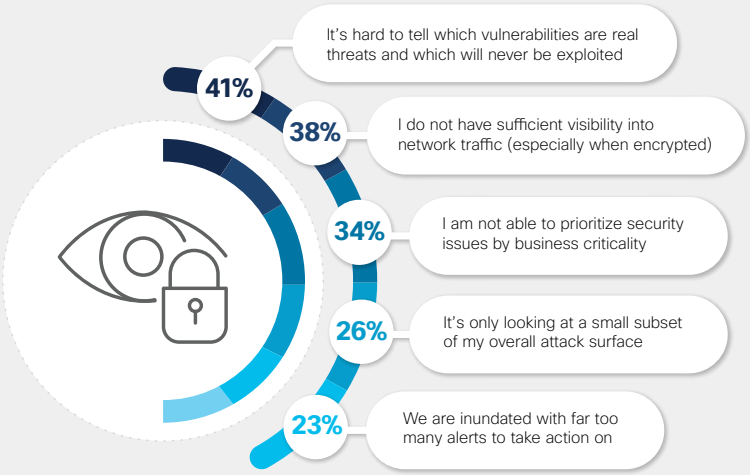
Cybersecurity INSIDERS RECOMMENDED

PRODUCT REVIEW: BLUECAT INFRASTRUCTURE ASSURANCE

BLUECAT™

Proactively find problems to avoid outages for DDI, firewalls and load balancers.

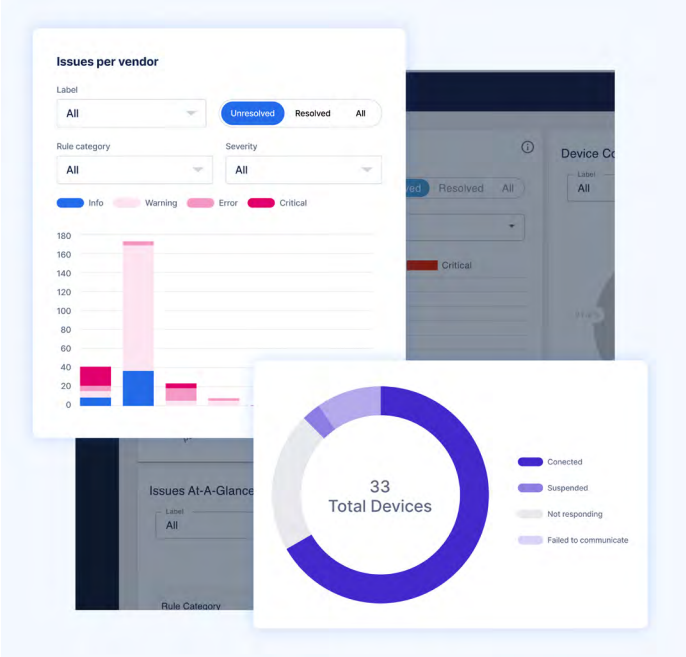
Network teams are increasingly overwhelmed as the complexity of multi-vendor environments—spanning DDI, firewalls, and load balancers—makes troubleshooting more difficult. Traditional SNMP-based tools only offer limited, retrospective insights, resulting in reactive management and excessive manual work. With the rising costs of downtime, security breaches, and compliance failures, ensuring continuous network performance and security is more critical than ever.



Which of the following concerns do you have about your current security visibility?

Limited visibility into security threats is a critical issue for cybersecurity teams, as it hampers the ability to protect systems, identities, applications and workloads.

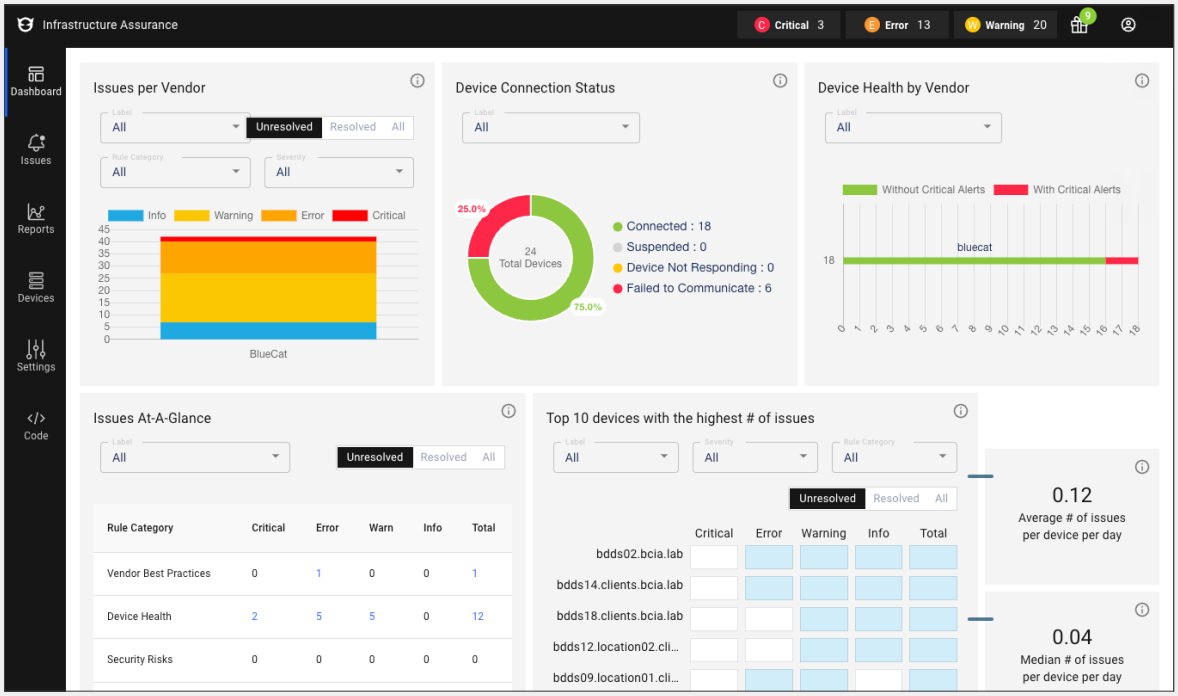
Source: 2022 Security Visibility Report produced by Cybersecurity Insiders



BlueCat Infrastructure Assurance is a proactive solution designed to prevent network disruptions through automation and deep observability of critical network and security infrastructure components like DDI, firewalls, and load balancers.

By continuously analyzing these systems, Infrastructure Assurance identifies potential risks, performance issues, and configuration errors before they escalate.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved



BlueCat Infrastructure Assurance dashboard

THE PROCESS IS STRUCTURED INTO THREE KEY STAGES

1 | Continuous Measurement:

Infrastructure metrics, security, performance, and configuration data are continuously measured and cross-referenced with benchmarks and internal standards. This stage ensures that any deviations from expected norms are detected early.

2 | Auto-Triage and Root-Level Diagnosis:

When issues like misconfigurations, vulnerabilities, or downtime are detected, the system automatically performs a root cause analysis with contextual awareness, providing a comprehensive understanding of the problem.

3 | Automated Remediation Recommendations:

Leveraging a global expert knowledge base, Infrastructure Assurance offers precise remediation steps and certified automation elements, enabling rapid resolution of issues without extensive manual intervention. This approach streamlines network management and minimizes the risk of disruptions.

PROACTIVE NETWORK PROBLEM MANAGEMENT

The platform proactively automates the detection and root cause of network problems before they lead to outages, making the management of complex network environments more efficient. It offers network teams actionable insights and remediation steps, shifting their approach from reactive to proactive. This helps maintain uptime and compliance while reducing the manual workload.

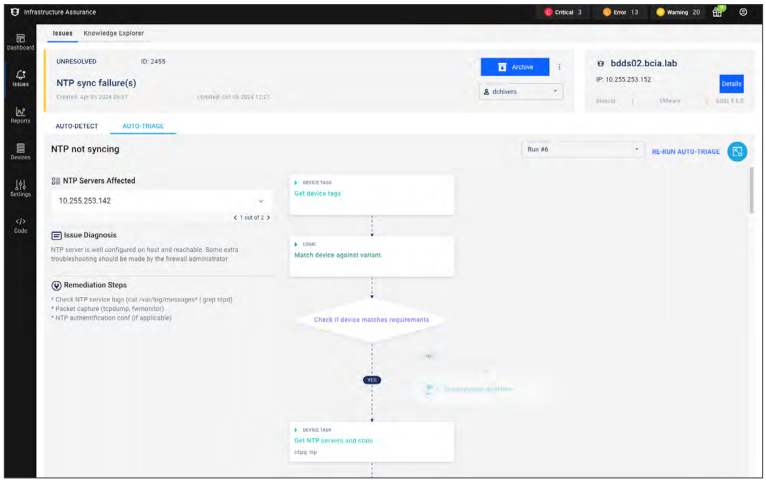
Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

ADDRESSING NETWORK COMPLEXITIES AND SKILLS GAP

Infrastructure Assurance addresses the increasing complexities within network systems and the challenges of troubleshooting across different technology stacks. It aims to overcome the shortcomings of traditional monitoring tools, which often provide insights only after issues have occurred. By automating the inspection and triage of network devices, the solution reduces the reliance on manual work, helping to fill the cybersecurity skills gap with smarter, more efficient tools. This approach not only keeps networks secure but also ensures they are managed proactively, aligning with modern network security needs.

ADVANCED OBSERVABILITY AND AUTOMATED REMEDIATION

Infrastructure Assurance provides advanced observability, troubleshooting, and recommended remediation for network components such as DDI systems, firewalls, and load balancers. It automates the identification of network issues through a three-stage process. This process employs SSH, REST API, and SNMP protocols to execute collection scripts on devices, utilizing CLI commands, SNMP polling, and vendor-specific APIs for comprehensive network management.



Auto-triage Border Gateway Protocol peer problem

INFRASTRUCTURE ASSURANCE FOR FIREWALLS

Infrastructure Assurance for firewalls is a comprehensive cybersecurity solution designed to ensure seamless service connectivity (e.g., with Syslog, NTP, DNS, and identity servers). This platform detect security risks, ensure compliance and facilitates maintenance through backups for optimal firewall performance.

It also introduces sophisticated troubleshooting and stateful health checks, assessing device configurations against expected standards to identify discrepancies such as enabled debug modes, next-hop inaccessibility, and misconfigured authentication profiles.

Additionally, it ensures high availability by addressing cross-device inconsistencies like unsynchronized cluster configurations, thereby safeguarding against potential availability risks. Through these measures, Bluecat's offering streamlines operational efficiency, reinforces security posture, and maintains high availability, exemplifying a strategic approach to firewall infrastructure management in complex security landscapes.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

ADVANTAGES OF INFRASTRUCTURE ASSURANCE

Infrastructure Assurance surpasses network monitoring tools in four critical ways, setting a new benchmark in network and security infrastructure management.

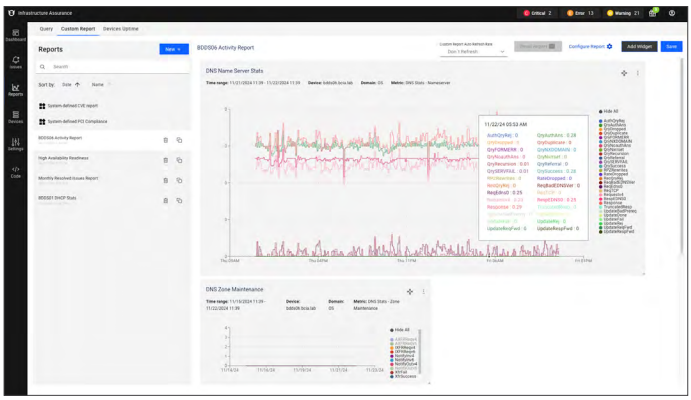
1 | Community-Driven Automation Intelligence: Firstly, its automation components are enriched by a broad community of experts, including contributions from certified security practicioners and Fortune 1,000 companies. This collective intelligence approach harnesses a diverse pool of device knowledge and experience, offering solutions that individual entities alone might not provide.

2 | Proactive Issue Detection and Alerts: Secondly, the deployment of Infrastructure Assurance in security settings harnesses machine learning models to detect early symptoms of potential issues, enabling proactive problem prevention. The system immediately alerts users to a wide range of concerns, including misconfigurations, runtime errors, vulnerabilities, and non-compliance. By analyzing patterns and anomalies, it identifies risks before they escalate, offering a level of foresight that many traditional monitoring tools, which rely on generic, reactive protocols, simply do not provide.

3 | Automated Troubleshooting and Root Cause Analysis: Thirdly, after identifying potential issues, Infrastructure Assurance doesn't just stop at sending alerts; it dives deeper into automated troubleshooting to uncover the root causes of these problems. This stands in stark contrast to other solutions that may provide alerts, but leave the burden of diagnosis and resolution on IT teams. By automating the detection and analysis, Infrastructure Assurance not only pinpoints the underlying issues but also aids in preventing their recurrence, thereby minimizing downtime.

4 | Actionable Remediation Steps: Lastly, after diagnosing issues, Infrastructure Assurance distinguishes itself further by offering actionable remediation steps. Unlike other solutions that may provide vague alerts, it delivers specific, expert-backed recommendations for resolving identified problems. This not only speeds up the troubleshooting process but also empowers IT operations teams with knowledge and strategies derived from BlueCat's extensive experience, significantly cutting down on the time and resources spent on network management tasks.

Each of these aspects underscores BlueCat Infrastructure Assurance's unique approach, emphasizing proactive issue identification, expert-driven automation, and efficient resolution mechanisms designed to streamline and secure modern network environments.



BlueCat Infrastructure Assurance time series chart

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

BLUECAT INFRASTRUCTURE ASSURANCE FOR DDI

BlueCat Infrastructure Assurance for DDI ensures the reliability and high availability of DNS, DHCP, and IPAM services through advanced monitoring and proactive management. The platform conducts continuous stateful health checks to identify and rectify issues such as DNS lookup failures and failed DNS query rates, while also preempting connectivity problems caused by firewall policy changes. The solution vigilantly analyzes for cross-device inconsistencies and misconfigurations that threaten service continuity, offering alerts for downed servers or unsynchronized configurations. By verifying server settings against gold-standard frameworks and detecting manual overrides, it prevents configuration drift and aligns network operations with best practices.

This integrated approach ensures that network services are uninterrupted, secure, and fully optimized, making Infrastructure Assurance an essential tool for maintaining robust DDI infrastructure.

KEY BENEFITS OF BLUECAT INFRASTRUCTURE ASSURANCE

Infrastructure Assurance delivers significant advantages to network security teams, enhancing both performance and reliability of security infrastructure through the detection of hidden issues and the automation of remediation tasks. Here are the key benefits:

- **Prevent Network Downtime:** Proactively addresses misconfigurations, high availability inconsistencies, and neglected maintenance to ensure network stability and avoid outages.
- **Optimize Security Infrastructure Performance:** Leverages automation to streamline IT operations, allowing for the efficient delivery of optimal security services.
- **Accelerate Mean Time to Resolution:** Employs automated root cause analysis for faster troubleshooting, significantly reducing the need for human intervention.
- **Enhance Operational Efficiency:** Surfaces actionable insights that improve the effectiveness and productivity of IT operations teams.
- **Automate Routine Checks:** Simplifies essential tasks, such as configuration backups and license SSL certificate expiration, through automation, minimizing errors and saving valuable time.
- **Improve Infrastructure Stability:** Results in a more stable security setup with significantly fewer issues, contributing to overall network resilience.
- **Increase Visibility:** Ensures problems are identified before they impact users, enhancing the overall security posture.
- **Reduce Administrative Tasks:** Reduces escalations and the need for after-hours support, leading to higher satisfaction among engineers.
- **Save Time on Manual Tasks:** Frees up teams to focus on higher-level tasks by automating time-consuming manual processes, maximizing resource allocation.
- **Ensure Regulatory Compliance:** Automates auditing and compliance checks, providing peace of mind that all configurations and operations adhere to regulatory standards, saving significant manual time and reducing the risk of costly non-compliance penalties.

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

DEPLOYMENT AND PRICING

Infrastructure Assurance is delivered as software, designed for flexible deployment by customers either on-premises or within cloud environments. This adaptability extends to Managed Service Providers (MSPs), who utilize the platform to bolster the infrastructure security of their clients, showcasing the platform's versatility across different deployment scenarios.

Deployment Timeframe: The deployment of Infrastructure Assurance is notably swift, with a typical setup completed in less than an hour. This rapid deployment capability underscores the platform's efficiency and its minimal impact on operational workflows, allowing for almost immediate integration into existing security frameworks.

Pricing: Infrastructure Assurance is available under an annual subscription model and is licensed based on the number and type of devices the software is connected to. This approach provides customers with predictable budgeting for their cybersecurity infrastructure needs and ensures continuous access to the latest features and updates without the need for significant upfront investment. The subscription model aligns with the evolving needs of organizations, offering scalability and flexibility to adapt to changing security demands.

CONCLUSION

Infrastructure Assurance excels in streamlining network and security infrastructure management through its automated issue detection and root cause analysis capabilities. This solution proactively identifies and addresses network disruptions before they occur, significantly reducing downtime and manual workloads. Its unique blend of community-driven intelligence and advanced troubleshooting stands out, offering unparalleled efficiency and stability. By prioritizing proactive management and employing expert-driven automation, BlueCat not only enhances operational efficiency but also ensures robust network security and compliance, making it an ideal choice for organizations aiming to fortify their network infrastructure with minimal effort.

ABOUT BLUECAT

BlueCat provides core services and solutions that help our customers, and their teams, deliver change-ready networks. With BlueCat, organizations can build reliable, secure, and agile mission-critical networks that can support network modernization initiatives such as cloud adoption, SD-WAN, SASE and automation of key network provisioning and administration tasks. Learn more at bluecat.com.

www.bluecat.com | info@bluecatnetworks.com | 1-866-895-6931

Copyright © 2024 Cybersecurity Insiders. All Rights Reserved