: ATP Buyers Guide and Forrester Sandbox Survey
- Solution: ATP Framework Whitepaper and Animated Video
- Solution: FortiSandbox and ATP Sales Presentations
- Selection: NSS Labs BDS SVM and PARs and Podcasts, ICSA ATD Report
- Training: NSE 2- ATP Solution, NSE 3- FortiSandbox, FortiMail, FortiClient