Case Study

Centripetal Networks & ThreatConnect Case Study:
Fortune 50 Financial Services Organization Sees Success with Smarter Threat Intelligence

Industry: Financial Services

Description: Fortune 50 Financial Services Company

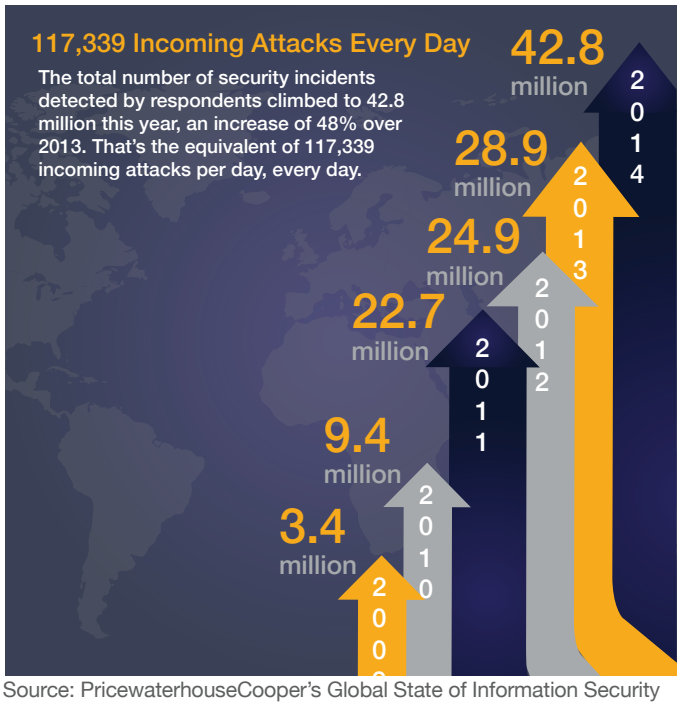
About the Company: This Financial Services firm plays a key role in the global economy and they place an emphasis in ensuring their enterprise is protected as they are a constant target of many diverse adversary groups

Challenge: Managing threats to the infrastructure in facilities across the United States while automating and enforcing threat intelligence data

Solution: Deployment of Centripetal Network's RuleGate® appliance and the ThreatConnect® Threat Intelligence Platform for network enforcement

The Threat Landscape

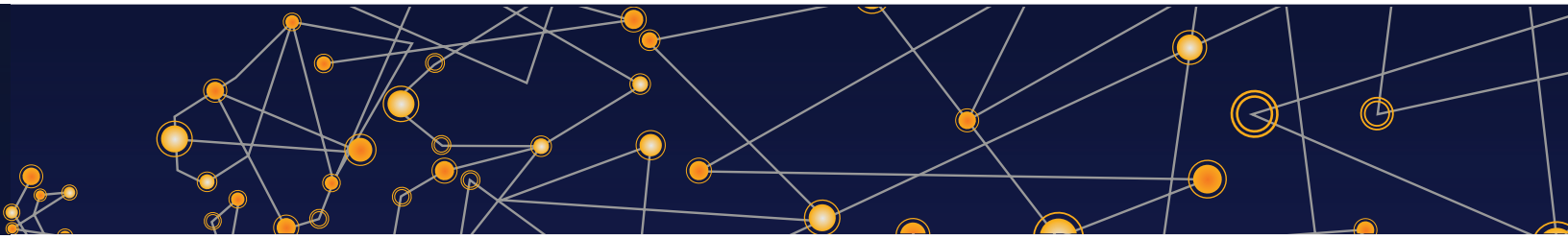
The threat landscape is forever expanding and adapting. Cyber threats have grown at an average rate of 66% annually since 2009. In 2014, however, the number of detected security incidents soared to 43 million, a 48% jump from 2013. With millions of malicious users hiding amongst billions of legitimate users, cyber security systems must be able to meet the breadth of today's cyber attacks. Without this solution in place, the next breach could be right around the corner.



Source: PricewaterhouseCooper's Global State of Information Security Survey 2014

One of the biggest factors in predicting breaches on a company's security stack is based upon which industry the organization is rooted in. Heavily regulated industries such as healthcare, education, pharmaceutical and financial services have per capita data breaches that cost substantially higher than the overall mean. In fact, 45% of financial services organizations have been the target of cyber attacks, as opposed to the 17% of other institutions.

Case Study



The Challenge

This financial services firm was unable to manage adversary changes to the infrastructure at their various data centers throughout the United States. The organization needed a way to gain situational awareness of specific threats to their company while correcting the high noise-to-signal ratio their security team saw from irrelevant or inaccurate sources of threat intelligence.

As a Fortune 50 financial services organization, this company was aware of the high risk they faced from cyber attacks and wanted to ensure the privacy of their customers' records and integrity of their networks. This organization's security team needed a solution that provided fully correlated data of their network traffic as well as a way to operationalize relevant threat intelligence in real-time.

The Solution

RuleGate®'s sophisticated packet filtering combined with the ThreatConnect® Threat Intelligence Platform's analytic capabilities provided a way for this organization's security team to control what sources and types of threat intelligence are used to defend their network. RuleGate leverages criticality ratings, confidence, tags, and deep contextual associations supplied by ThreatConnect to define granular policies for alerting and blocking. The RuleGate and ThreatConnect combined solution enabled the organization to input threat intelligence from their own research, open and private communities, and third party vendors for real-time protection of their network.

The joint solution provided the organization's security teams with the ability to focus their investigative resources to deliver faster-than-ever incident response and gain real-time visibility into the threat landscape over their multiple datacenter locations. The RuleGate operationalized the threat intelligence received from ThreatConnect to allow for immediate enforcement of dynamic threat indicators.

Case Study

THREATCONNECT™ & CENTRIPETAL NETWORKS

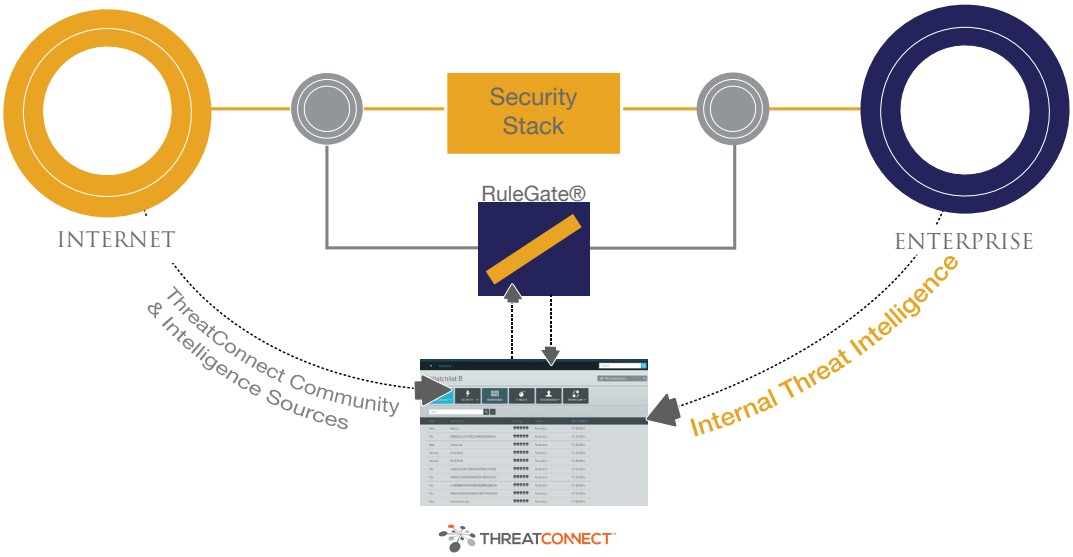
Aggregate, Analyze, Act

ThreatConnect is the first and only Threat Intelligence Platform built to bridge incident response, defense, and threat analysis. ThreatConnect allowed this organization to easily aggregate, analyze, and act on all of the threat intelligence data received and manage incident response and threat analysis tasks across their entire security team from within the same platform. Through the integration, the ThreatConnect platform leverages threat intelligence from multiple industry and threat specific trusted communities, open source, and vendor intelligence sources to seamlessly deliver data between ThreatConnect and RuleGate, bringing in both public and private data sources for defense.

Persistent Threats Require Persistent Protection

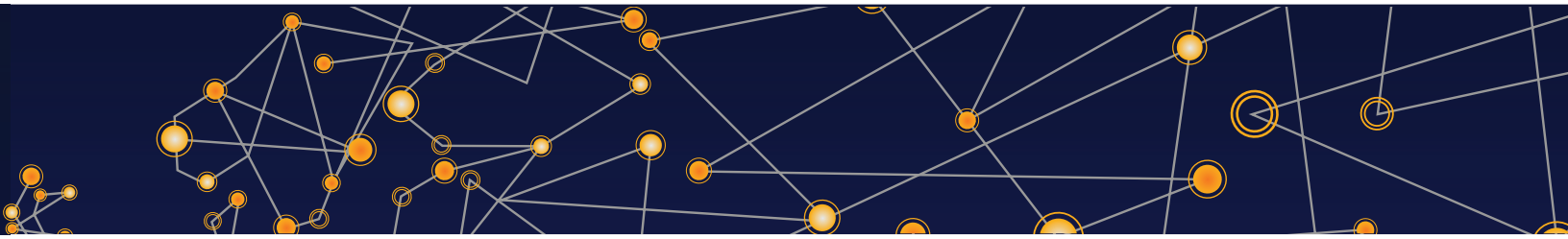
Centripetal Networks' RuleGate appliance enables large dynamic policies with high fidelity indicators to actively protect the network in real-time. RuleGate systems enforce cyber security policies with millions of rules, at full line rate and without degradation in network performance or user experience. This level of scale allowed for this company's analysts to detect threats that had gone unnoticed prior to the deployment of RuleGate. Their previous cyber-security system simply could not scale to meet their needs.

RuleGate's sophisticated packet filtering combined with ThreatConnect's analytical platform and data provided this organization with a way to control what sources and types of threat intelligence are used to defend the network with RuleGate. Their security teams were able to choose which rules to apply by leveraging ThreatConnect's criticality ratings, confidence, tags, and contextual associations of past incidents and known threat groups.



CENTRIPETAL NETWORKS THREATCONNECT™

Case Study



Threat Indicator Matches

ThreatConnect and the RuleGate systems installed in multiple datacenters provided real-time feedback to the Security Operations Center (SOC) team conducting research on the network. Indicators of compromise in the ThreatConnect platfom were identified and attributed to activity with known internal hosts on the network in multiple locations. This led to a faster collaboration on the severity of the incident and targeted efforts for the incident response team.

The data tables below show matching indicators in two datacenter locations that were fully correlated to internal hosts using Centripetal's QuickThreat application.

Indicator Matches at Primary Datacenter

THREATCONNECT_SOC_5						
THREAT(S) 2 CORRELATED HOST(S) 4						
IP address	Packets	Risk Score	Country	Bytes	Ports	Correlated Hosts
X.X.201.208	9524	14.0	United-States	3.0 K	443.80	X.X.219.19, X.X.196.3
X.X.225.80	64	13.0	Switzerland	11.1 K	25,53,80	X.X.134.192, X.X.181.247, X.X.133.208

Indicator Matches at Secondary Datacenter

THREATCONNECT_SOC_5						
THREAT(S) 2 CORRELATED HOST(S) 4						
IP address	Packets	Risk Score	Country	Bytes	Ports	Correlated Hosts
X.X.201.208	68	9.0	United-States	19.3 K	80	X.X.113.82, X.X.113.83, X.X.45.48
X.X.225.80	4	9.0	Switzerland	186.0 B	80	X.X.160.247

- Data has been truncated for operational security
- Matches on custom watch list source compiled in ThreatConnect from correlated threat data
- Multiple hits seen at different datacenters within QuickThreat

The Results

This financial services firm has seen continued and demonstrable success in protecting their network. The current deployment allows for fully correlated data inbound and outbound. The combined solution enabled the organization to spot previously undetected outbound network threats and provided a level of visibility and control that they did not have with their previous security solutions. They were able to identify malicious hosts on their network and block outbound communications to known bad actors without disruption. The integration allowed the security team to react faster to threats and act according to threat data found within ThreatConnect and rules established by RuleGate.

This combined solution has enabled this customer to systematically regain control of their network and keep their data secure.

2251 Corporate Park Drive, Suite 150
Herndon, VA 20171 • (571) 252-5080

3865 Wilson Blvd., Suite 550
Arlington, VA 22203 • 1.800.965.2708