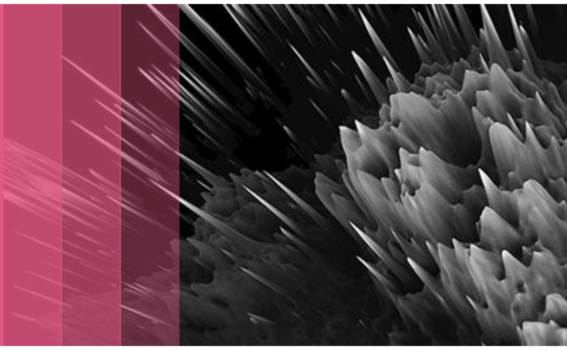
THREAT INTELLIGENCE: DRIVING THE FUTURE OF SECURITY



DEFINING THREAT INTELLIGENCE

Before understanding what threat intelligence means, let's take a look at what we mean by "intelligence." According to the Oxford Dictionary, one of the definitions of *intelligence* is the "collection of information." If you think about it, with the vast amount of data and knowledge around us, it's impossible to gain access to the most robust knowledge from just one source. Threat intelligence is exactly this – it's the process of collecting intelligence on threats from multiple sources because one source does not and cannot provide the best intelligence by itself.

According to Gartner, "'Threat Intelligence' is evidence-based knowledge - including context, mechanisms, indicators, implications and actionable advice – about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard."[1] Gartner also describes threat intelligence as "the product of a process, rather than a series of individual data points."[1]

We agree. In IT Security, threat intelligence is much more than a firewall or antivirus system protecting your network. It takes into consideration all of the data points and network data to provide real-time monitoring, notifications, and threat profiles. It provides a higher level of protection, especially in networks with multiple points of entry.

WHY THREAT INTELLIGENCE IS SO CRITICAL

Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider. When an organization has financial, personal, intellectual, or national assets, a more comprehensive approach to security is the only way to protect against today's attackers. And one of the most effective proactive security solutions available today is threat intelligence.

Threat intelligence combines information from multiple sources, providing a more effective protection screen for your network. Organizations are quickly understanding the need for adopting a tool such as threat intelligence into their security architecture. In fact, estimates from IDC indicate that by 2020, threat intelligence will be the fastest-growing section of the fifty billion dollar network security market, becoming ten times more valuable than traditional security solutions. This much attention has attracted a number of companies offering a variety of solutions in the threat intelligence space representing varying capabilities, quality, and usability.

In October, 2014 Gartner published two reports: "Competitive Landscape: Threat Intelligence Services Worldwide, 2015" and "Market Guide for Security Threat Intelligence Services". These reports recognize several companies' threat intelligence solutions, including Check Point for its ThreatCloud IntelliStore. We believe these reports characterize a high-growth market producing tailorable threat analysis to protect organizations from the increasing complexity of targeted attacks.

HOW TO CHOOSE THE RIGHT THREAT INTELLIGENCE

Now that we have talked about what threat intelligence means and why it's important, let's take a look at how to choose the right threat intelligence amongst the numerous solutions that are available in the market today.

March 17, 2015

While any threat intelligence solution is better than none, quality trumps quantity. The type of intelligence, where it comes from, how it is used, and how it integrates into your existing network security solution are all things to take into consideration. Gartner suggests that organizations should "be aware that not all "threat intelligence" is the same. Some vendors do not offer much more than information about IP addresses and the implication of URLs in current activity. This provides you with an ability to respond rapidly to the contemporary threat environment, but does not clue you in on may happen in the next month or year. Other vendors can provide advice on adversarial capabilities and plans, but this information is expensive and almost always involves a degree of informed inference."[2]

In a recent report by Forrester Research, Inc., "Use Actionable Threat Intelligence to Protect Your Digital Business," Principal Analyst Rick Holland[3] mapped out some of the main characteristics you should be looking for while shopping for threat intelligence. We found this to be a very useful guide:

- **Accurate** – Measures results on a continuous basis to ensure accuracy.
- **Aligned with your intelligence requirements** – The "one size fits all" rule does not apply to threat intelligence. Your threat intelligence should be unique to your organization's needs and strategic goals.
- **Integrated** – Automatically integrates into your existing security solution.
- **Predictive** – Provides indications and warnings that something malicious is about to occur.
- **Relevant** – Relevant to your specific business whether it is vertical, geographies, or threat types.
- **Tailored** – Tailored to the audience it is serving.
- **Timely** – Analyzes and integrates intelligence quickly.

THREATCLOUD INTELLISTORE — ACTIONABLE. CUSTOMIZEABLE. INTELLIGENCE.

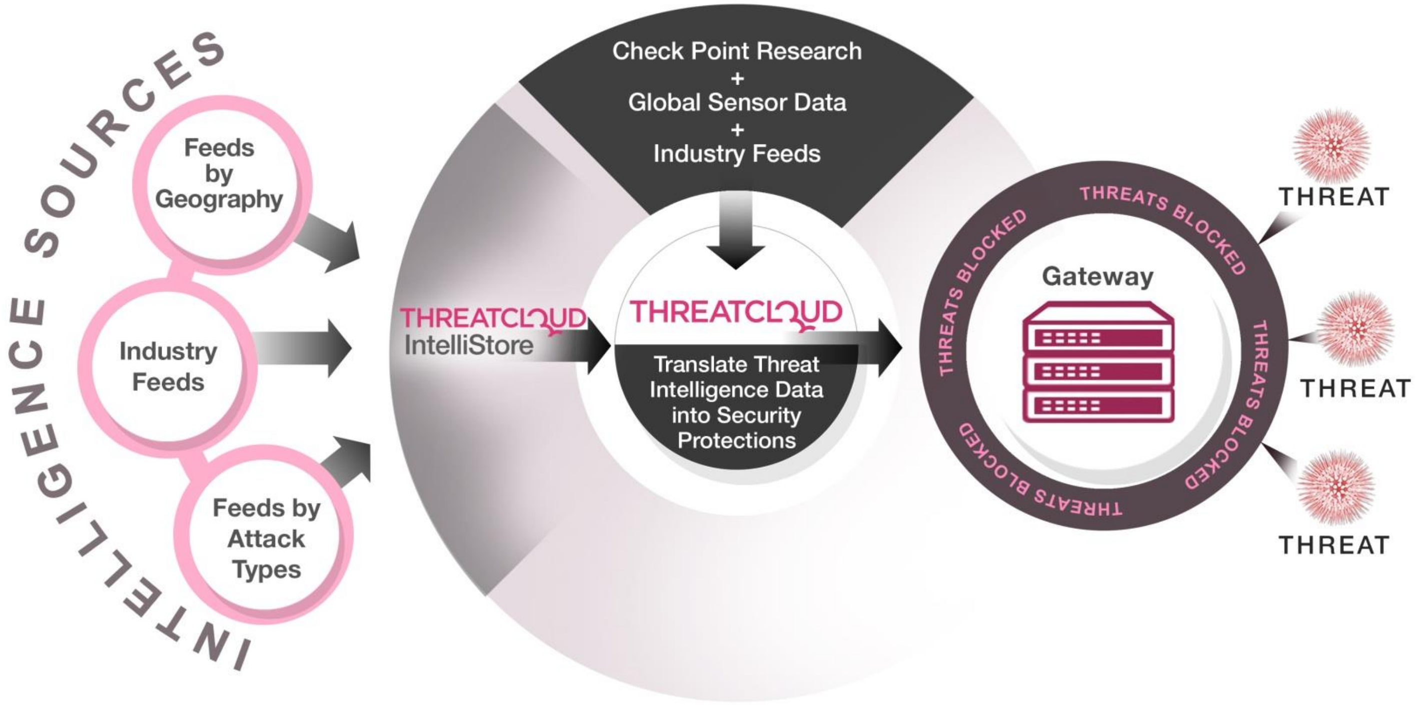
WIDEST PROTECTION WITH THREATCLOUD INTELLISTORE MARKETPLACE

As discussed in the first half of this paper, threat intelligence services, in general, provide knowledge about specific kinds of information, security threats, and security-related issues. Threat intelligence is the process of collecting intelligence on threats from multiple sources because one source alone does not and cannot provide the best intelligence. Certain vendors may specialize in financial industries, while another specializes in critical infrastructure or retail – they don't typically specialize in everything. If they do, they are no longer a specialist. They are a generalist.

This is why we decided to offer IntelliStore. ThreatCloud IntelliStore is an intelligence marketplace that gives organizations access to a wide variety of real-time threat intelligence sources instead of limiting them solely to a single vendor's recommendation. This service not only provides access to a wide range of protection, but also allows the picking and choosing of threat intelligence feeds based on a company's unique needs (by geography, industry, or threat type).

Our sources come from one of the largest security networks in the industry. We derive our threat intelligence information from:

- **Sensor Feeds** – We have one of the largest deployments of security gateways in the industry. Every new threat stopped creates a threat signature that is then included in ThreatCloud. More security gateway sources mean we find and catalog threat data every minute of every day.
- **Internal Research and Incidence Response Teams** – We have a large internal team dedicated solely to analyzing networks attacks, regional trends, attack types, and more.
- **External Industry Feeds** – Our Threat Intelligence marketplace enables customers to select from a wide range of threat intelligence feeds relevant to them from industry-leading partners including: Norse, CrowdStrike, IID, iSIGHT Partners, Netclean, PhishLabs, SenseCy, Malware Patrol, Mnemonic and Zero Fox.



AUTOMATICALLY TRANSLATE THREAT INTELLIGENCE INTO ACTIONABLE SECURITY PROTECTION FOR IMMEDIATE DISTRIBUTION

From this data we create a robust set of security protections and update your security gateway. According to Gartner, “to be more effective and proactive, there is the need for a more active collaboration and exchange of threat intelligence data.”[4] At Check Point, we believe in innovating and leading in the market, and this is why we introduced the ThreatCloud IntelliStore intelligence marketplace in May 2014.

Via ThreatCloud, the IntelliStore converts the intelligence into proactive protections that are automatically delivered to security gateways. This ensures that turning the threat intelligence information into security protections does not become a secondary step and provides timely defense.

GET YOUR NETWORK PROTECTED TODAY

Visit checkpoint.com/intellistore to learn more about ThreatCloud IntelliStore.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Sources:

[1] “Market Guide for Security Threat Intelligence Services,” page 2, Gartner, 14 October 2014
[2] “Market Guide for Security Threat Intelligence Services,” page 18, Gartner, 14 October 2014
[3] “Use Actionable Threat Intelligence to Protect Your Digital Business,” page 4, Rick Holland, Forrester Research, August 2014
[4] “Competitive Landscape — Threat Intelligence Services,” page 7, Gartner, October 2014

March 17, 2015