Solutions | Whitepaper

BLUECAT™

Strengthening Cybersecurity and Compliance

BlueCat Solutions: CIS Controls and DORA

Executive Summary

Cybersecurity challenges continue to escalate as enterprises engage in network modernization initiatives. Concurrently, regulatory requirements, particularly in sensitive industries like finance, demand rigorous compliance measures.

This convergence of challenges necessitates a strategic approach to cybersecurity, one that integrates proven frameworks with regulatory mandates. The widely used Center for Internet Security Critical Security Controls (CIS Controls)—and in particular its latest version, CIS Controls v8, with 18 controls—offers actionable recommendations for organizations of all sizes to prevent cyber attacks.

Meanwhile, the Digital Operational Resilience Act (DORA) strengthens operational resilience for financial entities within the European Union (EU). The act focuses on risk management, incident reporting, resilience testing, third-party risk management, and information sharing.

Integrating the CIS controls framework into DORA helps organizations streamline their cybersecurity processes. It provides a practical methodology for achieving the resilience required by DORA through proven security practices detailed in widely used CIS Controls. When the two are applied in an integrated approach, organizations across multiple industries can reap numerous benefits.

Effective DNS, DHCP, and IP address management—together known as DDI—is also crucial for network security. DDI carries inherent cybersecurity risks. Poor management can lead to conflicts, unauthorized access, and DNS-based attacks. Unified DDI solutions enhance the security posture of your network by providing centralized visibility and control over these critical services.

BlueCat's portfolio of offerings enhances security, ensures continuity, and supports compliance. Integrity provides centralized and automated DDI management for large enterprises. Gateway allows for automating business processes with custom integrations, plugin development, and DDI workflows. Edge offers intelligent DNS forwarding, policy enforcement, and easy DNS resolution across clouds. And Infrastructure Assurance offers deep visibility and automation to uncover and remediate issues found in network devices.

Supported by BlueCat's solutions, integrating CIS Controls and DORA offers organizations a comprehensive approach to managing cybersecurity risks and regulatory compliance.

Table of Contents

Introduction

In the evolving landscape of global cybersecurity, operational resilience and regulatory compliance are paramount. The widely used CIS Controls offer a broad set of security best practices applicable across various sectors and for organizations of all sizes. Meanwhile, new laws such as DORA, which is specific to the financial sector in the EU, are being enacted to strengthen organizations' security and resilience. Both aim to protect critical data and systems but from slightly different perspectives.

Organizations can leverage CIS Controls to meet or exceed DORA's (and other) mandates. By merging the proactive security measures advocated by CIS Controls with DORA's regulatory requirements, organizations can employ a more holistic strategy. Doing so provides the necessary tools and insights to build a resilient cybersecurity infrastructure capable of withstanding modern cyber threats while adhering to regional and global regulations.

Adopting this dual framework helps organizations maintain a healthier security posture. It is a comprehensive approach that is suitable for diverse industries worldwide.

Understanding CIS Controls

CIS Controls are a set of recommended best practices to prevent the most prevalent cyber attacks. Developed by cybersecurity experts at the CIS, these controls provide organizations with a structured approach to securing their IT systems and data.

The latest version, CIS Controls v8, was released in 2021 and reduced the number of controls from 20 to 18. Version 8 recognizes that discrete or physical boundaries are less important, giving credence to the idea that edge security is a trend worthy of attention.

These revised CIS Controls also align with and reference existing independent standards and security guidelines whenever possible. They correlate with over a dozen industry-standard frameworks, such as SOC 2, HIPAA, MITRE ATT&CK, NIST, and PCI DSS.

To help organizations with assessing, monitoring, and prioritizing their implementation of CIS controls, CIS offers a CIS Controls Self Assessment Tool.

List of CIS Controls in v8

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

There are multiple safeguards within every control prescribed by CIS (there are 153 safeguards in CIS Controls v8). The safeguards for each control are split into Implementation Groups (IGs), which reflect organizations' risk profiles and available resources. CIS recommends that every organization start with the safeguards in the first group, IG1, which are considered "essential cyber hygiene." For organizations with higher risk profiles and/or additional resources, IG2 builds on IG1 and so on.

Implementation Group descriptions:

IG1: An IG1 enterprise is typically small- to medium-sized with limited IT and cybersecurity resources. These enterprises are mainly focused on maintaining business operations due to their low tolerance for downtime. The data they protect, including employee and financial information, is not highly sensitive. IG1 safeguards can be implemented with minimal cybersecurity expertise and are designed to defend against broad, non-specific attacks. They are compatible with small business or home office commercial off-the-shelf hardware and software.

IG2: An IG2 enterprise incorporates IG1 controls but also includes dedicated staff for managing IT infrastructure across various departments with different risk profiles. These organizations often handle sensitive client or business information and can tolerate brief service interruptions. A significant concern is the potential loss of public trust in the event of a breach. Addressing this heightened operational complexity, IG2 safeguards require enterprise-grade technology and specialized expertise for proper implementation and configuration.

IG3: An IG3 enterprise includes IG1 and IG2 controls and employs specialists in various cybersecurity areas, such as risk management and penetration testing. These organizations manage highly sensitive data under strict regulatory oversight, and are focused on maintaining service availability and protecting data confidentiality and integrity. Successful attacks could significantly harm public welfare. IG3 safeguards are designed to counter sophisticated, targeted attacks and mitigate zero-day threats.

Example of how safeguards are assigned to implementation groups

Control 1: Inventory and Control of Enterprise Assets

Safeguards:

1.1 Establish and Maintain Detailed Enterprise Asset Inventory
1.2 Address Unauthorized Assets
1.3 Utilize an Active Discovery Tool
1.4 Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
1.5 Use a Passive Asset Discovery Tool

- If a company falls into IG1, they should fulfill safeguards 1.1 and 1.2.
- If a company falls into IG2, they should fulfill safeguards 1.1 – 1.4.
- If a company falls into IG3, they should fulfill safeguards 1.1 – 1.5

Exploring DORA

DORA is a new act set to take effect in January 2025 to enhance the operational resilience of financial entities within the EU. The act focuses on risk management, incident reporting, resilience testing, third-party risk management, and information sharing for information communication and technology (ICT). But DORA is also a framework that helps organizations more broadly understand how to mitigate security threats. It can apply to large enterprises with financial arms and venture funds and offers a blueprint for similar regulatory frameworks across other sectors.

Key requirements of DORA

DORA's requirements are built around ensuring that organizations can withstand and quickly recover from ICT disruptions. This includes establishing robust risk management frameworks, detailed incident response strategies, and regular resilience testing.

DORA focuses on five domain requirements:

1. ICT risk management
    - Develop and maintain resilient ICT systems and tools to mitigate ICT risks.
    - Identify, classify, and document essential functions and assets.
    - Continuously monitor for ICT risks to implement protective and preventive measures.
    - Quickly detect anomalous activities.
    - Create detailed business continuity policies and disaster recovery plans, with annual testing that includes all support functions.
    - Implement mechanisms to learn and adapt from both external events and internal ICT incidents.
2. ICT-related incident reporting
    - Develop a process for recording and classifying all ICT incidents, identifying serious incidents based on criteria set by the regulation and specified by the three European Supervisory Authorities (EBA, EIOPA, and ESMA).
    - Submit initial, interim, and final reports on ICT-related incidents.
    - Standardize the reporting of ICT-related incidents using templates developed by the European Supervisory Authorities.
3. Digital operational resilience testing
    - Annually conduct basic ICT testing of tools and systems to identify, mitigate, and quickly address any weaknesses or gaps in countermeasures.
    - Periodically carry out advanced threat-led penetration testing for critical ICT services, with mandatory participation and full cooperation from third-party ICT service providers.
4. Third-party ICT risk management
    - Monitor risks from dependence on third-party ICT providers.
    - Maintain an updated register of all outsourced activities, including changes and intra-group services.
    - Address risks related to IT concentration and sub-outsourcing activities.
    - Standardize essential service elements and relationships with third-party ICT providers for comprehensive monitoring.
    - Ensure contracts with third-party ICT providers include detailed monitoring conditions, service level descriptions, and data processing locations.
    - Critical third-party ICT service providers are subject to a union-wide oversight framework that issues risk mitigation recommendations. Financial entities must evaluate risks from providers not adhering to these recommendations.
5. Information sharing
    - Financial entities can establish arrangements to exchange cyber threat information and intelligence among themselves.
    - The supervisory authority will provide anonymized cyber threat information and intelligence to financial entities.
    - Entities must implement mechanisms to review and act on the information provided by the authorities.

Looking at DORA through the lens of CIS Controls

Integrating the CIS controls framework into DORA helps organizations streamline their cybersecurity processes. It provides a practical methodology for achieving the resilience required by DORA through proven security practices detailed in widely used CIS Controls. This integration facilitates a more efficient, structured approach to managing cybersecurity risks, reducing complexity, and clarifying compliance efforts.

Integrating the CIS controls framework into DORA offers several advantages beyond just regulatory alignment. They include:

Unified approach to cybersecurity
CIS Controls provide a globally recognized and comprehensive set of security best practices that cover a wide range of cybersecurity domains. By mapping other frameworks like DORA to CIS Controls, organizations can adopt a unified approach to cybersecurity and compliance management, ensuring consistency and coherence across their security initiatives.

Simplified management
Many organizations already use CIS Controls as the foundation of their cybersecurity programs due to their practicality and effectiveness. By mapping additional frameworks like DORA to CIS Controls, organizations can simplify their cybersecurity management processes by leveraging existing infrastructure, resources, and expertise.

Efficient resource allocation
CIS Controls offer clear guidance on the implementation of security controls, making it easier for organizations to allocate resources effectively. By mapping DORA requirements to CIS Controls, organizations can prioritize their efforts based on the relative importance and impact of each control, ensuring that resources are allocated where they are most needed.

Scalability and adaptability
CIS Controls are designed to be scalable and adaptable to organizations of all sizes and industries. By mapping DORA or other regulatory frameworks to CIS Controls, organizations can ensure that their cybersecurity measures remain flexible enough to accommodate changes in regulatory requirements, technological advancements, and evolving threat landscapes.

Continuous improvement
CIS Controls are continuously updated and refined to reflect emerging threats and evolving security practices. By aligning other frameworks like DORA to CIS Controls, organizations can tap into this ongoing process of improvement, ensuring that their cybersecurity measures remain up to date and effective in mitigating emerging threats.

Mapping CIS Controls to DORA requirements

DORA requirement: ICT risk management	
CIS Controls alignment:	
	CIS Control 1: Inventory and Control of Enterprise Assets • Maintain a current and accurate inventory of all enterprise assets that connect to the network to ensure visibility and management of any asset that could be attacked or compromised.
	CIS Control 2: Inventory and Control of Software Assets • Actively manage all software on the network to ensure that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
	CIS Control 7: Continuous Vulnerability Management • Implement a robust vulnerability management program that includes regular scanning, prioritization of vulnerabilities based on risk, patch management processes, and verification of patch effectiveness.
	CIS Control 12: Network Infrastructure Management • Establish and maintain an accurate inventory of network assets, configure network devices securely, monitor network traffic for suspicious activities, and enforce network segmentation to limit the impact of potential breaches.
	CIS Control 17: Incident Response Management • Develop and regularly test an incident response plan, establish clear roles and responsibilities for incident response team members, deploy detection and monitoring tools to identify security incidents, and establish communication channels for reporting and escalating incidents.
	CIS Control 18: Penetration Testing • Conduct regular penetration tests to identify and address vulnerabilities in systems and applications, simulate real-world attack scenarios to assess the effectiveness of security controls, and prioritize remediation efforts based on the findings of penetration tests.

DORA requirement: ICT-related incident reporting

CIS Controls alignment:

CIS Control 8: Audit Log Management

- Configure systems and applications to generate detailed audit logs, centrally collect and store audit logs for analysis, establish log retention policies to meet regulatory requirements, and regularly review audit logs for signs of unauthorized access or malicious activities.

CIS Control 17: Incident Response Management

- Develop incident response procedures that include processes for detecting, reporting, and responding to security incidents, establish communication channels for reporting incidents to appropriate stakeholders, and define criteria for classifying and prioritizing incidents.

DORA requirement: Digital operational resilience testing

CIS Controls alignment:

CIS Control 7: Continuous Vulnerability Management

- Continuously monitor for vulnerabilities in systems and applications, prioritize remediation efforts based on risk assessments, and regularly validate the effectiveness of security controls through vulnerability scanning and assessment.

CIS Control 17: Incident Response Management

- Conduct tabletop exercises and simulated cyber attack scenarios to test the effectiveness of incident response procedures, identify gaps in incident detection and response capabilities, and refine incident response plans based on lessons learned from testing.

CIS Control 18: Penetration Testing

- Conduct regular penetration tests to identify and address vulnerabilities in systems and applications, simulate real-world attack scenarios to assess the effectiveness of security controls, and prioritize remediation efforts based on the findings of penetration tests.

DORA requirement: Third-party ICT risk management

CIS Controls alignment:

CIS Control 12: Network Infrastructure Management

- Identify and assess risks associated with third-party ICT providers, establish contractual requirements for third-party providers to meet security standards, and monitor third-party providers for compliance with contractual obligations.

CIS Control 15: Service Provider Management

- Establish a formal process for evaluating and selecting third-party ICT providers, conduct due diligence assessments to evaluate the security posture of potential providers, and establish contractual agreements that include provisions for security requirements and oversight.

CIS Control 17: Incident Response Management

- Include third-party providers in incident response planning and coordination efforts, establish communication channels for reporting and responding to security incidents involving third-party providers, and conduct regular reviews of third-party provider performance and compliance.

DORA requirement: Information sharing

CIS Controls alignment:

CIS Control 14: Security Awareness and Skills Training

- Provide security awareness training to employees to educate them about cybersecurity risks and best practices, conduct phishing simulations to test employee awareness, and encourage reporting of security incidents and concerns.

CIS Control 17: Incident Response Management

- Establish information sharing partnerships with industry peers and relevant authorities to exchange threat intelligence and cybersecurity best practices, participate in information sharing forums and communities, and contribute to collective efforts to improve cybersecurity resilience.

Impact on industries

CIS Controls have broad applicability to organizations of all sizes and types. And while DORA aims to enhance the operational resilience of financial entities, its principles can offer guidance to other industries as well. When the two are applied in an integrated approach, organizations can reap numerous benefits. Below are examples of the impacts that integrating the CIS Controls framework into DORA can have on various industries.

Financial services

In the financial sector, compliance with DORA and CIS Controls mitigates risks associated with online transactions and data breaches, enhancing trust and ensuring business continuity. Financial institutions and lines of business must particularly pay attention to DORA's stringent requirements for operational resilience and the management of third-party ICT risks.

Healthcare and life sciences

DORA's principles, although primarily aimed at financial services, provide a valuable blueprint for managing ICT disruptions that can also be applicable in healthcare, particularly in securing data exchanges and ensuring the availability of critical healthcare systems. DORA also offers a framework for protecting sensitive patient data and research information, crucial for compliance with regulations such as HIPAA and GDPR.

Manufacturing

For manufacturers, integrating CIS Controls with a DORA framework can fortify defenses against cyber threats to industrial control systems and safeguard intellectual property critical to maintaining competitive advantage. The emphasis on resilience and third-party risk management can help ensure that manufacturing operations are not disrupted by ICT failures.

Retail

Retailers benefit by securing consumer data and financial transactions, thus maintaining consumer trust and compliance with data protection regulations like GDPR. The adoption of DORA's approach to operational resilience can help prevent downtime during peak shopping periods caused by ICT-related incidents.

Energy

The energy sector can apply DORA frameworks to enhance the security and resilience of infrastructure critical to public safety and economic stability. By adopting CIS Controls and considering DORA-like resilience testing, energy businesses can better manage the risks associated with digital and physical threats to energy grids and other critical infrastructure.

Education

Educational institutions handling vast amounts of student data can use CIS Controls for securing databases and networks. While not directly under DORA, the act's focus on resilience and third-party management can guide educational policies on ICT risk, especially as institutions increasingly depend on digital platforms.

Telecommunications

Telecom businesses, integral to the functioning of modern economies and societies, can enhance network security and service availability by integrating CIS Controls and adopting DORA's focus on resilience. This is particularly pertinent given their role in managing vast amounts of data and their susceptibility to large-scale cyberattacks.

Implementing CIS Controls and DORA in DDI solutions

Inherent cybersecurity risks in DDI

The most important first step any organization can take before launching any network transformation or compliance project is to get its house in order. Understanding what is on the network, where devices are located, and how they currently communicate is imperative. This is why core services like DNS, DHCP, and IP address management—together known as DDI—are so important. But they are often overlooked when planning new IT projects.

The management of DHCP configurations and IP addresses also comes with inherent risks. DHCP, which dynamically assigns IP addresses to devices on a network, can be exploited to issue incorrect or malicious configurations if not properly secured. Similarly, ineffective IP address management can lead to conflicts and unauthorized network access, creating vulnerabilities that can be exploited by external threats.

DNS's critical role in network functionality also makes it a significant target for cyber attacks. Threats like DNS hijacking, tunneling, and poisoning can disrupt operations and lead to severe data breaches. The security and resilience of DNS services are paramount, as they help prevent unauthorized access and ensure that traffic is correctly routed to legitimate destinations.

The role of unified DDI solutions

In this context, unified DDI solutions are crucial. These solutions not only streamline and automate DDI management. They also enhance the security posture of the network by providing centralized visibility and control over these critical services. By integrating DDI into a cohesive system, organizations can better detect anomalies, enforce policies, and respond to incidents, thereby reducing the attack surface and improving overall network resilience.

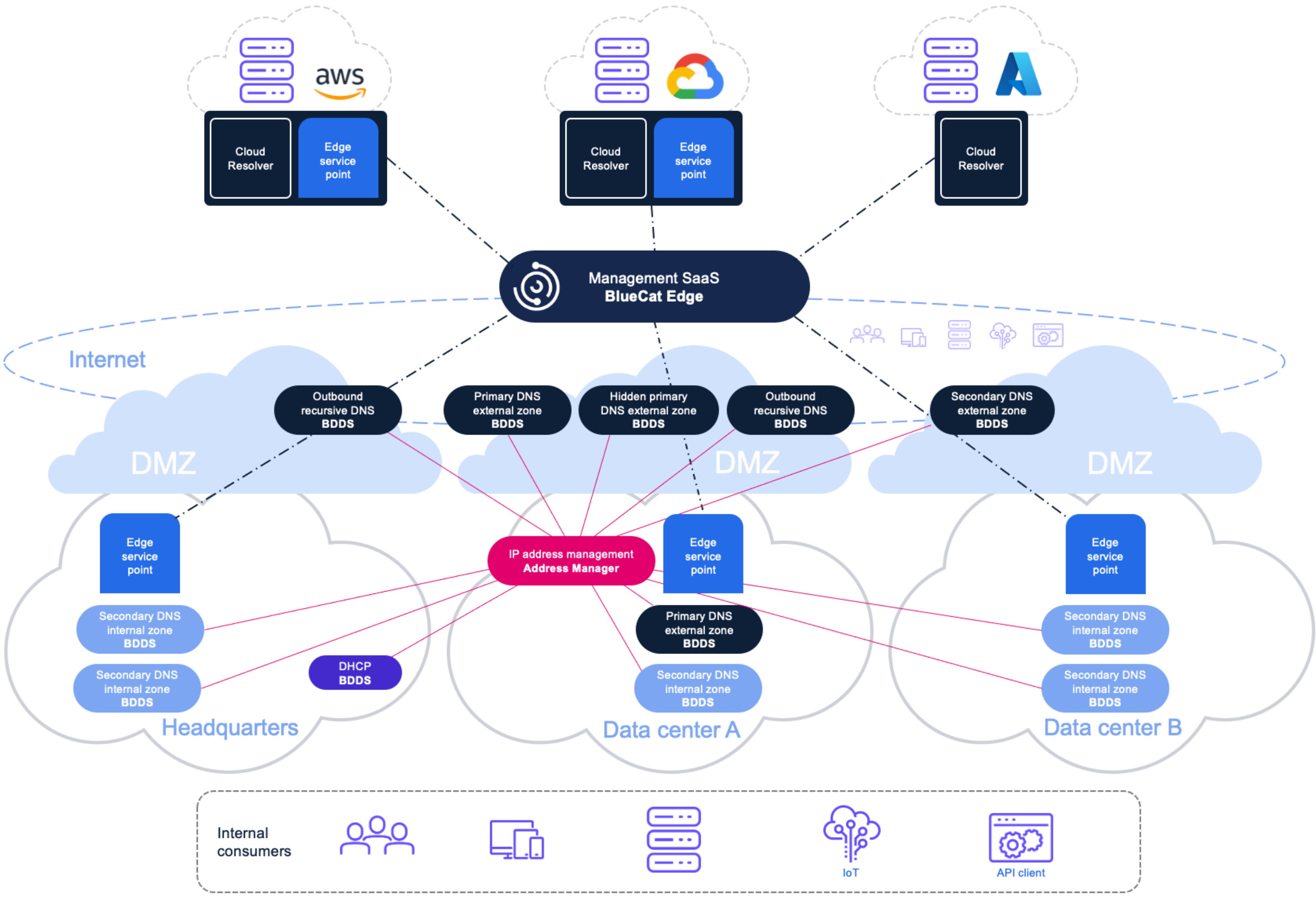
BlueCat's portfolio of offerings enhances security, ensures continuity, and supports compliance with key regulatory frameworks such as CIS Controls. The next section will delve deeper into how BlueCat's products and features align with these controls, providing practical examples of their application in real-world scenarios. This will further illustrate the critical role of advanced DDI solutions in safeguarding modern digital infrastructures.

BlueCat's role in cybersecurity and compliance

Networks vary in their requirements for DNS-related resolution, routing, and security. Some sites require special policies and enhanced security observability due to their risk profile and location. Using BlueCat's solutions, you can meet these cybersecurity and compliance requirements with features that provide:

- Intelligent DNS resolution
- Policy enforcement
- Deep query searches for troubleshooting and forensics
- Integration with SIEMs
- Enhanced real-time security using threat intelligence feeds to build dynamic domain lists for use in policies
- The ability to limit specific protocols, such as DNS over HTTPS queries

Unified DDI for intelligent DNS discovery and routing


aws
Cloud Resolver
Edge service point
Cloud Resolver
Edge service point
Cloud Resolver
Management SaaS
BlueCat Edge
Internet
Outbound recursive DNS BDDS
Primary DNS external zone BDDS
Hidden primary DNS external zone BDDS
Outbound recursive DNS BDDS
Secondary DNS external zone BDDS
DMZ
DMZ
DMZ
Edge service point
IP address management
Address Manager
Edge service point
Edge service point
Secondary DNS internal zone BDDS
Secondary DNS internal zone BDDS
DHCP BDDS
Headquarters
Primary DNS external zone BDDS
Secondary DNS internal zone BDDS
Data center A
Secondary DNS internal zone BDDS
Secondary DNS internal zone BDDS
Data center B
Internal consumers
IoT
API client

As footprints expand and workloads evolve, it is essential for security and detection teams to rely on solid, observable foundations. Teams must clearly understand the boundaries of their managed IP and namespaces. Trust in IP routing, DNS routing, and DHCP scopes is crucial to ensure secure and accurate data flow to its intended endpoints. This goes beyond merely being a repository or orchestration tool that integrates cloud and on-premises networks; it serves as a prime observation and policy enforcement point for identifying and blocking digital threats before any data transmission begins.

The diagram above illustrates real-time, cloud-aware intelligent DNS discovery and routing across hybrid or multicloud environments using BlueCat Edge. This approach eliminates manual forwarders, isolated DNS islands, and inconsistent resolutions. The setup automatically addresses access and zone overlap issues and facilitates the creation of reverse zones for seamless, organization-wide resolution. DNS routing and selective forwarding are policy-based, dynamically adapting to domain lists and query origins, with updates from Cloud Resolver enabling smart management of forwarders and actions.

With Edge, network teams can use built-in integrations with best-of-breed services such as Cisco Umbrella to enhance security defenses across an organization. This allows for improved threat detection and protection by monitoring both east-west and north-south DNS traffic. Leveraging Umbrella's threat intelligence, BlueCat Edge provides proactive mitigation of attacks before they connect to command-and-control channels.

Mapping BlueCat's solutions to CIS Controls

BlueCat's solutions offer centralized control, enhanced visibility, and advanced security features that support compliance and mitigate risk. How BlueCat's products map to specific CIS Controls and their safeguards is detailed below.

Integrity

Integrity is BlueCat's platform for integrated DDI management for large enterprises. It simplifies and consolidates DDI visibility and management across the most complex network infrastructures. Powered by RESTful APIs, Integrity automates all aspects of DDI management. Integrity is comprised of BlueCat Address Manager and BlueCat DNS and DHCP Server (BDDS).

Address Manager performs IP address management and acts as the main DNS and DHCP management platform (cluster or single node). Depending on the requirements, architecture, and footprint, BDDSes are single instances or clusters that selectively provide authoritative DNS and/or DHCP services.

Cloud Discovery & Visibility, an application within Integrity, discovers the entirety of your on-premises and multicloud footprint and streams that data to Address Manager for up-to-date information.

Each component is flexible and can be deployed in multiple form factors, either physical or virtual.

Mapping to CIS Controls and safeguards

Control 1: Inventory and Control of Enterprise Assets

- Safeguards: 1.1, 1.2, 1.3, 1.4, 1.5

Control 2: Inventory and Control of Software Assets

- Safeguards: 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7

Control 4: Secure Configuration of Enterprise Assets and Software

- Safeguards: 4.1, 4.2, 4.4, 4.5

Control 5: Account Management

- Safeguards: 5.1, 5.3, 5.5

Control 9: Limitation and Control of Network Ports, Protocols, and Services

- Safeguards: 9.1

Control 11: Data Recovery

- Safeguards: 11.1, 11.2

Control 12: Network Infrastructure Management

- Safeguards: 12.1, 12.3

Control 13: Network Monitoring and Defense

- Safeguards: 13.4, 13.6

Control 16: Application Software Security

- Safeguards: 16.2, 16.5, 16.7, 16.9, 16.10, 16.12

Gateway

While all BlueCat solutions offer open, robust, and updated APIs, Gateway brings together all the building blocks to allow for automating business processes with custom integrations, plugin development, and DDI workflows. Gateway uses an API with a set of Python classes for integrating third-party solutions with Integrity's Address Manager or BDDS, or with Edge.

Additionally, with BlueCat's existing catalog of adaptive applications and plugins, teams can immediately build and innovate around providers or platforms such as:

- **Networking:** Cisco, VMware, Microsoft, Nutanix, OpenStack, ServiceNow, and Ansible
- **Cloud:** AWS, Microsoft Azure, and Google Cloud
- **Security:** Palo Alto Networks, Cisco, Splunk, IBM, ArcSight, and CrowdStrike

Mapping to CIS Controls and safeguards

Control 1: Inventory and Control of Enterprise Assets

- Safeguards: 1.1, 1.3

Control 5: Account Management

- Safeguards: 5.1, 5.3, 5.5

Control 7: Continuous Vulnerability Management

- Safeguards: 7.1, 7.2, 7.3, 7.4

Control 8: Audit Log Management

- Safeguards: 8.2

Control 10: Malware Defenses

- Safeguards: 10.7

Control 12: Network Infrastructure Management

- Safeguards: 12.1, 12.2, 12.3

Control 13: Network Monitoring and Defense

- Safeguards: 13.7

Control 15: Service Provider Management

- Safeguards: 15.4, 15.5

Control 16: Application Software Security

- Safeguards: 16.2, 16.5, 16.7, 16.9, 16.10, 16.12

Control 17: Incident Response Management

- Safeguards: 17.9

Control 18: Application Software Security

- Safeguards: 18.3

Edge

Edge brings additional IP forwarding, discovery, resolution, and security capabilities to standard DDI infrastructure in three key areas: networking, security, and cloud. Edge is a lightweight, cloud-managed software solution that delivers advanced DNS capabilities via service points deployed across the edge of your network.

For networking, Edge uses intelligent forwarding via service points to set conditions and direct queries to the right destination.

For security, Edge provides advanced threat protection that also blocks malicious queries, policy enforcement, and intelligence from cutting-edge threat data feeds.

For cloud, network teams can resolve DNS queries across complex cloud deployments with ease, using Cloud Resolver.

Edge provides an intelligent layer of control to address threats, solve namespace collisions, and optimize query response latency based on organizational policies. By mapping directly to these frameworks, Edge users can meet or exceed security and compliance requirements.

Mapping to CIS Controls and safeguards

Control 1: Inventory and Control of Enterprise Assets

- Safeguards: 1.1, 1.3

Control 9: Malware Defenses

- Safeguards: 9.1, 9.2

Control 10: Malware Defenses

- Safeguards: 10.6

Control 12: Network Infrastructure Management

- Safeguards: 12.1, 12.3

Control 13: Network Monitoring and Defense

- Safeguards: 13.1, 13.2, 13.3

Control 16: Application Software Security

- Safeguards: 16.2, 16.5, 16.7, 16.9, 16.10, 16.12

BlueCat's role-specific training

Control 14: Security Awareness and Skills Training

- Safeguards: 14.2, 14.3, 14.4, 14.8, 14.9

Infrastructure Assurance

Infrastructure Assurance provides proactive observability, troubleshooting, and remediation for network and security infrastructure, including Integrity, firewalls, and load balancers. It identifies hidden issues, conducts automated diagnosis, and offers expert-recommended remediation steps.

With deep visibility and automation, it prevents network disruptions and streamlines tasks like maintenance and high availability validation, efficiently analyzing critical data based on best practices. Key capabilities include:

- Auto-detection
- Auto-triage
- Automated configuration backup
- Automated operations maintenance
- Benchmarking for infrastructure

Mapping to CIS Controls and safeguards

Control 1: Inventory and Control of Enterprise Assets

- Safeguards: 1.1, 1.2, 1.3

Control 3: Data Protection

- Safeguards: 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14

Control 4: Secure Configuration of Enterprise Assets and Software

- Safeguards: 4.1, 4.2, 4.4, 4.5

Control 5: Account Management

- Safeguards: 5.1, 5.3

Control 6: Access Control Management

- Safeguards: 6.1, 6.4, 6.5

Control 7: Continuous Vulnerability Management

- Safeguards: 7.1

Control9: Limitation and Control Network Ports, Protocols, and Services

- Safeguards 9.1

Control 10: Malware Defenses

- Safeguards: 10.1, 10.5, 10.6, 10.7

Control 11: Data Recovery

- Safeguards: 11.1, 11.2, 11.3

Control 12: Network Infrastructure Management

- Safeguards: 12.1, 12.2, 12.3

Control 13: Network Monitoring and Defense

- Safeguards: 13.1, 13.2, 13.5, 13.6

Control 15: Service Provider Management

- Safeguards 15.4

Control 16: Application Software Security

- Safeguards: 16.2, 16.3, 16.5, 16.7, 16.9, 16.10, 16.12

Control 17: Incident Response Management

- Safeguards: 17.9

Control 18: Penetration Testing

- Safeguards 18.3

The future outlook

Supported by BlueCat's solutions, integrating CIS Controls and DORA offers organizations a comprehensive approach to managing cybersecurity risks and regulatory compliance. By leveraging these frameworks and technologies, businesses can ensure that they are not only protected against current threats but are also prepared for future cybersecurity challenges.

As threats evolve and regulatory environments become more complex, organizations will need to continually adapt their cybersecurity strategies. The integration of advanced solutions like BlueCat's will be crucial for maintaining security and compliance across all sectors.

BlueCat helps enterprises achieve their network modernization objectives by delivering innovative products and services that enable networking, security, and DevOps teams to deliver change-ready networks with improved flexibility, automation, resiliency, and security.

Headquarters
4100 Younge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 I 1-866-6931

bluecat.com

Ready to learn more?

Connect with a BlueCat representative and see how we can help you manage, build, and secure your network.

Contact us