blackpoint

Cloud RESPONSE

Year in Review

At the beginning of 2022, we had a simple, yet complex, goal—take MDR where it had never been before: the cloud. As companies settled into their 'new normal' post-COVID, we knew that hybrid and cloud-based work environments weren't going anywhere. This expanded attack surface demands protection of the same caliber as our true, in-house MDR—24/7, fully managed protection brought to you by the Blackpoint SOC. While most solutions on the market require you to act on alerts independently, we sought to provide fast and unified response to cloud threats on your behalf.

So that's what we did.

From June 2022 to now, we have:

1,389

Disabled 1,389 potential Business Email Compromise attacks

19 minutes

Maintained an average response time of 19 minutes for senior MDR analysts to resolve escalations

1.88x

Handled 1.88x more Cloud Response alerts than on-premises MDR alerts

Our observations have led to the following conclusions:

Top 5 common cloud attacks seen:

1. **Lack of multifactor authentication / MFA bypass**
2. **RSS and external forwarding rules**
3. **Logins from proxy or VPN to bypass conditional access geoblocking**
4. **Legacy authentication**
5. **Logins from suspicious user agents**

Top 5 countries seen brute forcing:

1. **China**
2. **US** *(There are many proxies to the US due to people geoblocking and detecting other countries.)*
3. **India**
4. **Korea**
5. **Brazil**

Business email compromise also continues to be a prevalent threat. While new tactics, techniques, and procedures are always sure to arise, threat actors will never abandon the basics: gain entry via email.

According to Verizon's 2023 Data Breach Investigation Report, BEC attacks have almost doubled, and email alone makes up 98% of initial access vectors in social engineering breaches. Additionally, according to IBM's Security X-Force Threat Intelligence Index 2023, the average number of spam emails with encrypted compressed extensions attached, delivered per week, increased ninefold in 2022.

When it comes to protecting your business and clients from these email threats, time is of the essence. While other vendors can take an hour or more to respond, our Blackpoint SOC prides itself on responding within minutes. Whether that's during your morning meeting, when you're packing up for the day, or while you're asleep, our SOC team is actively protecting you.

Cloud Response doesn't stop there, though. It isn't in our Blackpoint blood to 'set and forget.' Over the last year we've analyzed our internal data alongside the Adversary Pursuit Group to launch necessary, innovative updates to this product. In mid-July, we launched the following updates, enhancing our partners' experience with faster response and better visibility.

98%

BEC attacks have almost doubled, and email alone makes up 98% of initial access vectors in social engineering breaches

9x

the average number of spam emails with encrypted compressed extensions attached, delivered per week, increased ninefold in 2022

FASTER RESPONSE

- **Record Suspicious Forwarding Rule, MFA Capture:** We can now immediately detect instances of Suspicious Forwarding Rules
- **Detect Cloud Devices on New Device IP:** We can isolate devices on IPs outside of typical usage, should Microsoft 365 Single Sign On get compromised

BETTER VISIBILITY

- **Impossible Travel Ingest:** We'll know if impossible travel is occurring, such as bouncing between time zones or countries*
- **New notifications on:**
  - All Cloud Response detections
  - Cloud Response becoming disabled or deleted
  - Classifications and warnings for potential threats

**Available with upgraded Microsoft license*

About Cloud Response

Cloud Response extends Blackpoint's managed detection and response (MDR) service and 24/7 security operations center (SOC) to support hybrid and cloud environments, minimizing your attack surface so you can operate your business safely. Currently, Cloud Response supports Microsoft's 365 service including Azure Active Directory (AD), Exchange, and SharePoint.

Unsure if Cloud Response is the right fit for your business? You're not alone! More than 75% of Palo Alto Network's *The State of Cloud Native Security Report 2023* respondents reported their organization struggles to identify which security tools can help meet their needs. Therefore, they're testing us!

In July, a long-time MSProtect partner of ours did some troubleshooting with licensing in their tenant. One of our top competitors alerted the partner as well, but our MDR-enabled SOC beat them by an hour. When all was said and done, we prevented 47 Business Email Compromise attacks and 16 SNAP-Defense incidents.

Ready to see active response in the cloud for yourself?

SIGN UP FOR A DEMO NOW!

blackpoint

blackpointcyber.com