​​Dabble Blueshift

A screen shot of a computer

Description automatically generated

## SECURITY + VISIBILITY

## *Blueshift, your single source for security visibility and performance monitoring*

Dabble Blueshift, a visibility platform providing detailed insight into network security and performance. Blueshift leverages leading edge data analysis, threat detection and classification techniques to identify users, issues, trends and security threats across the enterprise.

Information security issues are on the rise, yet many organisations still have limited or no visibility of traffic across the network. Blueshift couples the discipline of intrusion and threat detection with traditional performance management to provide a whole of network security and visibility solution.

Blueshift cuts through much of the technical jargon to present information about the ‘who‘, ‘what‘ and ‘where‘ of network data flows. Unlike many pure performance monitoring offerings, information is collected from a variety of data sources to build an enriched data set for reporting.

Deployed as an appliance or virtual machine, Blueshift’s distributed architecture scales meets the security and visibility requirements of organisations scaling from small companies right through to large enterprise.

## At a Glance

|  |  |
| --- | --- |
| * Threat Detection * Real time performance monitoring * Location Analysis * Packet Capture * Capacity Planning * Event and alerting * Deep packet inspection | * Context sensitive dashboards * Built in reports, volume, applications, protocols, top talkers, web sites, operating systems geo-IP and more… * NetFlow collection * Compatible with standard web browsers * Subnet Analysis |

## Threat Detection

The Blueshift Threat Detection Module is a passive system that brings real time visibility into potential network compromise. The Threat Detection dashboard provides real time and historical view of identified threats with the ability to quickly drill down to specific timeframes or individual threats with a few simple clicks.

## A screenshot of a video game Description automatically generated

The Blueshift Threat Detection module is a signature-based intrusion detection system that monitors incoming and outgoing network traffic for malicious activity and security policy violations. The Blueshift Threat Detection module acts as an intruder alarm, triggering an event if there is indication of activity that could lead to network or data compromise. It does this by inspecting the packets that flow across the network in order to detect known indicators of compromise and traffic patterns that suggest suspicious activity.

Security and threat signatures are updated daily to ensure protection against the latest emerging and zero day attacks identified in the wild. The Blueshift Threat Detection module is an essential part of ensuring network security and integrity.

## Performance Monitoring and Reporting

Data collection, user centric monitoring, data enrichment and deep packet inspection are all critical elements in providing security and visibility solutions but are meaningless without clear and concise information presentation. Blueshift is built with an easy to use intuitive web-based interface that allows seamless access to performance and security information to assess the health of the network.

A series of views provide the ability to take a high-level view of overall performance with the ability to drill down to granular information right down to individual network flows in just a few clicks. The graphs are context sensitive or ‘clickable’ to quickly identify areas of interest. For example, if Facebook traffic is of interest, simply click on the Facebook slice of the application pie chart to quickly and easily identify associated information such as top talkers, conversations utilisation.

There are a number of other views that present visibility information graphically or schedule reports for IP accounting.  Put simply, Blueshift is a complete visibility window to the network.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Blueshift Dashboard View**  The interactive Blueshift dashboard allows quick drill downs from high level enterprise wide data through to isolating individual applications flows in just a few clicks. Dashboard charts are all context sensitive to facilitate complex filters quickly and easily. | | | A screenshot of a cell phone  Description automatically generated | |
| A picture containing black, road, monitor  Description automatically generated | | **Blueshift Summary View**  Network traffic can be configured to be displayed by subnet, site or groups of sites to display a quick summary of overall usage. The summary view provides a snapshot of performance across the entire enterprise quickly highlighting sites that may be experiencing performance issues.  More details can be accessed by clicking on the various links on the summary page to identify site or group specific information | | |
| **Blueshift Topology View**  The topology view provides a more graphical view of the network.  Network traffic flows can be represented via the topology view to identify the movement of application traffic across the network.  Similar to the summary view, more information is available by clicking on the various nodes in the topology view to display more detailed information. | A screen shot of a computer  Description automatically generated | | | |
| A screenshot of a video game  Description automatically generated | | | | **Blueshift Capacity View**  The ability to schedule reports to display long term capacity data is essential to identify long term trends or IP accounting.  The Blueshift Capacity view allows for long term historical reports to be generated ad hoc or scheduled daily, weekly or monthly runs.  Capacity reports are available via the web interface or downloaded as CSV files. |

## Application Classification

Blueshift uses a combination of techniques including deep packet inspection and certificate inspection to achieve comprehensive application classification for both encrypted and non-encrypted traffic.

Application information is presented via the Blueshift context sensitive dashboard allowing fast drill downs to identify application usage for the entire network, specific subnets or even individual users and hosts.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Address Type**  Identify the address or packet type of traffic traversing the network – unicast, multicast or broadcast. Packet type monitoring provides an effective indicator of potential security issues across the enterprise. | **IP Type**  Displaying the underlying IP protocol used such as TCP, UDP, ICMP and so on. Ongoing collection of IP type assists in traffic profiling to help define network normal. | **TCP/UDP Service**  Layer 4 TCP /UDP service and port information allowing for identification of strange activity and potentially malicious traffic. |
|  |  |  |
| **Application Type**  Application type is a detailed analysis of actual applications traversing the network. Application type is available for both encrypted and non-encrypted traffic. | **Top Websites**  Top website monitoring goes beyond normal network monitoring to identify where users travel across the Internet. Comprehensive website visibility is critical for monitoring of cloud based applications | **Operating System Distribution**  Identification of operating systems has become increasingly important in BYOD environments. OS distribution provides clear and concise indication of strange devices that may connect to the network. |

Complete stack visibility is provided from IP protocol type right through to high level application statistics. Blueshift application classification identifies hundreds of applications as well as allowing for custom application definitions.

Blueshift application visibility provides quick and comprehensive real-time and historical snapshots of user experience – what they are doing, where they are going and how fast they are doing it.

Blueshift, a simple turn-key solution to satisfy all your network performance and capacity planning requirements.

## Location and Subnet Analysis

Location analysis of where users go on the Internet and more important where traffic originated from is an important metric for assessing potentially malicious traffic entering the environment. The geolocation of the origin and destination of each Internet based flow and threat is collected to provide a detailed picture of the location of Internet based traffic.

|  |  |
| --- | --- |
| A screenshot of a computer screen  Description automatically generated | A screenshot of a computer screen  Description automatically generated |

IN addition to geo location information, Individual hosts can be queried to provide more ‘whois’ information to identify the actual source of traffic including domain owner, country, state, city and carrier information.

## Packet Capture

Blueshift includes a web based packet capture interface allowing for full packet capture on the remote appliance. The packet capture module is a ‘Wireshark’ style interface with full packet decodes, detail and filtering available in real time directly from the web interface.

The packet capture module supplements other security and performance monitoring for more detailed analysis of network traffic if required. As a web based interface, it also allows for packet captures to be taken at remote sites without the requirement of sending a network engineer with a traditional packet sniffer.

Packet captures are stores in standard PCAP format and are available for download for further analysis if required.

## A screenshot of a computer Description automatically generated

## Deployment

Blueshift deployment can be as simple as a single appliance to monitor the entire network right through to a distributed deployment monitoring hundreds of subnets and thousands of devices.

Blueshift Appliances are available in a number of different interface configurations including standard Gigabit Ethernet and 10 Gigabit Ethernet. Each support a range of different fibre and copper modules to ensure full compatibility to the existing Ixia distribution switches.

A picture containing indoor, monitor, wall, electronics

Description automatically generated

The Blueshift appliance requires minimal configuration and can ordinarily be installed within a few minutes. There is no scripting or complex command line interface required to install and configure the solution.

In addition to the appliance model, Blueshift is available as a virtual machine allowing for rapid deployment into a virtual environment. Similarly, the Blueshift data repository can also be stored on a cloud-based server for a full cloud-based implementation.

## Specifications and System Requirements

|  |  |  |
| --- | --- | --- |
|  | Blueshift 1G | Blueshift 10G |
| 1G RJ45 Ethernet Monitoring Ports | 6 | 8 |
| 1G SFP Port Monitoring Port | 2 | 0 |
| 10G SFP+ Monitoring Port | 0 | 4 |
| Disk Storage | 1TB | |
| Power | AC 110V – 220V | |

|  |  |
| --- | --- |
| **Certifications**  Safety: UL, CE  EMC: FCC, VCCI, C-Tick  Environmental: RoHS, WEEE  Protocol: Fully IEEE 802.3 Compliant | **Operating**  Operating Temperature: 0°C to 45°C  Storage Temperature: -20°C to 70°C  Relative Humidity: 5% min, 95% max, non condensing  Vibration: 0.5g rms/5-500Hz/random/operating |