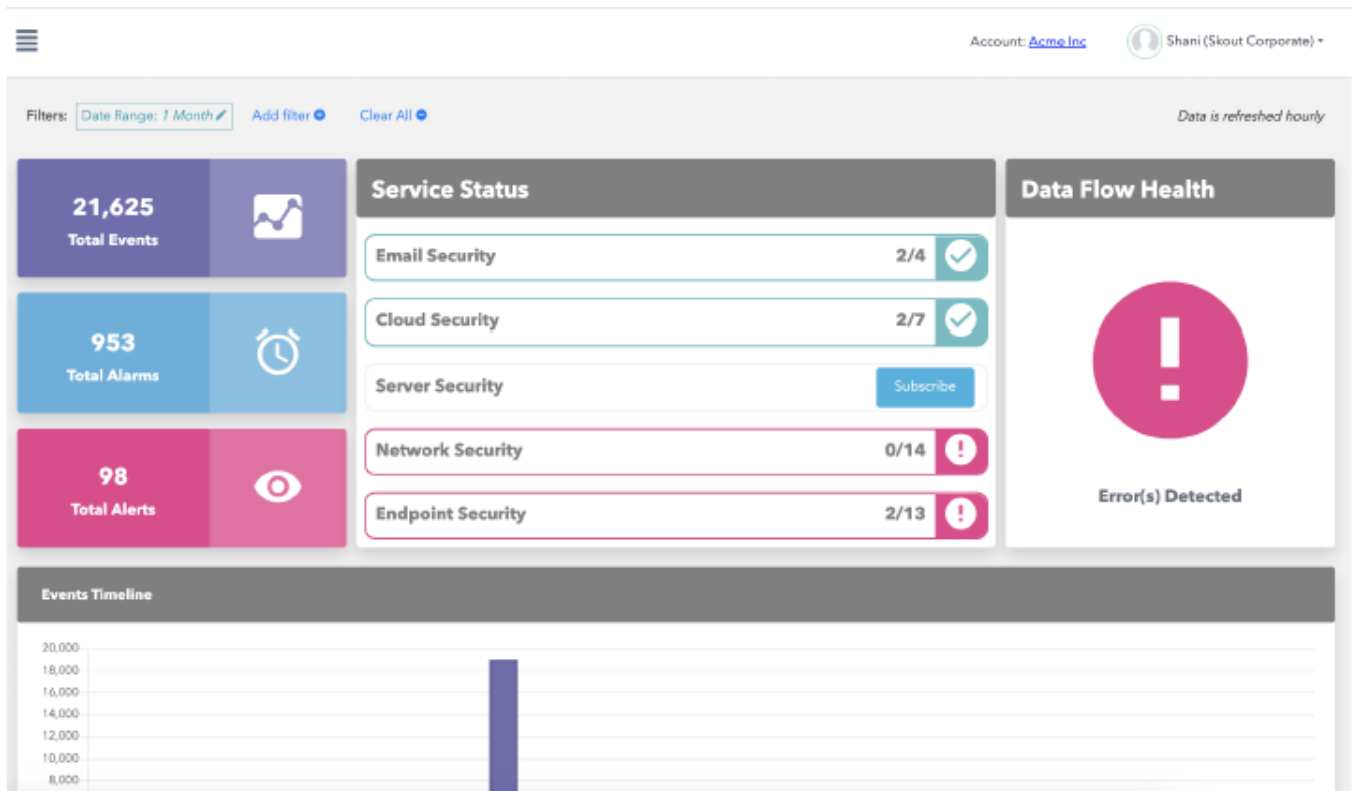


Barracuda XDR Release Notes — December 2022

<https://campus.barracuda.com/doc/98218124/>

New Homepage

The new homepage provides improved situation awareness. Many of the following features are supported when **All** is selected in the **Account** dropdown and will be particularly useful for users who manage more than one account.



The homepage introduces many new features, including:

- Realigned what **Alarms** and **Alerts** are and changed how **Alarms** are counted. An **Alarm** is a pattern of activity that implies a potential risk. This activity could indicate an identified threat to an information system, violate acceptable use policies, or the circumvention of standard security practices. An **Alert** is any **Alarm** escalated to a customer/MSP. Hover over **Alerts** to see how many are currently open.
- Also introduced a new statistic, called **Events**. An **Event** is a single, observable item in a monitored data source, e.g., a packet or token, aka the "raw data". The number of Events that XDR has analyzed demonstrates the amount of "work" needed to perform SOC duties and the value these services bring to XDR customers.

- **Events, Alarms, and Alerts** statistics are available when **All** is selected in the **Account** dropdown.
- **Service status** visualizes the different XDR products and what Integrations are available. **Service Status** communicates where XDR could provide more security coverage to the customer. Each service displays how many things you can monitor and how many you are monitoring.
 - There are two reasons a **Service Status** will get into an error state: A data flow issue, which will also show in the Data Flow Health area. This reflects data that was flowing into the XDR platform is now experiencing some sort of outage. Or no Integrations have been configured for a licensed product. This reflects an onboarding state for the respective product and will show the customer if they need to perform actions to get the data configured.
- **Data Flow Health** communicates whether there are issues with the configured Integrations. At any given point, the integrations being monitored by XDR could experience some sort of outage. This area is used to quickly communicate issues with a configured Integration. The **Data Sources** table below then shows which of the Integrations has the issue or validates that everything is flowing correctly. **Data Flow Health** is available when **All** is selected in the **Account** dropdown.
- **Events Timeline** visualizes all of the raw data being analyzed by XDR. Spikes in **Events** could indicate blocked brute-force attacks and other malicious activities. **Events Timeline** is available when **All** is selected in the **Account** dropdown.
- **Data Sources** table - Each row in the table represents an asset being monitored by XDR (e.g. a firewall, AWS CloudTrail, a Windows server, etc.) and helps customers manage that Integration. This table allows customers to readily see what assets are being monitored by XDR, including the total count of assets and relevant information about that **Data Source**. If the **Data Flow Health** on the top of the homepage is in an error or warning state, there will be one-to-many **Data Sources** listed in this table with either an error or warning. This gives customers the ability to readily identify what data may be experiencing outages. **Log Degradation**, which is enabled by default, creates Alerts if a Data Source is experiencing any type of loss or outage, can now be configured by clicking on the respective asset in this table. Once enabled, the outputted **Alerts** can be "snoozed" for either 1 day or 1 week to allow for legitimate maintenance activities on that asset. When the selected time passes, the **Log Degradation Alert** will be automatically reenabled. Customers can also disable this Alert altogether. The **Data Sources** table is available when **All** is selected in the **Account** dropdown.

Integration Enhancement

As an open-XDR platform, we are constantly expanding the data we can monitor to ensure we are meeting our customer's needs. As a result, we are excited to announce our newest Integrations, which are actively in beta:

- Mimecast
- Bitdefender

Updated Terms and Conditions

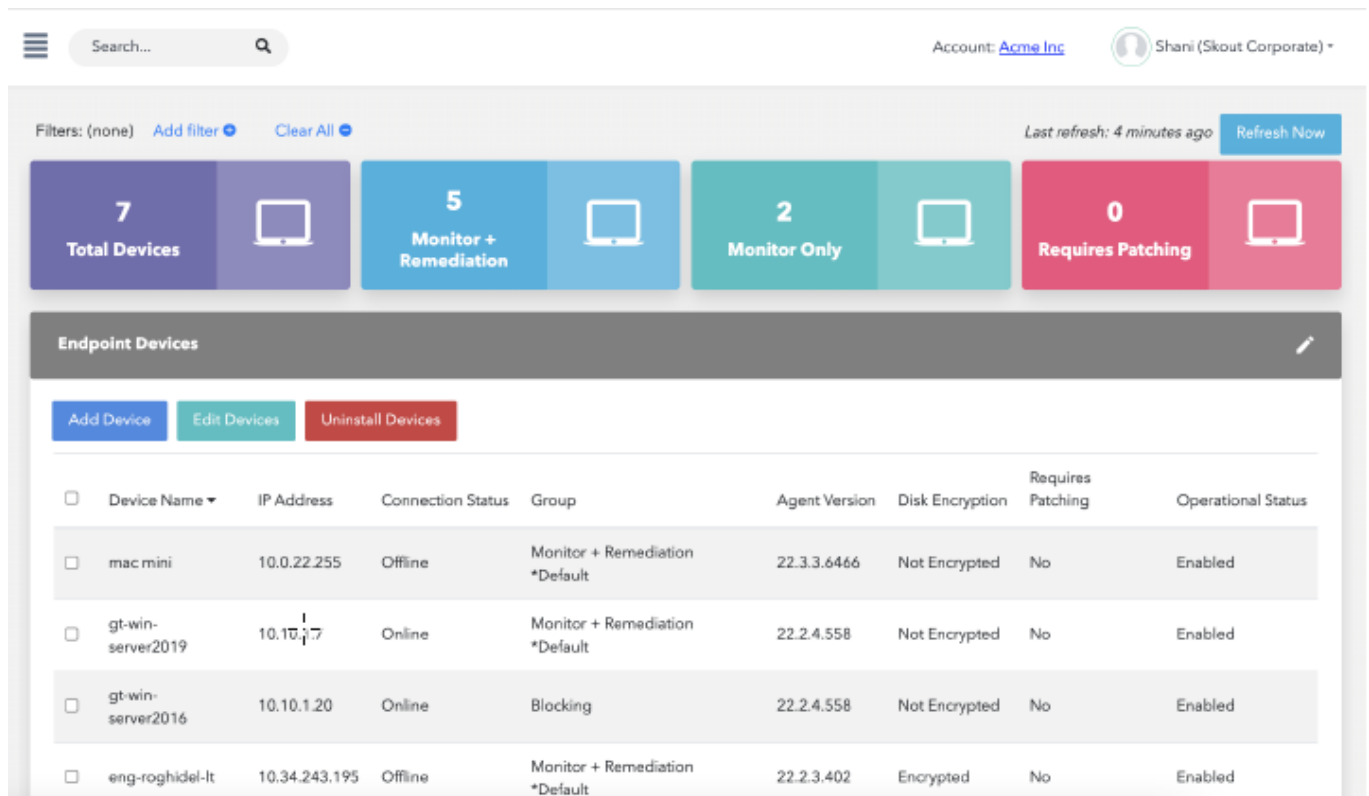
End-customer Terms & Conditions are executed for all new accounts, ensuring that Barracuda's responsibility is clearly communicated.

Enhancements to the Managed Endpoint Security service

Enhancements to the Managed Endpoint Security service includes:

- Exposing endpoint intel such as requires patching (OS- and application-level patches), has disk encryption, and more.
- Updated policy naming convention for all new customers to make it more user friendly.

Updates to the Setup > Integrations page



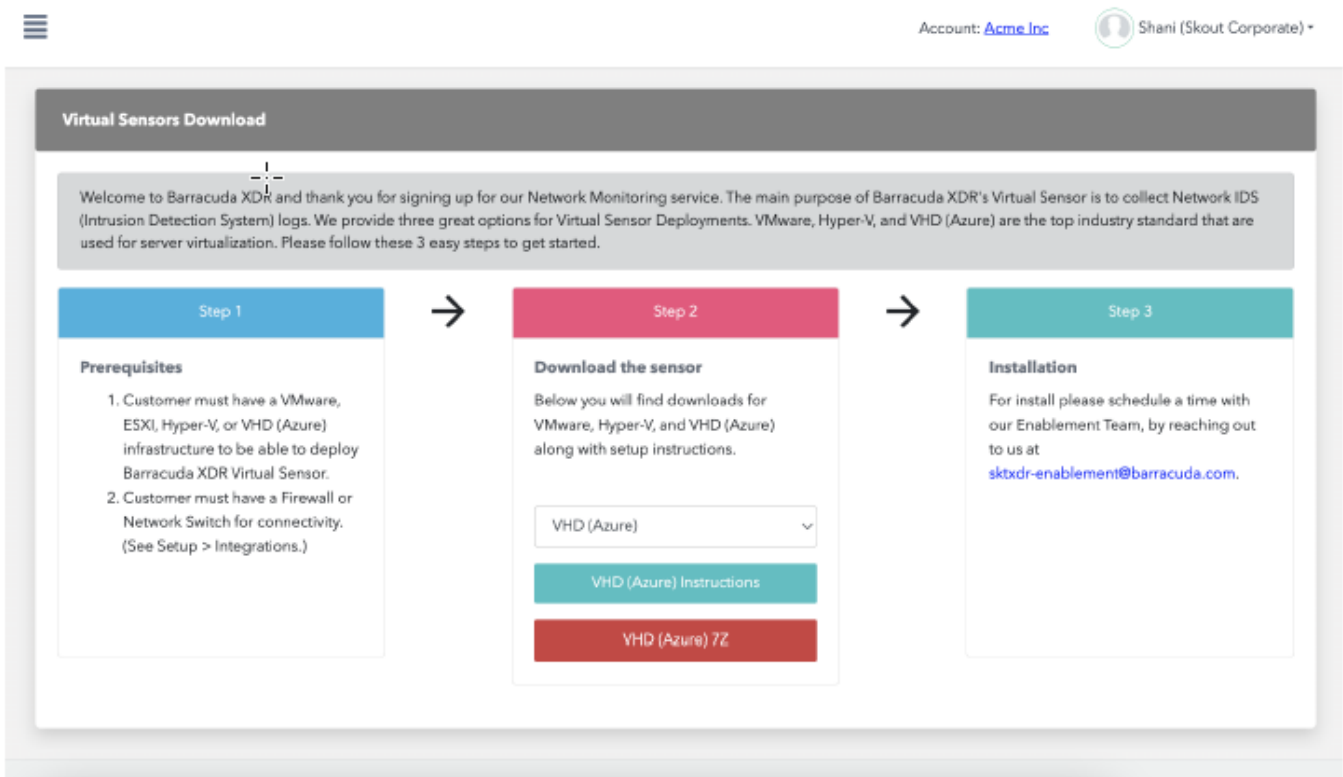
The screenshot shows the Barracuda XDR Managed Endpoint Security dashboard. At the top, there's a search bar and user information for 'Shani (Skout Corporate)'. Below this, a summary section displays four colored boxes: '7 Total Devices' (purple), '5 Monitor + Remediation' (blue), '2 Monitor Only' (teal), and '0 Requires Patching' (pink). Each box contains a laptop icon. To the right of these boxes, it says 'Last refresh: 4 minutes ago' and a 'Refresh Now' button. Below the summary is a table titled 'Endpoint Devices' with columns: Device Name, IP Address, Connection Status, Group, Agent Version, Disk Encryption, Requires Patching, and Operational Status. The table lists five devices: 'mac mini' (Offline, Monitor + Remediation *Default, Not Encrypted, No patching required, Enabled), 'gt-win-server2019' (Online, Monitor + Remediation *Default, Not Encrypted, No patching required, Enabled), 'gt-win-server2016' (Online, Blocking, Not Encrypted, No patching required, Enabled), and 'eng-roghidel-It' (Offline, Monitor + Remediation *Default, Encrypted, No patching required, Enabled). There are also buttons for 'Add Device', 'Edit Devices', and 'Uninstall Devices' above the table.

Device Name	IP Address	Connection Status	Group	Agent Version	Disk Encryption	Requires Patching	Operational Status
mac mini	10.0.22.255	Offline	Monitor + Remediation *Default	22.3.3.6466	Not Encrypted	No	Enabled
gt-win-server2019	10.10.1.7	Online	Monitor + Remediation *Default	22.2.4.558	Not Encrypted	No	Enabled
gt-win-server2016	10.10.1.20	Online	Blocking	22.2.4.558	Not Encrypted	No	Enabled
eng-roghidel-It	10.34.243.195	Offline	Monitor + Remediation *Default	22.2.3.402	Encrypted	No	Enabled

Updates include:

- New descriptions for each integration.
- Badges to visualize if the connection will use APIs, Syslog, or both.
- Show Barracuda IDS and Inky as available Integrations. That way, the number of Integrations found on the new homepage's Service Status now matches what is listed on this page when sorted by Product.
- UX enhancements.

Integration with Microsoft Azure



Virtual Sensors Download

Welcome to Barracuda XDR and thank you for signing up for our Network Monitoring service. The main purpose of Barracuda XDR's Virtual Sensor is to collect Network IDS (Intrusion Detection System) logs. We provide three great options for Virtual Sensor Deployments. VMware, Hyper-V, and VHD (Azure) are the top industry standard that are used for server virtualization. Please follow these 3 easy steps to get started.

Step 1

Prerequisites

1. Customer must have a VMware, ESXi, Hyper-V, or VHD (Azure) infrastructure to be able to deploy Barracuda XDR Virtual Sensor.
2. Customer must have a Firewall or Network Switch for connectivity. (See Setup > Integrations.)

Step 2

Download the sensor

Below you will find downloads for VMware, Hyper-V, and VHD (Azure) along with setup instructions.

VHD (Azure) ▾

VHD (Azure) Instructions

VHD (Azure) 7Z

Step 3

Installation

For install please schedule a time with our Enablement Team, by reaching out to us at sktxdr-enablement@barracuda.com.

You can now integrate Microsoft Azure using the XDR Virtual Sensor.

Also

- Various backend enhancements for upcoming releases.
- Various bug fixes, including **Threat Advisories** being shown in the Dashboard.

Figures

1. 2023-01-03_13-53-19.png
2. 2023-01-03_13-54-07.png
3. 2023-01-03_13-54-35.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.