DARKTRACE

CASE STUDY

Energy+

Overview

Industry

- Energy and Utilities

Challenge

- Incomplete visibility of the network
- Concerned about prevalence of fast-moving, automated attacks
- Wanted to adopt a proactive approach to cyber defense
- No ability to detect zero-day exploits

Results

- Threat Visualizer provides 100% network visibility
- Now capable of detecting 'unknown unknown' threats as they emerge
- Increased confidence in security stack and proactive approach
- Enterprise Immune System detects automated attacks in real-time

Business Background

Established over 100 years ago, Energy+ is a local energy distribution company. Based in Ontario, Canada, Energy+ provides electricity to over 64,000 residential, business, industrial, and institutional customers, covering roughly 1,700 square kilometers of power lines. Energy+'s network oversees the company's infrastructure, in addition to the sensitive information of thousands of stakeholders.

> Darktrace's machine learning approach means that our days of battling at the border are over... At the end of the day, the Enterprise Immune System is identifying threats as they are happening, and its spotting things that our legacy tools consistently miss.
>
> **Paul Martinello, Vice President of Information Technology**

Challenge

Given the rapidly-evolving threat landscape in Canada, Energy+ was primarily concerned about staying ahead of these sophisticated attacks. In particular, it was concerned about fast-moving and automated threats, like ransomware, that has the potential to compromise its network within minutes. With a security stack that primarily relied on border defense based on rules and signatures, Energy+ was unable to take a proactive approach to cyber defense.

Additionally, Energy+ felt it lacked visibility into its internal network. It wanted a solution that could provide insight into the behavior of users, devices, and the network as a whole. Whereas Energy+ had a myriad of security tools, it felt it lacked a technology that could detect 'unknown uknowns' and protect the network from the inside out.

"Before we deployed Darktrace, we had an incomplete picture of what was actually inside of our network," commented Paul Martinello, Vice President of Information Technology, Energy+. "We couldn't see any lateral activity, and it forced us to take a reactive approach to cyber defense – we needed a tool that could provide complete visibility, in addition to real-time threat detection."

"In security, its critical to have a layered approach," added Heath Higgins, Infrastructure and IT Specialist, Energy+. "We were missing a core layer, that could self-learn what's normal for our users and devices, and give us insight into the darkest corners of our network."

Solution

To meet this initiative, Energy+ installed Darktrace's Enterprise Immune System at the heart of its corporate network. After a swift installation, the value was immediately shown to the Energy+ security team. Darktrace instantly mapped the entire network, including every user and device, on to the Threat Visualizer's 3D graphical interface – without the need to tune or configure the system.

A few weeks later, the technology alerted Energy+ to a serious anomaly: a user was going to a malware site in Russia. Days later, a user was detected uploading sensitive data into a third party cloud provider. Energy+'s existing security stack, including perimeter tools, had failed to catch these incidents. Because Darktrace was able to alert it in real-time, Energy+ was able to mitigate the threat before it evolved into a crisis.

"Darktrace's ability to detect even the subtlest threats was an eye-opener for us," commented Paul Martinello, Vice President of Information Technology, Energy+. "At the end of the day, the Enterprise Immune System is identifying threats as they are happening, and its spotting things that our legacy tools consistently miss."

Powered by unsupervised machine learning, the Enterprise Immune System works by establishing a 'pattern of life' for every user and device within Energy+'s network. With the probabilistic understanding of what's normal and abnormal, potential cyber-threats can be detected at their nascent stages, before any damage is done.

Benefits

Armed with the Enterprise Immune System's innovative self-learning technology, Energy+ has renewed confidence in its security stack's ability to detect and mitigate evolving and increasingly automated attacks. Because the technology filters each threat by potential gravity, it also enables security professionals to optimize their resources for increased efficiency.

"The Energy+ security team is leaner, and we didn't have time to fine-tune the technology or input rules and signatures," commented Higgins. "With Darktrace, it automatically began learning and identifying sophisticated threats, without the need for configuration or the use of prior assumptions – allowing us to focus our time on only the most important in-progress threats."

With complete visibility of its network, Energy+ can now use the Threat Visualizer to obtain a complete picture of its network, including every user and device on the network, and all lateral movements, knowing that if significantly abnormal behavior occurs, security professionals will be alerted immediately.

"Darktrace's machine learning approach means that our days of battling at the border are over," added Martinello. "Before Darktrace, we had no way of preventing unknown threats, and we had a reactive approach to cyber defense. Now, the Enterprise Immune System secures our network from the inside out, allowing us to catch even the subtlest and most advanced forms of threat at their earliest stages."

By deploying the Enterprise Immune System, Energy+ has regained control of its network. Even as its network grows more complex, Darktrace will continue to adapt and learn so that Energy+ can always remain one step ahead in the face of a rapidly-evolving threat landscape.

> With Darktrace, it automatically began learning and identifying sophisticated threats, without the need for configuration or the use of prior assumptions – allowing us to focus our time on only the most important in-progress threats.
>
> **Paul Martinello,**
> **Vice President of Information Technology**

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010

info@darktrace.com
darktrace.com