BLUECAT

Connector for IBM QRadar

Accelerate threat detection and response with real-time network intelligence

The Connector for IBM QRadar allows organizations to pinpoint attacks and threats by providing detailed information about every device on the network. With BlueCat DNS and DHCP data, delivered in QRadar native data interchange format, security teams can identify and respond to external DNS attacks, malware outbreaks and botnet-infected devices. QRadar customers can also watch for developing patterns that could indicate a malicious agent is preparing for an attack. BlueCat network and device data offers an additional layer of network security intelligence with no blind spots or gaps in compliance or control.

Access Normalized Network Data from IBM QRadar Dashboards

The Connector for IBM QRadar sends real-time network data through the native data interchange format in QRadar so that it can be correlated with other security-related data points to provide more detail and faster threat response. This native format accelerates analytics and causes significantly less resource utilization than a basic syslog stream, providing customers with faster security response and lower costs.

Ensure a Risk-Free BYOD (Bring Your Own Device) Strategy

BlueCat provides QRadar customers with visibility into all device connections including the personal laptops, smartphones and tablets used by employees, contractors and guests. QRadar customers can perform analysis and quarantine devices that are infected, non-compliant or represent a security breach.

Detect and Contain Malware

This connector provides QRadar users with greater visibility into all device activity on the network, accelerating the detection of malware threats and "rogue devices." Time-stamped DNS query information, along with the origin of the request, is sent directly to QRadar, allowing security teams to identify requests that do not match typical flow patterns, such as an increasing number of DNS lookups to an unusual zone or machine. Infected devices can be quarantined to contain the spread of the outbreak.

Improve Forensic Analysis

BlueCat and IBM QRadar allows security teams to map traffic or application access to a specific user/device combination, enabling security teams to quickly determine the first combination that either queried a bad zone, or became infected with malware. QRadar analysts can also use historical DNS events to perform analysis to identify advanced threats.

Reduce Compliance Costs

The Connector for IBM QRadar provides real-time DNS and DHCP data to better highlight offences and create reports to demonstrate compliance. This information can be retained for a corporate-defined period, allowing security teams to perform security and compliance analysis simply by running reports at regular intervals.

Blacklist "Bad" Domain Names

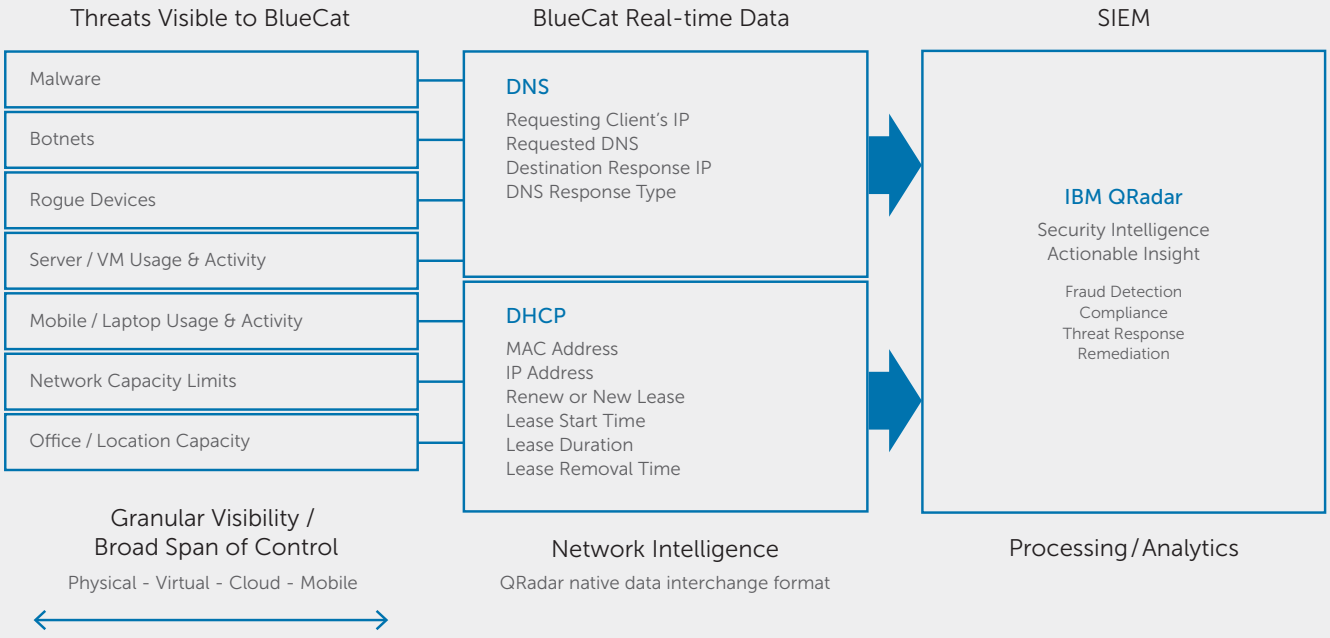
Block unauthorized application access at the DNS level to prevent any network connection from occurring and stop malicious agents from positively establishing "proof of existence" or target points for future attacks. Any query made to a "bad domain" is blocked directly by the DNS caching server and the user's request can be either silently dropped or redirected to a notification web page that indicates a bad site was requested.

BlueCat Network Intelligence

In evaluating security, context is the key to decision-making. The BlueCat IPAM platform provides an authoritative source for information about the network including the connection between devices, IP addresses and their activity on the network. This information is essential to monitor which applications are being accessed, by whom, and how sensitive business data is being used.

BlueCat Network Intelligence extends across wired and wireless networks, virtual environments and mobile end points, and encompasses DHCP scopes, IP address utilization, DNS host records, zones, subzones and devices. The Connector for IBM QRadar enables these key data points to be interconnected and correlated within QRadar to provide a complete view of the security posture of all connected devices.

BlueCat Enriches Security Intelligence and Accelerates Threat Response



BlueCat Security Highlights

Security

Safeguard DNS and DHCP core services against exploits and attacks with hardened servers

- Hardened Linux Kernel
- DNS Blacklisting
- Secure DNS (DNSSEC) Management
- Optional FIPS 140-2 Level 3 Certified HSM-based Key Security
- DHCP MAC Filtering
- Certificate-Based Security
- Regular Software Updates to Address CERT Vulnerabilities

Remediation

Drive the remediation of threats detected by QRadar straight through to a network level response

- Track All Devices Associated with a User
- Control User Access Privileges (e.g. restrict users to pre-determined subnets)
- Remove All Devices Associated with a User
- Blacklist Malicious Users
- Quarantine Malware or Botnet-Infected Devices
- Block Inappropriate Sites

Compliance

Reduce the costs of reaching network data to demonstrate compliance

- Live and Historical Activity Monitoring
- Tie Connected Devices Back to Specific Users and IP Addresses
- Audit and Track Which Users are Accessing Which Resources
- Identify Non-Compliant or "Rogue" Devices
- Reduce False Positives and False Negatives

BLUECAT

www.bluecatnetworks.com