Solution: **Security** Industry: **Computer Services**

Centripetal Networks Inc.

Operationalize threat intelligence to act against cyberthreats in real time

Centripetal created its CleanINTERNET service to protect against network infiltration and data exfiltration by cybercriminals. It taps into live feeds of critical cyberthreat intelligence, including the high-confidence IBM® Security X-Force® Exchange Commercial Application Programming Interface (API) solution, to shield against the highest-risk threats in real time.

Share this

→ Discover the value of IBM Security X-Force Exchange solutions.

Business challenge

Adapting in real time to an ever-changing cyberthreat landscape is a challenge that requires the proactive use of vast amounts of dynamic threat intelligence.

Patent Owner, Centripetal Networks, LLC - Ex. 2013, p. 1

Transformation

Centripetal Networks Inc. uses the IBM Security X-Force Exchange Commercial API solution to feed millions of threat indicators into its CleanINTERNET service, which shields against malicious attacks bi-directionally in real time.

Results

Actively shields highest-risk traffic in real time

based on operationalized threat intelligence

Automatically updates monitor-worthy intelligence

to shield-worthy as IBM threat indicators change

Improves end customer analyst and security stack efficiency

by reducing event volume and false alerts

Business challenge story

Think differently about threat intelligence

Today, no company can operate without robust cybersecurity. While companies dedicate resources to responding to possible cyberthreats, their cyberteams are overburdened by

Patent Owner, Centripetal Networks, LLC - Ex. 2013, p. 2

spending valuable time researching threats that have passed, rather than concentrating on real-time prevention. Despite their efforts, it remains extremely difficult to collect, process and operationalize threat intelligence on a live network.

“Having massive libraries of information with the only action of producing reports for others to read is useful for strategic decision-makers in understanding threats to their industry but not necessarily the best approach tactically,” says Jess Parnell, Vice President of Security Operations for Centripetal. “Producing intelligence is highly valuable, but not using it actively and in a timely manner in defending the network has historically been a grave mistake.”

As cyberthreats have evolved, so has the field of threat intelligence. Today, more than enough intelligence is available to detect and stop almost any cyberattack. But until recently, there was no effective way to take all that intelligence and automatically apply it to prevent threats in real time.

To counter this problem, Centripetal designed its proprietary RuleGATE threat intelligence gateway to automatically operationalize threat intelligence on a zero-trust basis. Centripetal stops cyberattacks bi-directionally, before they can infiltrate into or exfiltrate data from the network. The company created this filtering engine that can ingest, apply dynamic rules to and act on billions of threat indicators, all in real time. Leveraging all available intelligence and inspecting every single network packet provides the most advanced level of zero-trust security.

Centripetal receives threat intelligence from multiple sources, but its gateway needs a reliable, accurate and frequently updated source of threat intelligence to successfully stop cyberthreats. As the company ramped up and refined its gateway technology to create a service offering to customers, it sought new cyberthreat intelligence sources.

“We don’t actually make threat intelligence,” says Parnell. “We call it gasoline for the engine, our RuleGATE. It needs intelligence to pinpoint malicious activities within the network and to proactively protect it.”

In 2018, Centripetal and a team from IBM Security X-Force connected through a mutual customer. Centripetal tested the IBM Security X-Force Exchange Commercial API software as a service (SaaS) solution and decided that it wanted to use it, but at a rate far higher than any other client. Many times, IBM Security X-Force clients subscribed to the service in one or multiple packs of 10,000 records per month. In this case, Centripetal wanted to consume records immediately upon availability, which amounted to 17 million records monthly. The IBM team was able to offer a solution to meet Centripetal’s needs.

Patent Owner, Centripetal Networks, LLC - Ex. 2013, p. 3

> “The IBM scoring mechanisms and the way that X-Force evaluates the risk levels are very reliable. That's not the case for all of the different variety of intelligence that we're getting.”
>
> **— Jess Parnell, Vice President of Security Operations, Centripetal Networks Inc.**

Transformation story

Operationalize intelligence to reduce risk

Centripetal offers its CleanINTERNET service to customers who want to protect their networks proactively rather than reactively. The company uses the IBM Security X-Force Exchange Commercial API feed from IBM as one of its key sources of threat intelligence, making it actionable through its service. All of this happens with no discernable network traffic delay, and with no firewall or other security stack device involvement, thanks to the RuleGATE gateway. Centripetal can customize its end user customers’ consumption of threat intelligence insights with its CleanINTERNET service, which accesses the cloud-based IBM Security X-Force Exchange platform through a RESTful API.

“We pull down the X-Force data in real time,” says Dave Ahn, Chief Architect and Vice President at Centripetal. “All the data — not just a subset, but all of it. We’re unique in this area in that most solutions can’t consume anywhere near that quantity of intelligence and make it actionable.” In fact, the Centripetal solution consumes billions of threat indicators daily from multiple threat intelligence sources, including the IBM Security X-Force solution.

Centripetal pulls the IBM Security X-Force threat intelligence, including IBM analyst-designated threat indicators, into its analytics platform, where the clearly “all-risk” threats are designated for immediate shielding by the RuleGATE threat intelligence gateway. The CleanINTERNET service shields these events proactively to enable a granular, detailed secondary inspection triage to occur in real time.

After the shielding event load reduction, Centripetal then uses these secondary inspection technologies to analyze all other threat events proactively along a risk gradient. A second category of “monitor-worthy” traffic emerges at this point which may be decrypted, payload analyzed and captured. Finally, some traffic is immediately scored as “low-confidence” or

Patent Owner, Centripetal Networks, LLC - Ex. 2013, p. 4

"informative," and no action is taken. The categorization varies by customer based on their risk profile and evolves over time as new threats emerge. As Ahn notes, "Our analytic platform and our analysts are engaged with the intelligence and with the customer to map the intelligence to what is actionable for each and every customer."

The Centripetal team has high confidence in the IBM Security X-Force threat intelligence indicators. "Our analysts ... feel very confident in IBM X-Force indicator set and many are readily shield-worthy," says Parnell. "IBM's scoring and the way that X-Force provides the intelligence are both very reliable. That's not always the case for all of the different variety of intelligence that we're getting."

The Centripetal CleanINTERNET service is also dynamic, automatically upgrading the monitor-worthy intelligence to shield-worthy as IBM threat indicators change. "The big gray area in the middle is really a lot of the value that you're providing us," says Parnell. "And the reason why it's so valuable to us is that we do a secondary inspection of the data."

In that secondary inspection, the Centripetal RuleGATE uses monitor-worthy intelligence indicators to pivot and pass potentially malicious traffic through deep packet analysis engines, such as content-based intrusion detection systems and signature-less inspection technologies where they may "fire" on a subset of targets, such as command and control infrastructure. This analysis enriches Centripetal's real-time decision-making and proactive response to the threats. The company's approach uses the original intelligence indicators to add valuable context about the traffic. "That makes the indicator truly actionable," says Parnell. "The end result is a greater degree of Shielding where we can offload risk."

> "With our CleanINTERNET service, our customers are benefiting from the IBM analysts' opinions in real time for their own threat protection. And that is extremely powerful."
>
> **— Jess Parnell, Vice President of Security Operations, Centripetal Networks Inc.**

Results story

Automate threat protection to save time, money

By operationalizing threat intelligence pulled from the IBM Security X-Force Exchange Commercial API solution, Centripetal provides its customers with a cyberthreat defense solution that actively shields the highest-risk traffic in real time. Centripetal chose the IBM solution for its high quality and because it is designed for reliability. The IBM Security X-Force Exchange Commercial API is not a one-size-fits-all intelligence feed. Centripetal leverages the raw data dynamically in its inspection architecture based on its individual customers' needs.

"IBM provides very good indicators of compromise in a very timely fashion," says Parnell. "We bring in those indicators, and within minutes those indicators are protecting our clients across the board." The high-confidence indicator sets, coupled with a low rate of false-positives, have made the IBM Security X-Force solution valuable for Centripetal.

The company's CleanINTERNET service automates threat protection and shields against threats with negligible impact on network performance thanks to the performance of each of Centripetal's patented inspection technologies. This is the crux of the difference between traditional, manual security postures, and the CleanINTERNET service, according to Parnell. "It's really cool to show traditional security stack people how this all happens without any user intervention," he says. "We're using machine to machine, we're using high-quality data, we're dynamically responding to billions of threats, and all of that has no negative IT impact. But it does effectively shield you from attack."

The combination of automation and the high-quality threat intelligence from IBM Security X-Force creates other, indirect benefits for customers. For example, when Centripetal used the IBM Security X-Force and other threat intelligence data to shield against malicious activity at a large hospital system in the Northeast, the group saw a 70% reduction in attacks that needed to be investigated and resolved, which helped improve analyst efficiency and reduce costs. This allowed their team to concentrate on mission-critical risks to dramatically increase their cybersecurity posture. And, Centripetal reports the IBM Security X-Force service falls consistently within the top tier of solutions that reduce attacks by the greatest percentage.

According to Ahn, the IBM Security X-Force solution and the Centripetal CleanINTERNET service are a winning combination. "It's the reliability and the consistency of the IBM threat research, input into our approach for applied intelligence, that leads to proactive protection," he says. "And the IBM research carries a lot more weight than some intelligence developed ad hoc."

Centripetal's customers benefit from the highly reliable intelligence from the IBM Security X-Force Exchange through Centripetal's use of the IBM Security X-Force Exchange Commercial API service. "With the Centripetal solution, our customers are benefiting from the IBM analysts' opinions in real time for their own threat protection," says Parnell. "And that is extremely powerful."

Subscribing to the IBM Security X-Force Exchange Commercial API solution gives Centripetal access to the wider collection of intelligence available through the IBM Security X-Force Exchange platform portal. This includes information on specific security investigations, or collections, consisting of both unstructured and structured data, incident descriptions and associated observables relevant to the incident, and comprehensive intelligence on emerging threat indicators and the context to understand them. "We can go to the portal and get enough information so we can make quick decisions about what to tell our clients and also potentially how to remediate the threat," says Parnell.

IBM Security X-Force and Centripetal are looking to the future of working together to improve threat intelligence. Already, thanks to its experience with Centripetal, IBM has created an Enterprise API version of the IBM Security X-Force Exchange intelligence feed designed for the kind of massive threads that Centripetal consumes. "We now have a number of years of history [with IBM Security X-Force], and we think that there can be a lot more collaboration," concludes Parnell. "We are very excited about that and to explore those future steps."

> "The IBM research carries a lot more weight than some intelligence developed ad hoc."
>
> **— Dave Ahn, Chief Architect and Vice President, Centripetal Networks Inc.**

Centripetal

Centripetal Networks Inc.

Founded in 2009 and headquartered in Herndon, Virginia, Centripetal (external link) delivers intelligence-driven security. Centripetal invented the Threat Intelligence Gateway and leverages its technologies to deliver CleanINTERNET, a comprehensive intelligence-led

cyberservice. With Centripetal, customers across every vertical and of every size can persistently prevent over 90% of known threats with intelligence applied in advance. Centripetal's technology is protected by over 50 US and international patents and is deployed protecting critical networks globally.

Solution component

- IBM X-Force Exchange Commercial API

Take the next step

To learn more about the IBM solution featured in this story, please contact your IBM representative or IBM Business Partner.

Print

View more client stories

© Copyright IBM Corporation 2021. IBM Corporation, Security, New Orchard Road, Armonk, NY 10504

Produced in the United States of America, January 2021.

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks

of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.