**What is the Alchemy Gold Discovery Appliance (BlockBox)?**

The BlockBox Appliance is a hardened Linux [virtual appliance](#Scenario ) with an on-board web server designed to provide a richly detailed but easy to understand portrait of your IT environment.

The information capture elements of the BlockBox are designed to capture an exhaustive and accurate inventory of all endpoints - Windows PCs and Servers, Linux or Solaris systems, OSX devices, SNMP-enabled Layer 2 & Layer 3 devices, or even mobile devices connected to your wireless network.

The on-board reporting provided by the BlockBox is designed to be easy to use, to require the fewest clicks possible, and to answer key questions about the hardware and software present in your environment.

We’d love to get the BlockBox stood up and deployed as soon as is convenient to get the most amount of time possible for discovery, which should allow ample time to capture the machines as they come on and off the network.

*Below is an illustrative example of how we might configure the different appliances, should we require more than one, and how they will all check back into our master reporting server:*

# BlockBox Network Diagram



***Fig 1.1: Data being collected locally, and optionally communicating with the Combine Online Reporting Server.***

# **Alchemy Gold BlockBox Discovery Appliance: Prework Instructions**

## For this deployment, you will need:

* The BlockBox appliance deployed on a virtual host
* A list of subnets in CIDR format (e.g. 192.168.1.0/24) to scan the entire organization
* A list of Active Directory domain controllers and/or vCenter servers
* Access through any network or local firewalls to endpoints.  At minimum, we need access to:
	+ Windows endpoints, via:
		- TCP 135, 1025-5000 and 49152-65535 (wmi)
		- TCP 445 (smb - remote procedure calls)
		- TCP 1025 (alternate netbios)
		- TCP 139 (netbios)
		- UDP 137 (netbios)
		- TCP 389 (ldap)
	+ Relevant Apple Macs, Linux, Solaris and UNIX endpoints over SSH (TCP port 22)
	+ Relevant VMware endpoints over HTTPS (TCP port 443)
	+ Relevant SNMP endpoints over UDP Ports 161 and 162
	+ TCP port 1521 (Oracle DB Connection; where applicable)
	+ TCP port 465 (SSL-encrypted email)
	+ HTTP 80 (external data feeds)
	+ Outbound internet access over TCP port 443 (HTTPS) for:
		- Receiving updates and patches
		- Data transmission to our cloud-based analytics platform
* **Windows** credentials (a ‘service account’) that has any two of the following 3 levels of access will accomplish inventory:
	+ Access to C$ (SMB)
	+ The ability to run NET RPC / Remote Registry
	+ Remote (read-only) WMI
	+ **A local and/or domain administrator account will have these privileges by default** and while administrator credentials are not required, they may prove a quick path to a successful inventory
	+ These credentials allow for the agentless inventory. They will be keyed in by a local resource at your organization
* **vCenter** SSO domain credentials
* **Mac, Linux, Solaris or UNIX** credentials (if applicable)
* **SNMP** community strings or v3 credentials (if applicable)
* Your **Office 365** global administrator account, for authentication of our application to gather read-only Office 365 data such as your Secure Score, Usage and Activation data (if applicable)

## **Appliance deployed in a virtual environment**

To obtain the discovery appliance for deployment on a VMWare ESXi / Microsoft Hyper-V / Nutanix host:

*System Requirements:*A VMware host running ESXi 5.0 or newer, Microsoft Hyper-V 2008 or newer, any Nutanix Hypervisor

*Network Requirements:*A network segment with access to the enterprise's assets and a static IP address

**VMware:**

1. Download a Virtualization Template (OVF) [here](http://download.block64.com/BlockBox_ESX.zip).

2. Provision the OVF template on the appropriate host in your environment.

3. Startup the appliance and, via the vSphere thick client or web client, open a remote console and follow the prompts.

**Microsoft Hyper-V:**

1. Download the virtual hard drive file [here](http://download.block64.com/BlockBox_VHD.zip) and extract it.
2. Create Hyper-V virtual machine in your environment with:
* Minimum: 2 vcpu and 4 GB memory (small environments, 100-1000 AD devices)
* Recommended: 4 vcpu and 8 GB memory (medium and large environments, 1000-10000 Active Directory devices)
1. Attach the extracted virtual disk to the newly created virtual machine
2. Start the BlockBox appliance

**Nutanix:**

1. Download the archive [here](https://download.block64.com/BlockBox_VHD.zip) and extract virtual disk **BlockBox-disk1.vmdk**
2. Create Nutanix virtual machine in your environment with:
* Minimum: 2 vcpu and 4 GB memory (small environments, 100-1000 AD devices)
* Recommended: 4 vcpu and 8 GB memory (medium and large environments, 1000-10000 Active Directory devices)
1. Attach the extracted virtual disk to the newly created virtual machine
2. Start the BlockBox appliance

# **Appendix: FAQ: Regarding Access Levels & Network Impact**

**Local Administrator privileges**

* *Why do we need this?*
	+ Our inventory work leverages three Windows services: SMB, WMI and RPC.  The most time-effective way to ensure we can communicate using those services is to use a service account with local administrator privileges. If this is a concern, we can also instruct you in enabling access to these services for a specific service account.

**Domain Administrator privileges**

* *Why do we need this?*
	+ Many servers do not have local administrator accounts – for example, PDC and BDC servers. In those cases, we leverage this privilege level to conduct any inventory activities that would otherwise have leverage local admin privileges / the administrative share. However, as above, an account with Remote Registry and read-only remote WMI can successfully complete an inventory. Domain Administrative privileges are a nice to have but not a must have.

**VMware Access**

* *What access do we need?*
	+ We need an account on your vCenter server that has read-only access to the complete vSphere environment, including license manager.
	+ This account is typically an account created in a vSphere SSO domain – this can be an SSO domain administrator or a new service account created for the purpose of inventory.
* *Why do you need this data?*
	+ Microsoft and Oracle products, in particular, base their licensing in many cases on the architecture of the host upon which a guest VM is running. To properly offer licensing advice and ensure a customer is not exposed to compliance risk or overpaying for this software, we must understand the details of the guest/host relationship and the hardware specifications of the host servers.
* *Do you need root access to our ESXi hosts?*
	+ Absolutely not. The vCenter SSO account should provide sufficient data regarding your virtual environment.

**Nutanix Access**

* *What access do we need?*
	+ We need an account that has a viewer role (read-only access to your Nutanix environment).

**Network Impact**

* *What will the impact to my network be?*
	+ We leverage standard protocols (NetRPC, SMBv2 & v3, etc) that should not cause any alert conditions in a standard environment
	+ The amount of bandwidth our solution consumes is configurable at the appliance level, or even via your virtualization technology itself.
		- In its default settings, our appliance will typically run at 150 – 250KBp/s, comparable in bandwidth to streaming a standard definition video on YouTube.
		- In its maximum settings, our appliance will typically run at up to 1000 KBp/s, comparable in bandwidth to streaming a high definition video on YouTube.