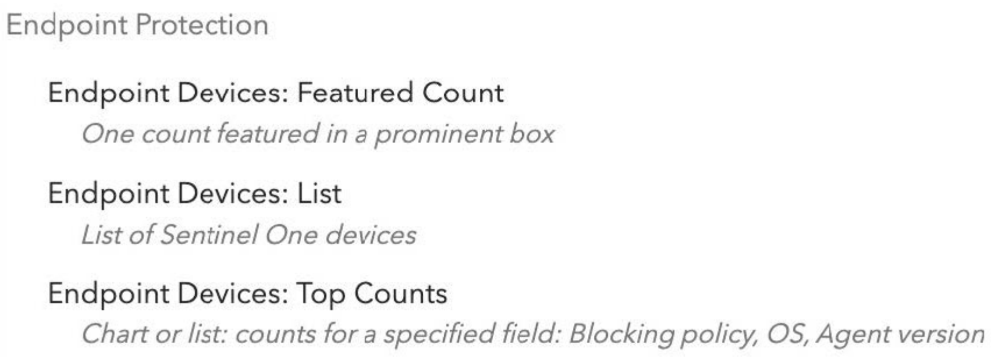
Barracuda XDR Release Notes — June 2023

https://campus.barracuda.com/doc/99616709/

The Barracuda XDR June release includes:

- **Customer Support** – XDR users can now contact Customer Support for security or technical support. For more information, see Contacting Customer Support.
- **More Customization for Reports** – We've expanded the customization available in the Build Your Own Report feature. This helps users tailor reports to what is most meaningful/relevant and helps users communicate the value that XDR brings to stakeholders. The added Managed Endpoint components are:
  - Endpoint Devices: Featured Count
  - Endpoint Devices: List
  - Endpoint Devices: Top Counts



Endpoint Protection

Endpoint Devices: Featured Count

One count featured in a prominent box

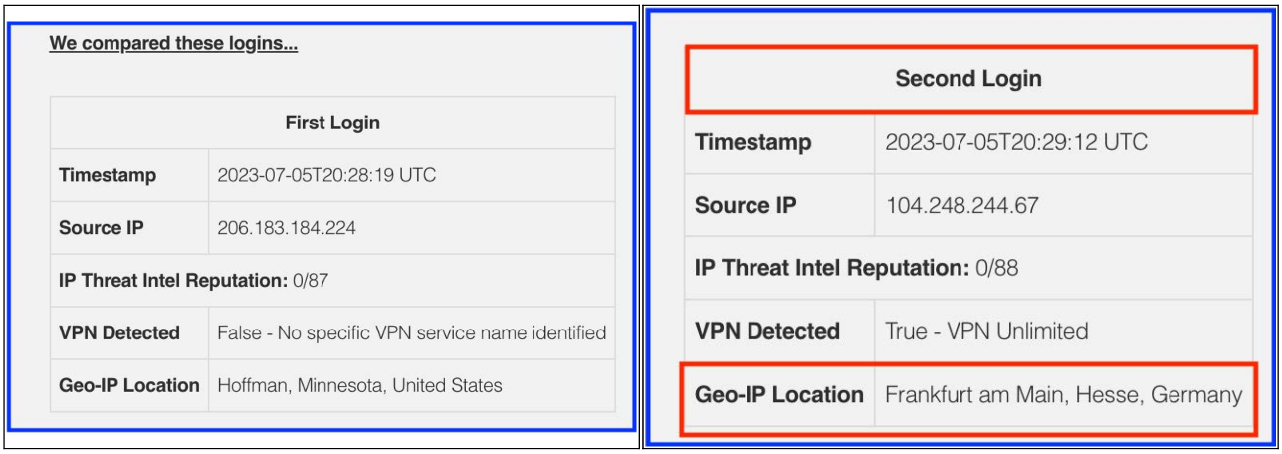
Endpoint Devices: List

List of Sentinel One devices

Endpoint Devices: Top Counts

Chart or list: counts for a specified field: Blocking policy, OS, Agent version

- **Enhanced M365 Impossible Travel Rule –** This rule calculates the distance and speed for every pair of user logins to determine if the distance change is feasible. If triggered, this could indicate a compromised account or other malicious activity. This improved detection includes more data to eliminate false positives.

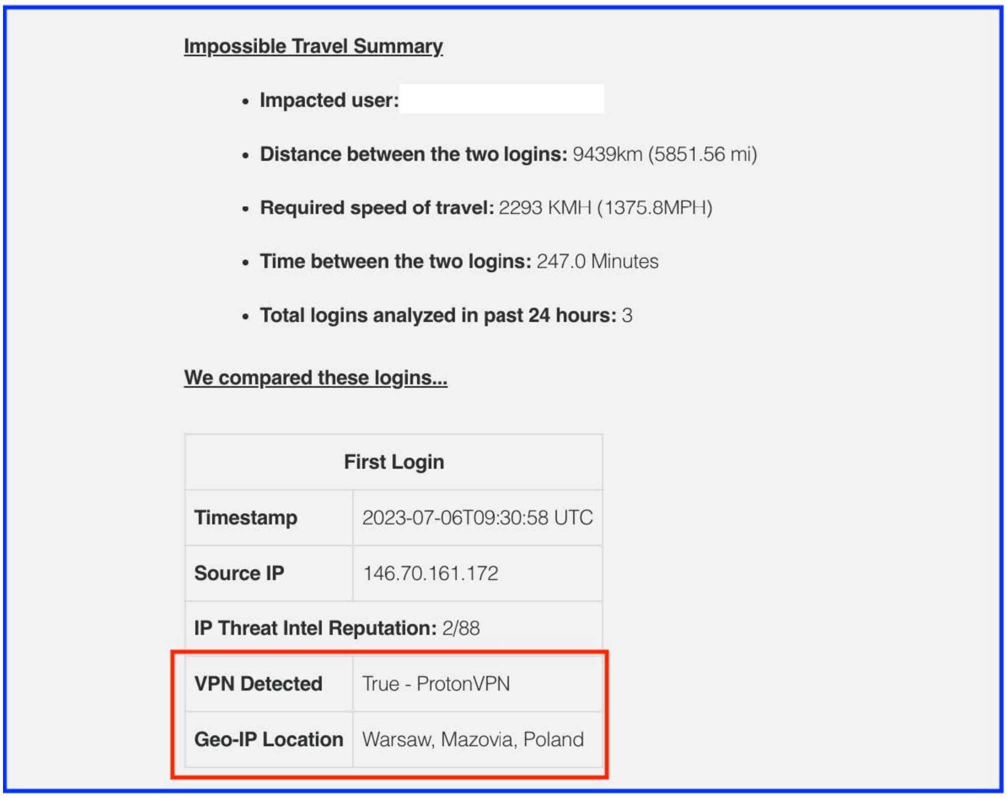


We compared these logins...

First Login	
Timestamp	2023-07-05T20:28:19 UTC
Source IP	206.183.184.224
IP Threat Intel Reputation: 0/87	
VPN Detected	False - No specific VPN service name identified
Geo-IP Location	Hoffman, Minnesota, United States

Second Login	
Timestamp	2023-07-05T20:29:12 UTC
Source IP	104.248.244.67
IP Threat Intel Reputation: 0/88	
VPN Detected	True - VPN Unlimited
Geo-IP Location	Frankfurt am Main, Hesse, Germany

- **VPN Enrichment –** XDR will take into account when over 85 commercial VPNs are being used, in order to identify threats better and eliminate false positives.



Impossible Travel Summary

- **Impacted user:** [redacted]
- **Distance between the two logins:** 9439km (5851.56 mi)
- **Required speed of travel:** 2293 KMH (1375.8MPH)
- **Time between the two logins:** 247.0 Minutes
- **Total logins analyzed in past 24 hours:** 3

We compared these logins...

First Login	
Timestamp	2023-07-06T09:30:58 UTC
Source IP	146.70.161.172
IP Threat Intel Reputation: 2/88	
VPN Detected	True - ProtonVPN
Geo-IP Location	Warsaw, Mazovia, Poland

- **"Live Attack" intel** – We've created a honeypot to gather live attack threat intelligence. This information helps XDR stay on top of the ever-evolving threat landscape, turning defense traps into valuable intelligence.
- **Updated terminology** – We've updated the terminology in the Managed Endpoint Security (See **Intelligence** > **Endpoint Security**.) from "Threat Events" to "Threats". This ensures consistent terminology across the XDR Dashboard:
  - **Events**: Raw data being analyzed
  - **Threats**: Potential risks found in Managed Endpoint Security
  - **Alarms**: Potential risks found with other XDR products
  - **Alerts**: Potential risks found that have been escalated to the partner/customer

Figures