**LIVE ASSET VISIBILITY**

**Visualize Alerts and Hunt Threats in Realtime Within the Context of your OT/IT Infrastructure**

- Live network map of Cisco, Juniper, endhost, server, mobile, and IoT devices
- Live alert visualization with network context
- Operational Technology (OT), Building Automation Systems (BAS), and Industrial Control Systems (ICS) asset discovery and mapping (with NICOS)
- Automatically generates Layer-2 and Layer-3 links using ARP, MAC tables, CDP, IP/Subnets, and DHCP (with NICOS)
- View integrated map of IT and OT assets
- Displays managed and unmanaged devices
- Displays Wi-Fi connected devices, including support for Meraki API
- Collects endpoint and router metadata, including running services and processes, netstats, users, configuration files, and more
- Provides on-demand device metadata collection
- Point-and-click down selection and filtering
- Quickly search device metadata, including services, processes, users, OS versions, etc.
- View up/down status for managed devices
- Detailed VLAN and subnet visibility, including endhost to VLAN mapping
- 3rd party product integration, including SIEM, anti-malware, and traffic analysis

---

**MULTI-POINT THREAT DETECTION**

**Identify Threats in Realtime Using SNAP Patented Detection Technology**

- Immediate lateral spread detection
- Immediate remote privileged activity detection
- Immediate network enumeration detection
- Immediate malware event detection (with anti-malware integration)
- Immediate process hash and process tree visibility during an alert
- Immediate removable storage detection
- Immediate syslog-based threat alerting with automated context enrichment
- Continuous and custom monitoring of Windows process and service threat indicators
- Automated alert correlation and enrichment, including affected devices’ users, VLANs, hostnames, OS versions, and more
- Customizable suppression rules reduce threat event operator/analyst overload
- Realtime SMS and email threat notifications
- Integrates, consolidates, and enriches alerts from numerous 3rd party security applications, including Sophos, Cisco AMP, Meraki, and more

---

**INCLUDED FEATURES**

- Live Asset Visibility
- Multi-Point Threat Detection
- Realtime Threat Response
- Privileged User Visibility
- Multi-Tenant for MSSPs
- Risk and Compliance Reporting
- Simplified Deployment and Management

**OPTIONAL ADD-ON**

OT/BAS/ICS Asset Visibility, Monitoring, and Protection with NICOS Module
REALTIME THREAT RESPONSE
Stop Threats in Realtime with Built-in, Immediate, and Effective Response
- Point-and-click response to detain compromised devices
- Easily understandable alerts enable rapid triage by Tier 1 analysts with detailed data for Tier 3 analysts
- Custom detainment notification message to device users
- Immediate notifications of un-detained devices
- Preserves compromised device state for follow-up forensics and threat analysis
- 3rd party response orchestration

PRIVILEGED USER VISIBILITY
Gain Unparalleled Live Insight into Privileged User Activity and Behavior
- Identify privileged user accounts
- View privileged user activity, including network shares, remote desktop, remote execution, and more
- Detect low-frequency privileged activity
- Automatically reports new, previously unseen privileged users and activity
- Immediately identify privileged insider threat

MULTI-TENANT FOR MSSPS
Manage Multiple Client Networks with a Single Installation and User Interface
- Consolidated alert and system status dashboard
- On-Prem, hybrid on-prem, or Blackpoint cloud provided hosting
- Monthly billing
- Rapid deployment to quickly add new clients
- Sales and marketing support
- Ideal for Hunt as a Service, Compliance as a Service, Incident Response, Continuous Monitoring, Network Security Assessments, and more

RISK AND COMPLIANCE REPORTING
Identify Security Risks and Ensure Continuous Compliance
- Quickly generate real-time and historical reports
SUMMARY REPORT:
- Outstanding alerts by criticality, type, and time
- Overall system health and status
- Suppressed events by type and time
COMPLIANCE REPORT:
- PCI-DSS
- HIPAA
- NIST 800-171
- NYCRR-500
- Sarbanes-Oxley (FY19)
- CJIS (FY19)
- CIP-NERC (FY19)
PRIVILEGED ACTIVITY REPORT:
- New/most/least active privileged users
- New/all remote executions
- Remote executions by user and application
- New/all RDP activity
- RDP activity by user, source, and destination
- New/all privileged share activity
SECURITY EVENTS REPORT:
- Anti-malware events by severity, type, and time
- Process and service threats by severity, type, and device
- New attack sources and targeted devices
- New point-to-point connections
- New/all USB activity
- USB activity by device
- New/all malware persistence techniques
NETWORK REPORT:
- Detected enumeration activity
- Enumeration activity by source, destination, and time
- Core network change detection
- SNMP community strings
- Insecure core network passwords
- Network Management devices, including TACACS, SNMP, NETFLOW, SYSLOG, NTP, and RADIUS
**SIMPLIFIED DEPLOYMENT AND MANAGEMENT**

**Easily Setup, Run, and Manage SNAP**
- On-prem, hybrid on-prem, or Blackpoint cloud hosted installations
- Point-and-click automated endpoint deployment
- Real-time system status, including SMS and email notifications
- Robust role-based permission and user management
- Two-factor login authentication
- Point-and-click upgrades

**NETWORKED INDUSTRIAL CONTROL OPERATIONS SECURITY (NICOS) MODULE**

Secure OT/BAS/ICS networks with live-monitoring, visualization, and actionable alerts
- Live OT/BAS/ICS asset mapping and visualization
- Live and customizable auditing and visibility of remote privileged OT/ICS/BAS asset access, including SSH, RDP, VNC, TeamViewer, and more
- Detect known bad traffic and unusual domains
- Detect obfuscated/anonymous traffic (TOR) and port scans
- Protect bi-directional lateral spread between OT and IT networks

<table>
<thead>
<tr>
<th>Optional Add-On</th>
<th>Included in Price</th>
<th>Extra Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live Asset Visibility</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Multi-Point Realtime Threat Detection</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Realtime Threat Response</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Risk and Compliance Reporting</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Privileged User Visibility</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Multi-Tenant for MSSPs</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Simplified Deployment and Management</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>OT/BAS/ICS Asset Visibility, Monitoring and Protection with NICOS Module</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>