BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Scrutiny™

ASSET AND FLOW VISIBILITY

Datasheet

Corporate IT security tools are not designed for industrial and critical infrastructure networks when specialized capabilities are needed to keep plant environments safe and cybersecure. Scrutiny™ is Bayshore's OT asset discovery and flow visualization tool.

Most OT network operators or engineering teams find value when they are able to gain insights into what equipment and protocols are in use in their process controls networks, and what is talking to what. After Scrutiny examines even a few minutes of plant traffic, most OT teams are surprised at what they may find. Real-world use cases include:

- **Equipment they thought was decommissioned is still communicating**
- **Large scale scans occurring in regular intervals from systems they didn't know were performing that function, consuming bandwidth and slowing things down**
- **Protocols or ports and services in use in segments of the network that shouldn't have been able to reach those segments or endpoints within it**
- **Manual inventories of equipment that doesn't align with what the network traffic reveals**

Who can use Scrutiny?

OT teams who want to understand more about the assets and communications going on within their production networks can use Scrutiny.

Corporate IT teams may wish to also use it to begin to understand their OT plant environment and the specialty needs and equipment that exist.

Scrutiny Key Features & Benefits

- *Free, licensed software downloaded from Bayshore Networks. Free is good.*
- *Installs as a Windows application on engineering desktops or laptops.*
- *Scrutiny captures OT traffic (PCAPs) in small batches for analysis which can reveal assets, protocol traffic, and communication flows between systems. See Supported Protocols list.*
- *Supports native traffic from industrial equipment manufacturers such as Siemens, Schneider, Allen Bradley, Rockwell, and other hardware vendors.*
- *HTML Reports can be separately exported to CSV for comparison, trending, and tracking.*
- *Manuals and Readme documents provided with each release.*

Designed for OT networks

Scrutiny can take a snapshot or packet capture (PCAP) of OT traffic, analyze it, and produce a report that will identify devices by OS, IP address, MAC address and vendor, country, and public DNS if available. It understands an array of industrial and IT protocols and can identify what equipment, protocols and ports are in use and who is talking to whom.

Easy Deployment

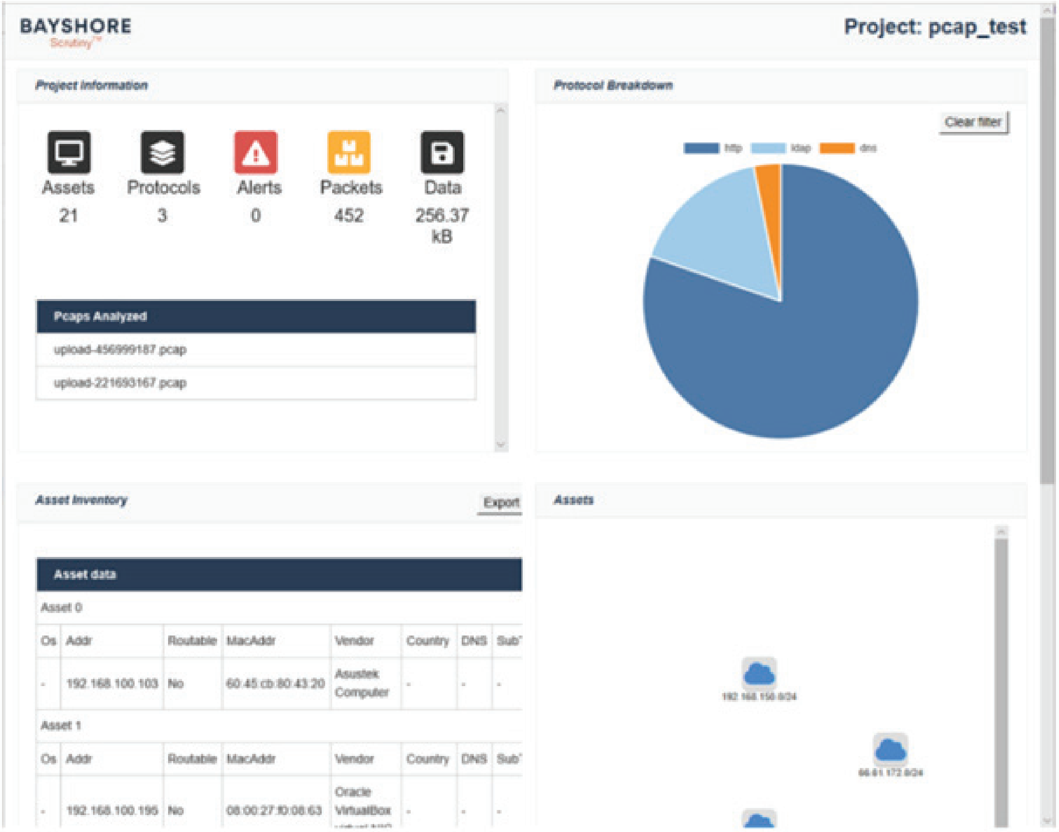
Scrutiny is available by licensed software download at no cost. It is a Windows-based application that can run on a personal desktop or laptop. It collects data from the local network interface, or a span/mirror port from a switch. It can process PCAPs offline or from live traffic.

Asset Inventory and Visual Topology

An OT network operator can build a record of all devices seen in their network at a snapshot in time, organized by ports, services and protocols in use as well as what source/destination pairs are active.
With the data available, Scrutiny can also report on network topologies.

Proactive

Scrutiny gives plant personnel the tool they need to proactively examine their own plant traffic and take action on what is shown. There may be unexpected assets, external IPs in play, and systems talking to systems they shouldn't be. These gaps could potentially impact production if not caught early and appropriate action taken.



Pcaps Analyzed

- upload-456999187.pcap
- upload-221693167.pcap

Asset data

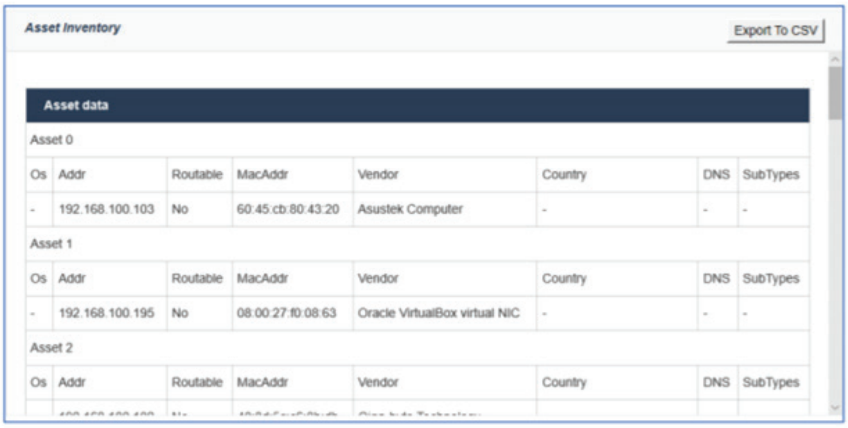
Asset 0

Os	Addr	Routable	MacAddr	Vendor	Country	DNS	Sub
-	192.168.100.103	No	60:45:cb:80:43:20	Asustek Computer	-	-	-

Asset 1

Os	Addr	Routable	MacAddr	Vendor	Country	DNS	Sub
-	192.168.100.195	No	08:00:27:f0:08:63	Oracle VirtualBox	-	-	-

Asset Inventory



Asset data

Asset 0

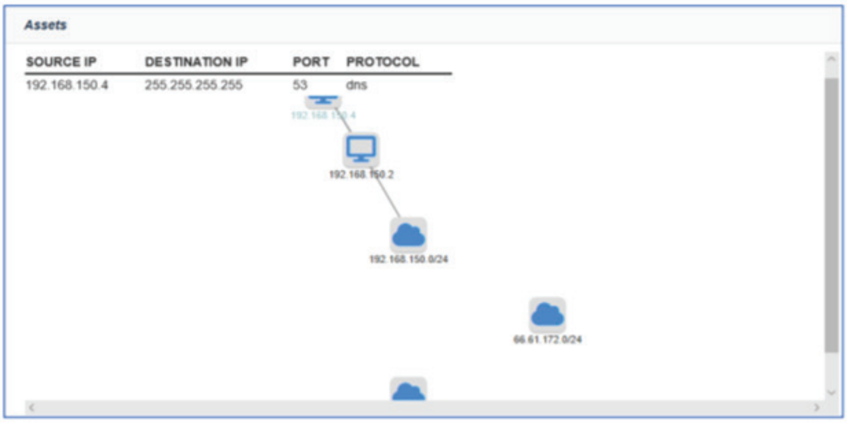
Os	Addr	Routable	MacAddr	Vendor	Country	DNS	SubTypes
-	192.168.100.103	No	60:45:cb:80:43:20	Asustek Computer	-	-	-

Asset 1

Os	Addr	Routable	MacAddr	Vendor	Country	DNS	SubTypes
-	192.168.100.195	No	08:00:27:f0:08:63	Oracle VirtualBox virtual NIC	-	-	-

Asset 2

Os	Addr	Routable	MacAddr	Vendor	Country	DNS	SubTypes



SOURCE IP	DESTINATION IP	PORT	PROTOCOL
192.168.150.4	255.255.255.255	53	dns

Hardware Minimums

- Windows 8 64-bit or newer
- Any modern CPU, desktop or laptop
- At least 8GB of RAM recommended
- Storage for potentially large PCAP files!

Supported Protocols

The supported protocols for Scrutiny are always evolving. This is what is available as of current release, and will change each subsequent release.

TCP Protocols
BGP
DNP3
DNS
EtherNet/IP
FINS
FTP
HTTP
HTTPS
iFIX
LDAP
LDAPS
Modbus TCP
OPC_UA_CONNECTION_PROTOCOL
OPC_UA_DISCOVERY_SERVER
OSIsoft_PI_SERVER
RADIUS
RADIUS-ACCT
S7comm
SSH
SMTP
SNMPTRAP
SRTP
TACACS
Telnet

UDP Protocols
BACNET_IP
DNP3
DNS
EGD CS (Command Service)
EGD RT (Real Time)
ETHERCAT
EtherNet/IP
FINS
NTP
OPC_UA_MULTICAST_DATAGRAM_PROTOCOL
RADIUS
RADIUS-ACCT
SNMP
SNMPTRAP
SYSLOG
TACACS
TFTP
-
-
-
-
-
-
-

For more information
Email info@bayshorenetworks.com.

BAYSHORE NETWORKS