blackpoint

CASE STUDY

Blackpoint Responds to Business Email Compromise

A Look at Cloud Response's Capability

Introduction

When we set out to create Blackpoint Cloud Response, our goal was to actively protect online workflows and remote workers. As crucial to business operations as on-premises activity is, we built the first MDR for the cloud. Over the last year, our partners and their end clients have experienced a new level of 24/7 protection. While they are enjoying time out of the office, our around-the-clock security analysts are leveraging our patented technology to protect your six. Read on to learn about two of our partners' experiences.

About Blackpoint Cloud Response

Cloud Response is a Blackpoint ecosystem add-on that integrates with SNAP-Defense, taking Blackpoint's MDR to the cloud. It enables our 24/7 SOC to see contextual data within Microsoft 365 environments and provide active response to even the fastest, most advanced cyberthreats. Additionally, partners can review policy settings and configure custom notifications directly in the portal. Set up can be done within minutes, and onboarding tenants is straightforward. *This add-on solution currently protects Microsoft's 365 service, including Azure Active Directory (AD), Exchange, and SharePoint.*

Blackpoint-Powered MSSP Protects an HVAC Company

BLACKPOINT PARTNER: Advantage Industries

TIME FRAME: 14 minutes from first alert to account disablement.

Advantage Industries is a managed security service provider that has served the Baltimore, DC, and northern Virginia region since 1999. A couple of years ago, they added Blackpoint Cyber to their security stack. The majority of their end clients now benefit from Blackpoint's 24/7 MDR, Cloud Response, and LogIC.

"It's a huge safety blanket for us. We're not a 24/7 shop so having this peace of mind that our clients are [protected around the clock] from malicious activity on their 365 accounts and their endpoints is huge for us," said Sean Weatherford, their Service Desk Manager. Kevin Dubois, Director of IT Services, chimed in, "We're also not even 24/7 with on-call, so it's a big add to have coverage there."

On August 9, 2022, they were glad to have 24/7 security. Before either Advantage Industries, or their end client, Commercial Express HVAC, were open for business, malicious actors attempted to access a Commercial Express HVAC employee's Microsoft 365 account from IP address located in the Netherlands and Nigeria.

> **"...We're not a 24/7 shop so having this peace of mind that our clients are [protected around the clock] from malicious activity on their 365 accounts and their endpoints is huge for us."**
>
> *– Sean Weatherford, Service Desk Manager, Advantage Industries*

Detection

08/09/22 – 05:14 A.M. EST

Blackpoint received a Cloud Response alert within SNAP-Defense for 'Login from New Device and IP.' The location, Netherlands, was labeled risky (see Figure 1).

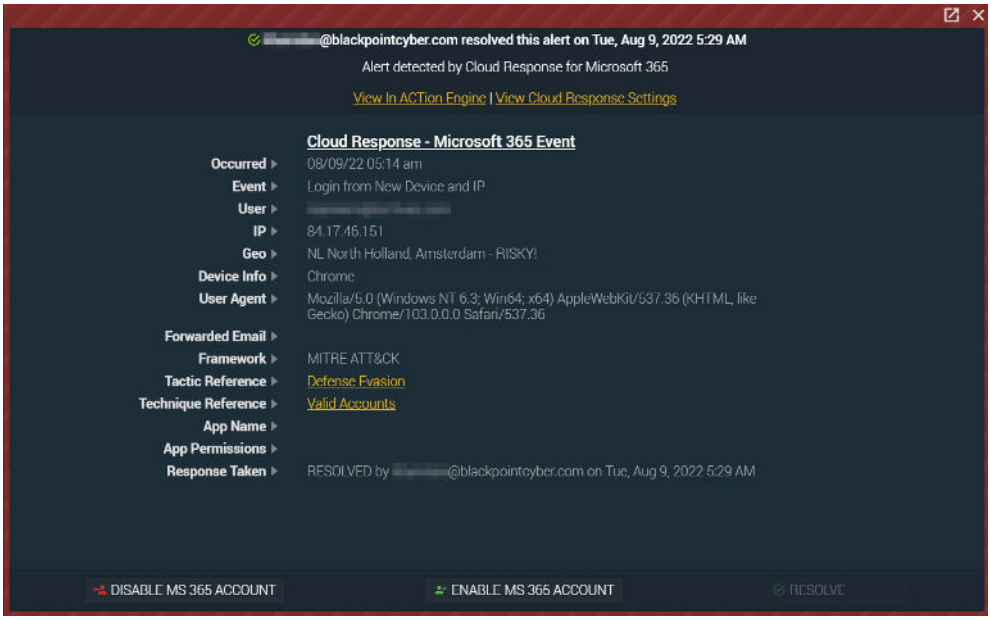

Figure 1: Amsterdam, North Holland, Netherlands Login

08/09/22 – 05:21 A.M. EST

Blackpoint received a Cloud Response alert within SNAP-Defense for 'Login from Unapproved Country.' The location, Nigeria, was labeled risky (see Figure 2).

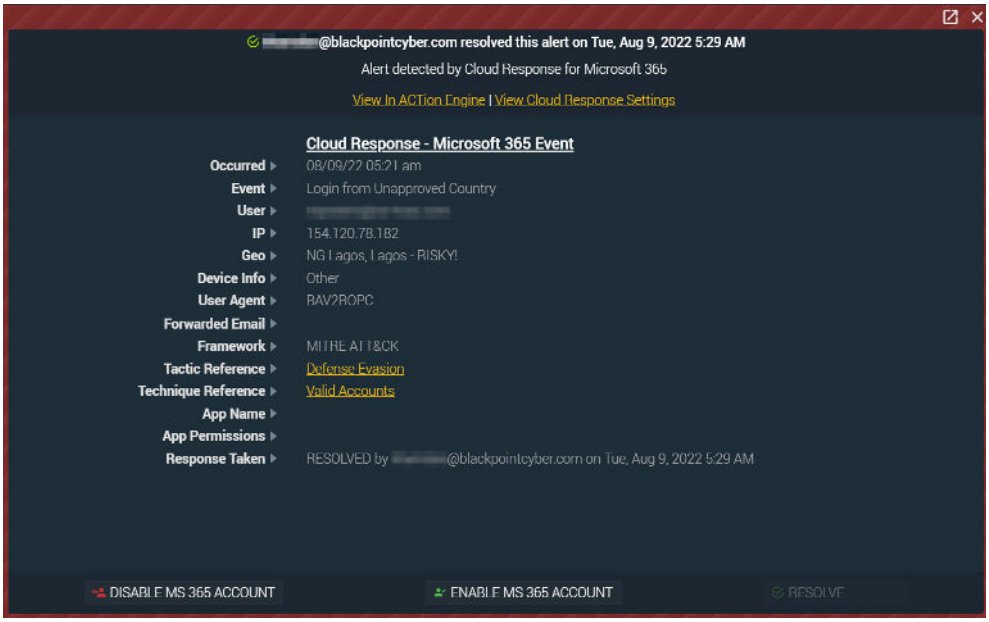

Figure 2: Lagos, Nigeria Login

08/09/22 – 05:23 A.M. EST

An MDR analyst escalated the ticket after reviewing both Cloud Response alerts for unapproved logins from risky countries.

08/09/22 – 05:23 A.M. EST

A Senior MDR analyst acknowledged and reviewed the escalation.

Alerts and Response

08/09/22 – 05:28 A.M. EST

The Senior MDR analyst:

- disabled the M365 user account,
- reached out to the partner on the emergency contact line, and
- began working on the incident response report.

08/09/22 – 07:34 A.M. EST

The Senior MDR analyst sent the incident response report to the partner.

Advantage Industries opened for the day at 8 a.m.

"By 8:30 a.m., we had already reached out to our points of contact there and started working through the process of getting the user set back up with their accounts, getting them back in, and making sure there were no more bad actors in there," recalled Sean. "They were obviously grateful that this was caught. We were able to get the user back into their accounts by 9:15 a.m. It was not a large disruption to their workday [which begins between 6-6:30 a.m.] ...The downtime in the grand scheme of things was minimal, which was fantastic."

14 minutes
from first alert to account disablement.

Blackpoint-Powered IT Service Provider Protects a Property Management Company

BLACKPOINT PARTNER: DenaliTEK

TIME FRAME: Three minutes from alert to account disablement.

Since 2001, DenaliTEK has provided IT services for small- and medium-sized businesses in south central Alaska. While developing their MSP offering in the spring of 2021, they added an important part of their security stack—the ability to detect and stop security threats. Now partnered with Blackpoint Cyber, their 24/7 on-call team is empowered with critical alerts to tend to cyberthreats any hour of the day.

While it was still the middle of the night for Alaskans, a malicious actor in Poland was spending their mid-day attempting to enter the DenaliTEK end client's Microsoft 365 account. Thankfully, Blackpoint's 24/7 SOC team was there to terminate the malicious act within three minutes.

Detection

08/10/22 – 05:57 EST

Blackpoint received a Cloud Response alert within SNAP-Defense for 'Login from New Device and IP.' The user was from an unapproved country, Poland, and was gaining connection through Tor (see Figure 1).

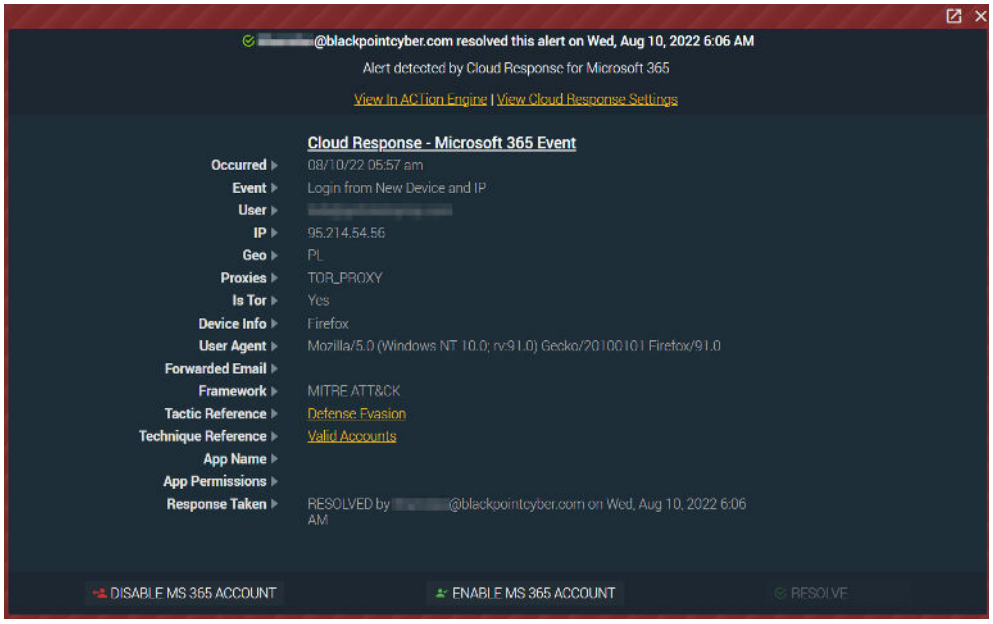

Figure 1: Poland Login

> **"Without having the partnership with [Blackpoint Cyber], we wouldn't have the alerts that we need."**
>
> *– Todd Clark, President, DenaliTEK*

What is Tor?

The Onion Router (Tor) is a web browser designed for anonymous web surfing and protection against traffic analysis. Tor is often associated with the Dark Web and criminal activity but is also used by individuals for legitimate reasons.

That said, Tor can be dangerous because of the level of anonymity it provides an attacker. Cyberattackers and hacking groups often use Tor to conduct attacks against organizations, making it difficult for cyber defenders and law enforcement agencies to uncover geolocation and other details about their base of operations.

08/10/22 – 05:58 EST

An MDR analyst escalated the ticket after reviewing the Cloud Response alert.

08/10/22 – 05:59 EST

A Senior MDR analyst acknowledged and reviewed the escalation.

Alerts and Response

08/10/22 – 06:00 EST

The Senior MDR analyst disabled the M365 user account.

3 minutes
from alert to account disablement.

08/10/22 – 06:06 EST

The Senior MDR analyst got through to the partner on their emergency contact line.

08/10/22 – 06:07 EST

The Senior MDR analyst began working on the incident response report.

08/10 – 06:25 EST

The Senior MDR analyst sent the incident response report to the partner.

By 3:34 a.m. AK, or 7:34 a.m. EST, DenaliTEK's on-call staff was able to report the resolved incident to the end client, hours before they would arrive at work.

"It's an important part of the system. Having the [Blackpoint] software and SOC [allows us to] know when something is going wrong...Without having the partnership with [Blackpoint Cyber], we wouldn't have the alerts that we need," summarized Todd Clark, DenaliTEK President.

Email and Cloud Security

Controlling access to your business' accounts and data around the clock is crucial. The most effective way to prevent Microsoft 365 account compromise and malicious foreign logins is to ensure multi-factor authentication (MFA), preferably app-based, is enforced on all human-associated accounts. In fact, MFA on accounts with administrative rights should be mandatory. Failure to do so will almost certainly lead to account compromise. In addition, controlling access to your cloud accounts based on location is imperative, especially amidst remote work.

With Blackpoint's Cloud Response, partners can create an approved list of countries, specific to the user, which can be active, upcoming, and/or temporary. Email notifications can also be turned on for when logins from unapproved countries occur.

Online settings and automated responses can't be your only defense, though. Adversaries' tactics, techniques, and procedures (TTPs) are adapting and advancing every day. A team of live security analysts are necessary to combat any threats that get through. Whether proper security settings are turned on or not, our 24/7 SOC team is here to address alerts, read into the context, and respond appropriately. With Cloud Response, you're able to sleep at night.

ACTIVE RESPONSE FOR YOUR CLOUD

- ✔ Trust in the human element
- ✔ MDR for the cloud
- ✔ Guided onboarding
- ✔ Manageable custom notifications
- ✔ Security policies in one click

Why Blackpoint Cyber?

Founded in 2014 by former National Security Agency (NSA) cyber operations experts, the Blackpoint team continues to bring nation-state-grade technology and tactics to our partners around the world. By fusing real security with real response, our elite SOC team is empowered by the proprietary technology we built from the ground up.

Together, we detect breaches faster than any other solution on the market. With insight into network visualization, tradecraft detection, endpoint security, suspicious events, and remote privileged activity, Blackpoint detects lateral movement in its earliest stages and stops the spread.

By the time you hear from us, the threat has been triaged and removed, often before the malicious actor even saw us coming. Lastly, we optimize our architecture and data to its fullest extent, ensuring robust services and valuable intel for our partners. That way, all facets of security—response, logging, cloud protection, and cyber insurance—can work in tandem to support an integrated cyber strategy. Sleep easy knowing we detect and detain threats on your behalf around the clock.

Our mission? To provide unified, 24/7 detection and response services to organizations of all sizes around the world.

SIGN UP FOR A DEMO TODAY!

CONTACT US

info@blackpointcyber.com

blackpointcyber.com