Cyber Threat Assessment Program (CTAP)

Provide an in-depth view of the current state of your customers' network for free.

What is CTAP?

The Cyber Threat Assessment Program (CTAP) is a fast and free assessment that TPx identify security risks for your customers and helps them understand their network usage. At no cost to you or your customer, our team will monitor key indicators within customers' networks.

After gathering information, customers will receive a Cyber Threat Assessment Report that will help them address important business concerns such as security, productivity, and/or utilization.

CTAP benefits

Customers learn…

- If their current security infrastructure can accurately detect today's sophisticated attacks
- If they have operational visibility to understand how applications (traditional and web-based) are truly being utilized on their network
- If their current security solution will be able to meet increased throughput and encryption demands (perhaps due to cloud-based storage, big data analytics or increased web usage)

Provides status of your security, productivity, and utilization

No cost or risk to you

Requires less than 30 minutes of your time

Completed in a week or less

What's in it for me?

- 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.)

Tips to win big

- Talk to the right decision maker: a CISO
- Enlist an internal champion (generally the security operations or IT contact)
- Establish yourself as a subject matter expert
- Always request an audience with C-level decision makers along with the internal champion when reviewing assessment results
- Print out and (ideally) bind the report; do not send an electronic copy in advance
- Allow the internal champion to chime in
- Ask them when they are planning to make a decision

Generating interest in CTAP

- How do you assess the effectiveness of your existing solution?
- Do you have the visibility you require to make informed decisions?
- What are your corporate use policies and how do you enforce them?
- Do you feel like you have control over your network?
- How long has it been since your last refresh cycle for this product?
- Are you having challenges getting security budget allocated?
- When your team brief executive staff members, do you feel that you have all of the metrics they're looking for?
- From a capacity planning standpoint, can your current solution keep up with the speed of your business?

Part of running a successful assessment will be the kinship you form with the "internal champion" who is generally the security operations or IT contact working on behalf of the prospect. Your job is to educate and elevate his/her understanding of their own network and they in turn will provide good opportunities for informed recommendations.

How it works

First, the CTAP device is installed at customer's site by a solution architect. Then, traffic logs are securely collected for 3-7 business days and a comprehensive report is generated. Finally, the solution architect reviews the report and discusses the insights with the customer and retrieves the CTAP device.

Why TPx's CTAP?

Superior visibility

Powered by content security and threat intelligence from FortiGuard Labs — 3,300+ application sensors (less than 2,000 for most competing CTAP), 8,100+ IPS signatures).

Additional insights and opportunities

Includes extensive performance section, at-risk hosts chart, sandboxing and more.

Deployment flexibility

Multiple deployment options in order to minimize network disruption.

Actionable recommendations

Each assessment report includes a set of actionable recommendations that technical staff can use to refine their security and network utilization.

How do I arrange a CTAP with TPx?

Contact your channel manager. Limited to Solution Architect location and availability.

What is in a CTAP report?

Security

- Application vulnerabilities observed
- Malware botnet detection
- At-risk devices within the network

Productivity

- Application categories and cloud usage
- Per-to-peer, proxy app and remote access
- Web-based applications and browsing habits

Utilization

- Bandwidth analysis and top consumers
- Average log rates/sessions for sizing
- SSL utilization and encryption impact

Handling common objections

I already have a solution for that and we're happy with it.

CTAPs are a good way to test the effectiveness of your existing solution. It's like getting a second opinion from a doctor — it can't hurt.

I don't have any more security budget.

Running an assessment can actually help obtain more security budget if we uncover anything important.

I'm too busy to evaluate any new products.

Assessments are designed to take less than 30 minutes of your time; we'll do the heavy lifting. And if we uncover something noteworthy, you'd probably want to know.

I have privacy concerns.

We intentionally do not identify individual user names (via LDAP for instance). Log data is transported to Fortinet for processing via a secured channel (SSL encrypted). Log data is only stored for the duration of the assessment. When an assessment is completed, raw logs are permanently erased from any processing servers automatically after 7 days.

Top Application Vulnerability Exploits Detected

#	Risk	Threat Name	Type	Victims	Sources	Count
1	5	WordPress.HTTP.Path.Traversal	Path Traversal	1	2	55
2	5	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	1	5	12
3	5	NETGEAR.DGN1000. Unauthenticated.Remote.Code.Execution	Code Injection	2	5	5
4	5	Bladabindi.Botnet		1	1	3

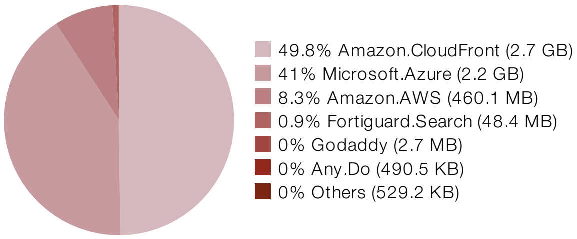
Top Malware, Botnets and Spyware/Adware Detected

#	Malware Name	Type	Application	Victims	Sources	Count
1	Bladabindi.Botnet	Botnet C&C	Bladabindi.Botnet	1	1	3
2	HTML/FakeAlert.QB!tr	Virus	HTTP.BROWSER_Chrome	2	1	2
3	Zeroaccess.Botnet	Botnet C&C	Zeroaccess.Botnet	1	1	2
4	Mirai.Botnet	Botnet C&C	Mirai.Botnet	1	1	1

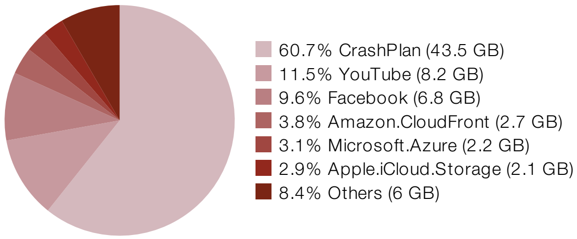
High Risk Applications

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Proxy.HTTP	Proxy	Network-Protocol	181	2.32 MB	2,433
2	5	Cloudflare.1.1.1.1.VPN	Proxy	Client-Server	2	2.51 MB	476
3	5	SOCKS5	Proxy	Network-Protocol	3	33.55 KB	30
4	5	SOCKS4	Proxy	Network-Protocol	10	34.15 KB	27

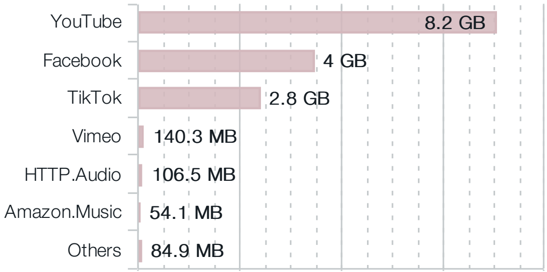
Cloud Usage (IaaS)



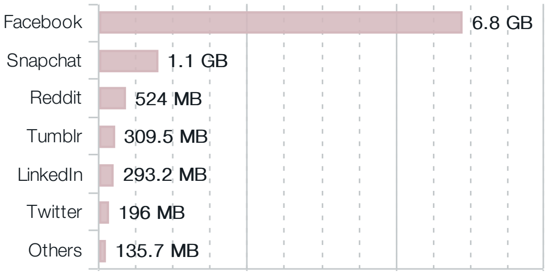
Cloud Usage (SaaS)



Top Video/Audio Streaming Applications



Top Social Media Applications



Ask us for a sample report