Billtrust

Overview

Industry

○ Financial Services

Challenge

○ Limited security resources

○ No tool to detect zero-day threats

○ Limitations of existing security tools to visualize anomalies in real time

○ Wanted to adopt a proactive approach to cyber defense and threat mitigation

Results

○ Deployed Enterprise Immune System at the heart of the network

○ Takes the burden off lean security team

○ Gives 100% real time threat detection and visualization

○ Increased confidence in security stack in face of changing threat landscape

Business Background

Based in Hamilton, New Jersey, Billltrust is the leading provider of outsourced billing services and payment cycle management. Its payment solution integrates three key areas of the invoice-to-cash process: presentment, payment, and cash application. With clients across many different industry sectors, Billtrust handles the sensitive banking information of over 4.5 million users.

> With the Enterprise Immune System, the machine learning technology allows our security team to focus on the real threats, without having to tune or tweak the software.
>
> **Laura Whitt-Winyard**
> **Director of Information Security**

Challenge

In today's rapidly-evolving threat landscape, it is critical for financial institutions to protect their data against potential attacks. Increasingly sophisticated, silent, and advanced threat actors target these types of organizations to extract or even change private banking information, with the potential to undermine trust and credibility in banks and services.

With this in mind, Billtrust wanted to ensure it was taking a mature security posture, especially given a stringent regulatory environment. Billtrust needed a technology that could detect zero-day threats without having to be continuously updated. Further, the security team felt that its existing tools could not visualize the entire network. Billtrust wanted a security tool that would also allow it to spot rogue devices and abnormalities within the network, in real time.

Solution

Following a thorough market review, Billtrust selected Darktrace's Enterprise Immune System to deploy into its own network for a four-week Proof of Value. "When we first heard of Darktrace, we thought it was too good to be true," commented Laura Whitt-Winyard, Director of Information Security at Billtrust. "However, the day it installed, we saw immediate return on investment". Based on unsupervised machine learning and new developments in Bayesian mathematics from specialists at the University of Cambridge paired with insight from government intelligence experts, Darktrace's innovative technology learns 'self' for a network as soon as it is installed. Once deployed, Darktrace's Enterprise Immune System immediately began mapping Billtrust's network and establishing a 'pattern of life' for every user and device.

Billtrust uses the Threat Visualizer on a daily basis to see and investigate potential threats in real time, before they escalate into a crisis. By visualizing all network traffic on the 3D graphical interface, Billtrust can see everything on their network: from understanding insider traffic, to spotting rogue devices within the PTI environment. "We are so grateful for the Darktrace solution," added Whitt-Winyard. "With over a thousand IP addresses and millions of sensitive user data, it's critical for us to be able to visualize exactly what is happening within our network. We needed a product that could show us network traffic, rogue devices, and abnormalities in real time, and Darktrace provided exactly that."

The understanding of normality for every individual user, device, and network enables the Enterprise Immune System to grow with the company, adapting to changes, and detecting potential threats, even in times of transition and growth.

Benefits

Due to the Enterprise Immune System's unique ability to learn a sense of 'self', Billtrust now has complete awareness of its entire network. Darktrace is able to detect threats that have never occurred before, the 'unknown unknowns'. Each threat is ranked according to the level of deviation from 'normal' for that network, allowing Billtrust's security team to focus on only the most important threats via the Threat Visualizer. Billtrust can now stay ahead of zero-day threats and focus on legitimate attacks or threats, in real time.

"With the Enterprise Immune System, the machine learning technology allows our security team to focus on the real threats, without having to tune or tweak the software," added Whitt-Winyard. "We no longer have to try and define what 'bad' looks like in advance. We all feel more comfortable knowing that Darktrace's technology understands what is normal for our network and will detect the anomalies and legitimate threats."

By basing its security stack on Darktrace's advances in unsupervised machine learning, Billtrust has increased its confidence that its sensitive customer information is protected from rapidly-evolving cyber-threats. The company has also found that, aside from real-time awareness of network traffic, the Threat Visualizer also helps raise security policy awareness within the company. By relying on 'immune system' technology, Billtrust has established itself as an industry leader and remains proactive in the face of sophisticated and advanced forms of cyber-threat.

> "
> We needed a product that could show us network traffic, rogue devices, and abnormalities in real time, and Darktrace provided exactly that. "

Laura Whitt-Winyard
Director of Information Security