Barracuda XDR Release Notes — January 2024

https://campus.barracuda.com/doc/104369275/

Barracuda SecureEdge monitoring

Users who have a Network Security license can now integrate with Barracuda SecureEdge. This integration expands Barracuda XDR's coverage into another one of the most popular security products of our users.

New Security Detections

We've added the following new detections in the Network Security and Server Security categories:

Network Security

- **Watchguard Threat Detected and Not Blocked** - Encompasses all allowed events by the Intrusion Prevention System (IPS) and other threat-related activities identified by the Watchguard firewall. This includes but is not limited to, detecting DDoS attacks, botnet traffic, and file vulnerabilities, providing a comprehensive overview of potential security threats permitted through the firewall.
- **FortiGate Admin Login from Public IP** - Fully automated detection looks for successful external logins from potentially malicious public IP addresses to the FortiGate Firewall interface. Leveraging our robust threat intelligence and the Barracuda XDR risk score, we determine the legitimacy and reputation of these IP addresses.
- **Enhancement: Communication with Threat Intel IP** - Fully automated firewall-based detection monitors for successful inbound or outbound connections to or from malicious external source IPs. Using Barracuda XDR, this detection now correlates such traffic with a comprehensive threat intelligence database containing over 10 billion IOCs.
- **External Permitted Malicious Traffic** - Fully automated Barracuda XDR IDS (Instruction Detection System) based detection monitors both inbound and outbound traffic for connections to known malicious external IP addresses. Also, by employing baseline analysis, we determine if the IDS signature generated is anomalous for the customer's environment. Furthermore, using Barracuda XDR's comprehensive threat intelligence database, we assess the risk score of the traffic based on the reputation of the external IP.
- **SecureEdge ATP Threat Detected** - Fully automated detection monitors for SecureEdge Advanced Threat Protection (ATP) events, providing protection against advanced malware, zero-day exploits, and targeted attacks. ATP employs scanning mechanisms to assess the legitimacy of files. Among others, ATP scans include Microsoft Office files, PDF documents, and ZIP files.
- **SecureEdge IPS Threat Detected** - Fully automated detection monitors for allowed SecureEdge Intrusion Prevention System (IPS) events are designed to scan both local and

forwarded traffic for malicious activities. The SecureEdge IPS engine analyzes network traffic and continuously compares the bitstream against its internal signature database to detect patterns of malicious code. This detection capability encompasses over 1000 IPS signatures within the SecureEdge database.

Server Security

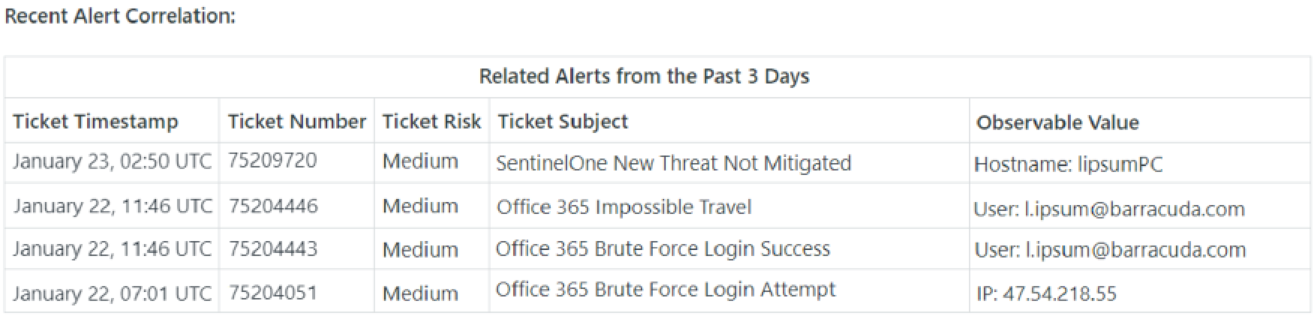
Seven new detections have been added for Windows monitoring, enhancing security against a range of potential threats. These include but are not limited to, detecting PowerShell-based activities like Kerberos ticket dumping, possible process injections, disabling firewalls, and turning off Defender security settings. Our detections monitor the creation of temporary scheduled tasks, which could signify unauthorized changes or activities in the system. These enhancements significantly bolster our ability to detect and respond to sophisticated threats in Windows environments.

- PowerShell Kerberos Ticket Dump
- Potential Process Injection via PowerShell
- Firewall Disabled via PowerShell
- Defender Security Settings Disabled via PowerShell
- Volume Shadow Copy Deletion via PowerShell
- RDP Enabled via Registry
- Temporary Scheduled Task Creation

Alert Enhancements: Alert Correlation for Automated Alerts

This feature not only streamlines the alert investigation process but also helps resolve alerts. When a new alert is generated, this feature automatically correlates and compiles all relevant alerts from the previous three days, integrating this comprehensive information directly into the ticket. It uses search parameters like related source/destination IPs, source/target usernames, and hostnames for thorough correlation.

This advanced functionality not only provides customers with immediate access to extensive contextual data, enabling quicker and more efficient investigations but also assists in the effective resolution of alerts.



Recent Alert Correlation:

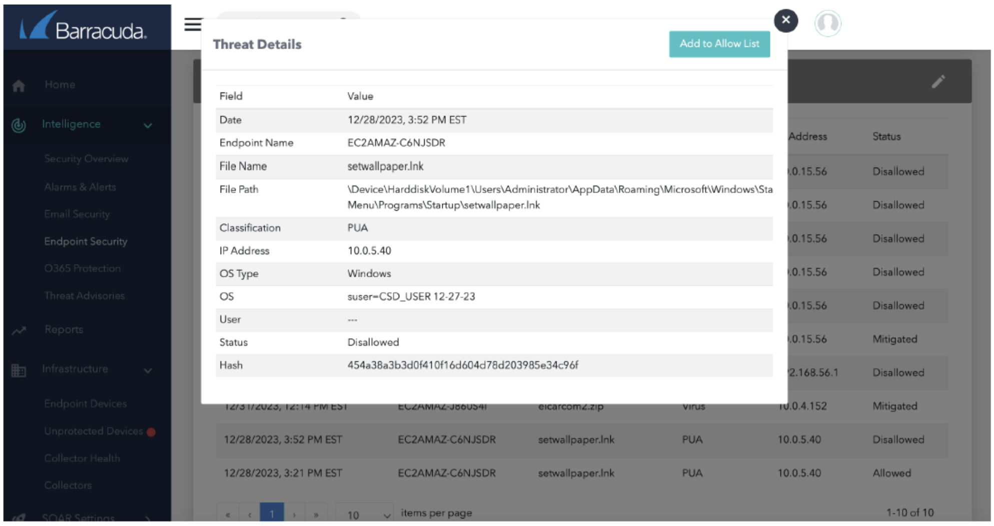
Related Alerts from the Past 3 Days				
Ticket Timestamp	**Ticket Number**	**Ticket Risk**	**Ticket Subject**	**Observable Value**
January 23, 02:50 UTC	75209720	Medium	SentinelOne New Threat Not Mitigated	Hostname: lipsumPC
January 22, 11:46 UTC	75204446	Medium	Office 365 Impossible Travel	User: l.ipsum@barracuda.com
January 22, 11:46 UTC	75204443	Medium	Office 365 Brute Force Login Success	User: l.ipsum@barracuda.com
January 22, 07:01 UTC	75204051	Medium	Office 365 Brute Force Login Attempt	IP: 47.54.218.55

Managed Endpoint enhancements

Self-service Allow List

Now users can quickly add threats to the Allow List without having to contact the SOC.

Self-service Allow Lists let users quickly mark threats as legitimate activity so they are ignored in the future. Threats are listed under **Intelligence** > **Endpoint Security**, and can be allowed by clicking the threat, then clicking the **Add to Allow List** button in the dialog box.



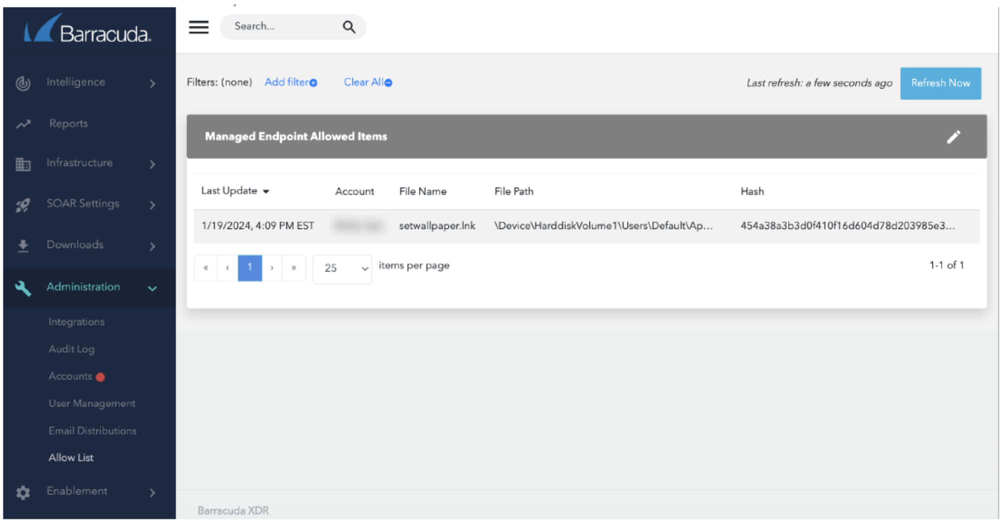
Threat Details

Field	Value
Date	12/28/2023, 3:52 PM EST
Endpoint Name	EC2AMAZ-C6NJSDR
File Name	setwallpaper.lnk
File Path	\Device\HarddiskVolume1\Users\Administrator\AppData\Roaming\Microsoft\Windows\Sta Menu\Programs\Startup\setwallpaper.lnk
Classification	PUA
IP Address	10.0.5.40
OS Type	Windows
OS	suser=CSD_USER 12-27-23
User	---
Status	Disallowed
Hash	454a38a3b3d0f410f16d604d78d203985e34c96f

12/28/2023, 3:52 PM EST	EC2AMAZ-C6NJSDR	setwallpaper.lnk	PUA	10.0.5.40	Disallowed
12/28/2023, 3:21 PM EST	EC2AMAZ-C6NJSDR	setwallpaper.lnk	PUA	10.0.5.40	Allowed

10 items per page 1-10 of 10

Once marked as allowed, the list of items can be found under **Administration** > **Allow List**.



Filters: (none) Add filter Clear All

Last refresh: a few seconds ago

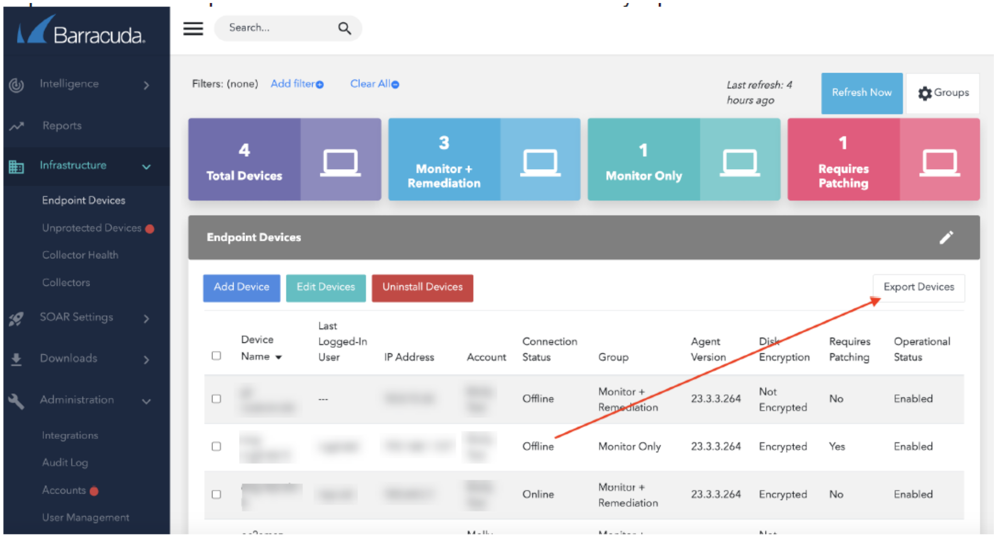
Managed Endpoint Allowed Items

Last Update	Account	File Name	File Path	Hash
1/19/2024, 4:09 PM EST	[redacted]	setwallpaper.lnk	\Device\HarddiskVolume1\Users\Default\Ap...	454a38a3b3d0f410f16d604d78d203985e3...

25 items per page 1-1 of 1

Export device list

Users can now export the list of Endpoint Devices to a CSV file letting you easily report on what is being monitored. On the **Infrastructure** > **Endpoint Devices** page, click the **Export Devices** button on the right in the **Endpoint Devices** table.



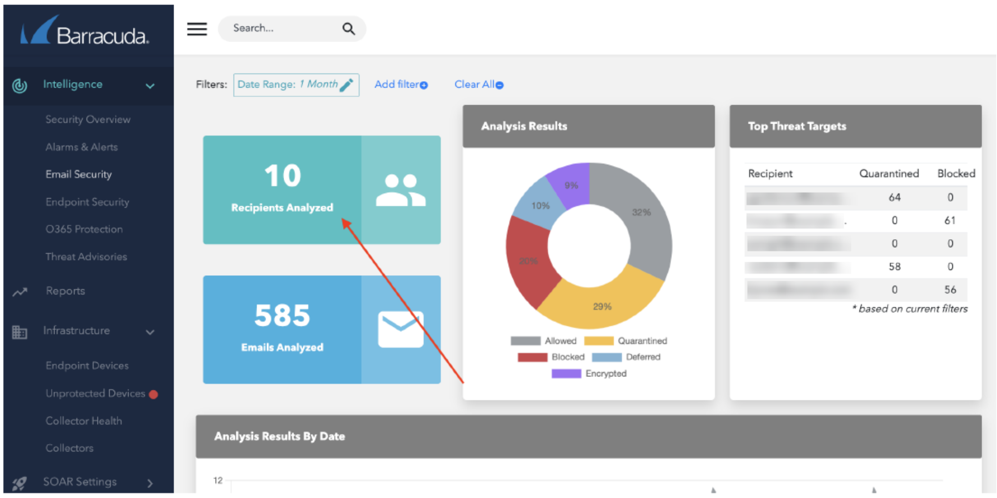
Endpoint Devices

	Device Name	Last Logged-In User	IP Address	Account	Connection Status	Group	Agent Version	Disk Encryption	Requires Patching	Operational Status
☐	[redacted]	---	[redacted]	[redacted]	Offline	Monitor + Remediation	23.3.3.264	Not Encrypted	No	Enabled
☐	[redacted]	[redacted]	[redacted]	[redacted]	Offline	Monitor Only	23.3.3.264	Encrypted	Yes	Enabled
☐	[redacted]	[redacted]	[redacted]	[redacted]	Online	Monitor + Remediation	23.3.3.264	Encrypted	No	Enabled

Ticket integration and other enhancements

To improve usability and minimize the learning curve, we've made the following changes:

- The configuration summary area now has a **Not Configured** status for better situational awareness.
- The UI text for deleting all settings for ConnectWise, ServiceNow, and AutoTask has been improved, making it clear that the user can only delete all settings and not an individual setting.
- In **Intelligence** > **Email Security**, the label has been changed from **Users Protected** to **Recipients Analyzed** to better reflect what is being represented.



Top Threat Targets

Recipient	Quarantined	Blocked
[redacted]	64	0
[redacted]	0	61
[redacted]	0	0
[redacted]	58	0
[redacted]	0	56

* based on current filters

- Under **Administration** > **Integrations**, Barracuda CloudGen has been renamed to Barracuda

CloudGen Firewall.

Figures