FORTINET

Welcome to the Fortinet's Cyber Threat Assessment Program Playbook

GET STARTED

"CTAPs are selling our product. They have become a very powerful tool because we can quantify what we are talking about… the customers can now see it."

"The CTAP report drove this opportunity from a $20K opportunity to a $200K+ opportunity. The report allowed management to see that security was an area of need and these projects are now being moved to the top of the list."

"At the start there was little interest in using the FortiGate for security. Within minutes we were seeing botnets, viruses, P2P, etc. The report was sent up the chain and quickly became a hot topic."

Fortinet's Cyber Threat Assessment Program

Fortinet Cyber Threat Assessment Program (CTAP) is a framework designed to assist you with offering your prospects a quick, easy and free insight into their security posture. It helps you build credibility, establish yourself as a trusted advisor and create a strong business case to choose Fortinet solutions to mitigate threats. CTAP takes advantage of FortiGuard services, independent 3rd party testing (Virus Bulletin, AV Comparatives, and NSS Labs) and validation of superior security intelligence and protection effectiveness.

How CTAP Helps You

- Demonstrate security expertise and establish yourself as a trusted advisor
- Accelerate prospect's decision to buy when threats are uncovered
- Gain a foothold into accounts (bridges the "demonstrate value" to "purchase" gap)
- Quickly prove FortiOS/FortiGuard value specific to customer environment
- Establish Fortinet Security Fabric as something tangible, not just a vision
- Overcome common objections related to PoC difficulties (time, cost, manpower, etc.)
- Standardize your sales processes and manage the end-to-end sales cycle

How CTAP Helps Fortinet

- By establishing a consistent run rate of opportunities through sales + channel partners
- Utilization of analytics gives Fortinet more marketing ammunition and thought leadership
- Expect a close rate approaching 90% for CTAP enabled deals
- More management oversight and visibility into sales cycles all around
- Partners are more engaged and enjoy a more controlled sales methodology
- Standardize our pre-sales tools and sales enablement processes
- Effectively, CTAP has become the de facto call to action at Fortinet

Customer Benefits

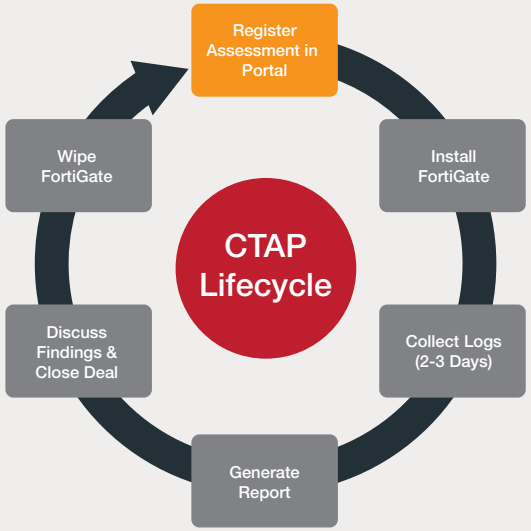
Your customer's network is a complex set of interactions between applications, users and content. It is at risk from sophisticated threats such as APTs, botnets and advanced malware. To manage the complexities and block the threats requires greater visibility and performance than traditional network firewalls can provide.

The Cyber Threat Assessment Program offers a FortiGate network security platform deployed as internal segmentation firewall (ISFW) or next generation firewall (NGFW) to provide your customer with an unprecedented insight into security and threat prevention, user productivity and network utilization without compromising performance or adding latency.

Most importantly, the Cyber Threat Assessment Report will translate this information into recommended actions your customer can take to mitigate security and threat concerns, improve user productivity and optimize network utilization with FortiGate's granular control over applications, users and content.

Organizations Who Run an Assessment Will Discover…

- Their network is bombarded with more than **6,900 IPS attacks daily** – those are all threats that are currently circumventing their existing gateway firewall!
- **3 pieces of freshly installed malware** and/or botnets attempting to dial home to various command and control servers around the world.
- About **192 applications are utilized per day on average** – many of them are unknown to the prospect's IT managers and include gaming, peer to peer, and remote access applications.
- More than **19 audio/video streaming** applications which consume about 35% of their organizational bandwidth on any given day.
- 2 or more malicious "drive-by download" websites accessed per week; each of them **attempting to install malware** on their network hosts.



Customer Concern	Recommended Solution	Top-Level Benefit
Security and Threat Prevention (including Advanced Threats)	FortiGate NGFW + FortiSandbox + FortiAnalyzer	Detects previously unknown attacks, high-risk applications, botnets, C&C activity, exploits, malware, etc.
User Productivity	FortiGate NGFW + FortiAnalyzer	Provides insight into which applications are consuming network bandwidth.
Network Utilization	FortiGate NGFW	Clarifies when the network is more heavily utilized.

What is the output of a CTAP?

- Duration to run a CTAP typically takes 3-7 business days
- Assessment report available within 2 days after receiving log files
- Report output is in PDF format
- Report can be branded with Partner Logo

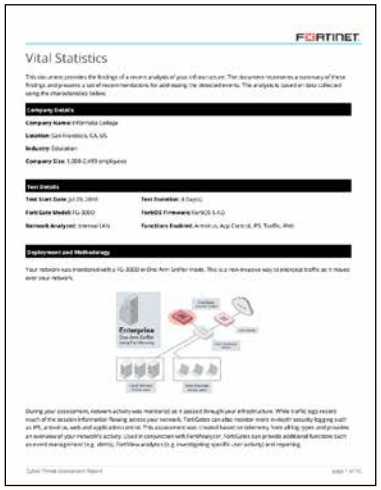
Fortinet supports FortiGate 100D, FortiGate 300D, or FortiGate 1500D models with CTAP. While we are evaluating other hardware models, there is an inherent complexity in supporting multiple models on new builds.

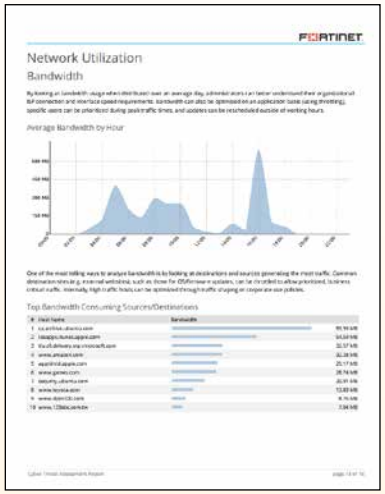
In general, it's better to OVERSIZE a network environment in order to capture logs properly. On the upper end, most large environments (which require more horsepower than a 1500D) have specialized qualification requirements which are more conducive to a custom evaluation.

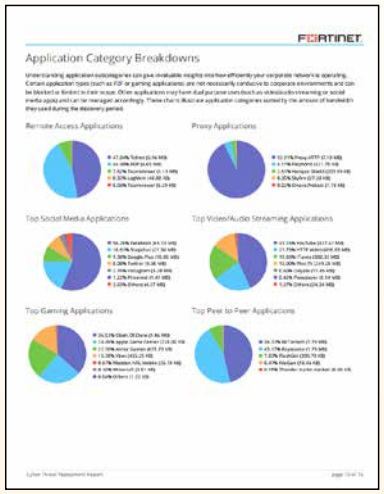
Here are some of the key differentiators when it comes to our assessments versus other security vendors:

- Performance section - We have an entire report section dedicated to network utilization/performance. Obviously, that's great for us since 1. performance plays to our strengths and 2. it will force prospects getting assessments from competitors to ask about missing sections.
- At risk hosts chart – We can utilize client reputation to determine the trustworthiness of individual hosts. Competitive programs do not provide similar insight.
- FortiGuard – We inherit all of the content security advantages of FortiGuard. This includes our 3,300+ application sensors (less than 2,000 for most competitors), 8,100+ IPS signatures, etc.
- Deployment flexibility - We allow streaming logs directly to a remote logging server OR uploading them to the portal. In addition, we support two deployment modes: sniffer and inline.
- Use of FortiAnalyzer - We use a FortiAnalyzer on the backend (eat our own dog food, so to speak). Most competitors use a separate tool entirely (and this is a great way to upsell a FortiAnalyzer unit!).
- Sandboxing included – There is no need to run firewall and sandbox reports separately. CTAPs can include sandboxing by choosing a checkbox, which demonstrates our Security Fabric in action.

Sample CTAP Report







CTAP is meant to be a quick deployment and status check of a prospect's network. Typically, these are greenfield (net new) opportunities, but existing customers (especially in upgrade/replacements scenarios) are also eligible. Generally speaking, CTAP is not meant for custom FortiGate configurations, integrations with other products (either Fortinet or third party), or RFP bake-offs. Extreme low-end (partner investment vs. return) and high-end opportunities (customization and high performance FortiGates) are generally not conducive to CTAP.

Concern	Risk of Breach	User Productivity	Upgrade	Firewall Refresh	Consolidation and Security Services Renewals	Performance
Question	Are you concerned about getting breached?	Do you have the visibility you need into your users productivity?	Are you looking to upgrade from a traditional firewall to a next generation firewall?	Are you looking at refreshing your firewalls soon, or adding additional firewalls to your growing organization?	Do you have to manage multiple point security products? Do you have a web filtering or IPS service renewal coming up?	Is your current firewall delivering the performance you need to keep up with the speed of your network?
Answer	Get a sneak peak into how FortiGate will provide better security and more control without disrupting your existing infrastructure. It's easy, no legal documents to sign or purchase orders to cut. Risk of data breach in today's threat landscape is high, get visibility into your risk with a free assessment. (Gartner predicts that 90% of new enterprise firewall purchases will be NGFW by the end of 2018)				See how you can simplify your management load by replacing your point security products with a FortiGate NGFW or do a graduated rollout by replacing point products with a better value FortiGate and turn on additional capabilities as you need them over time.	The FortiGate platform delivers 5x faster throughput performance compared to other similar NGFW solutions in the market today. Our high-speed performance is based on the Fortinet Optimum Path Processing architecture and our custom FortiASICs.

Engaging and Qualifying Prospects:

- Does your team regularly brief exec staff on your security status?
- Are you looking to upgrade to a NGFW?
- Have you ever been breached or do you have a breach response plan in the event your network is compromised?
- Do you know which applications are being used on your network?
- Do you think your firewall can keep up with bandwidth demands?
- When is your next firewall maintenance renewal?
- What are your corporate policies on P2P, proxy or gaming usage?

"I already have a Next-Gen firewall."

Perfect! Let's find out how effective it is without disrupting your network.

"I don't have any security budget."

There is no cost for running a CTAP; that said, maybe this would help expand your security budget for next year if we uncover any potentially malicious activity.

"I don't have time… I'm too busy."

CTAP will literally only take 30 minutes to setup. And if we uncover a breach or attack vector, you'd probably rather know about it than not.

PROSPECT CONCERNS OR NEEDS	BENEFITS OF CTAP
Unsure of current firewall's threat effectiveness	Generated CTAP Report uses FortiGuard to demonstrate superior detection capabilities & also shows what is bypassing their existing firewall
Unable to properly evaluate firewall for refresh due to limited resources	No time and limited personnel needed
Cannot afford disruption during assessment	FortiGate can be deployed as either a sniffer (no disruption) or inline (minimal disruption)
No budget available for external assessment	There is no charge to run a CTAP assessment
Increase in unmanaged/untrackable activity (cloud or SSL)	Generated CTAP Report will determine which cloud/SaaS applications are being used and actual HTTP/HTTPS ratio
Targeted attacks and potential zero day threats	CTAPs can also demonstrate the value of sandboxing without requiring a CPE based FortiSandbox
Comparison to similar companies	CTAP Reports can show how the prospect's network security stacks up relative to other organizations in the same industry

https://ctap.fortinet.com

1. Login to: ctap.fortinet.com (using your network credentials)
2. Read through the tutorial dialog that first pops up
3. Then read through supporting materials & FAQ

Suggested Materials List - Specific sales roles should understand these materials

MAM/RAM	CAM/Partners	Sales Engineering	BDR/ISR	Vertical Sales
NSE Training	NSE Training	NSE Training	NSE Training	NSE Training
Sample CTAP Report	Partner Toolkit	Sample CTAP Report	Sample CTAP Report	Sample CTAP Report
Portal Training Video	Sample CTAP Report	Talking Points for SEs Prezo	Talking Points for Inside Sales Prezo	Portal Training Video
Threat Landscape Report	Partner Overview Video	Portal Training Video	Threat Landscape Report	Threat Landscape Report
Prospecting Flyer	Portal Training Video	Configuration Checklist	Prospecting Flyer	Relevant blog entries
Test Your Metal	Partner $250 Reward	First-time Portal Tutorial	Test Your Metal	Prospecting Flyer
Prospecting Videos	Release Notes	FAQ	Prospecting Videos	Prospecting Videos
Supplementary Slides	Supplementary Slides	Supplementary Slides	Supplementary Slides	Supplementary Slides

Promote the Solution

Awareness	Engagement	Consideration
CTAP Customer Flyer CTAP Full Page Print Ad	CTAP Partner Toolkit CTAP Sales Presentation	CTAP FortiGate Configuration Checklist CTAP Campaigning: Talking Points for Inside Sales CTAP Report: Talking Points for SEs
CTAP Customer Pitch Video #1 (Kinetic Typography) CTAP Customer Pitch Video #2 ("Meet Ed" Series)	CTAP Partner Overview Video CTAP Portal Training Video	CTAP 3.1 Release Notes CTAP Customer Supplementary Slides
CTAP Partner $250 Reward	CTAP Threat Landscape Infographic (1H 2016)	CTAP Threat Landscape Executive Summary (1H 2016) CTAP Threat Landscape Full Report (1H 2016)

READY TO FOLLOW UP?

Cash Reward

Earn $250 for every completed customer Cyber Threat Assessment. Applies to Fortinet Sales and Partners.

Who to Contact

Review the CTAP portal Tutorials, FAQs, and Downloads. Any questions? Contact ctap@fortinet.com

How to

To initiate a CTAP with a customer, you need to acquire a FortiGate.

FortiGate acquisition…

- Internal units

1. Initiate an ITF through OA
2. Review instructions on setting up a FortiGate in a lab (be sure to CTAP test prior to deploying at an actual prospect)

- Partner units

1. Certain partners qualify for complimentary units
2. Others must order discounted NFR units
3. Some distributors maintain pools of FortiGates for CTAPs
4. Work with your Channel Account Manager

Prospect Materials

Sample CTAP Report w/ Sandboxing (Informata College) - English

Sample CTAP Report w/ Sandboxing (Informata College) - French

The Website

https://ctap.fortinet.com

1. Login to: ctap.fortinet.com (using your network credentials)
2. Read through the tutorial dialog that first pops up
3. Then read through supporting materials & FAQ

Relevant Blogs

https://blog.fortinet.com/2016/02/25/cyber-threat-assessment-threat-landscape-report

https://blog.fortinet.com/2016/06/15/cyber-threat-assessment-how-to-find-indicators-of-compromise

https://blog.fortinet.com/2015/10/26/even-it-heroes-need-cyber-threat-assessment-help

https://blog.fortinet.com/2016/03/29/unique-perspectives-on-the-threat-landscape-of-today-s-healthcare-networks

https://blog.fortinet.com/2016/09/26/overview-fortinet-threat-landscape-report