Transforming Remote Access with Google BeyondCorp Enterprise

Table of Contents

Executive Summary

Traditional VPN remote access solutions are no longer sufficient to protect organizations against sophisticated attacks. Google BeyondCorp Enterprise (BCE) offers a modern and effective approach to secure remote access while improving compliance with industry standards such as HIPAA, FedRam, and NIST 800-53 control frameworks. This whitepaper provides an in-depth overview of a successful migration project for a financial services organization, highlighting the steps involved in developing the business case, personas involved, critical decisions made, design considerations, and the implementation process. By following this approach, organizations can transform their remote access capabilities and achieve a zero trust security model with Google BeyondCorp Enterprise.

Introduction

In today's interconnected, hybrid work model world, remote access is a critical requirement for enabling a distributed workforce. However, VPN solutions have inherent limitations that hinder security, user experience, and compliance. Google BeyondCorp Enterprise is a cloud-native, zero trust solution that addresses these challenges by providing secure access to applications and resources based on user identity, device trustworthiness, and real-time context. This whitepaper outlines the key steps and considerations involved in migrating from a VPN remote access model to BeyondCorp Enterprise, drawing insights from a recent project with a large financial services organization.

Building the Business Case for Google BeyondCorp Enterprise

Develop the Business Case

Developing a business case is a critical first step in the migration to a zero trust security model. It involves a comprehensive analysis of existing remote access capabilities, identification of pain points and limitations, and articulation of the potential benefits and return on investment (ROI) associated with implementing Google's BeyondCorp Enterprise platform. The following steps provide detailed information of the key elements involved in developing the business case to ensure BCE is right for your business.

Current Remote Access Model Assessment

The assessment of the current remote access model is essential to understand its strengths, weaknesses, and risks. This evaluation involves examining the architecture, technology stack, security controls, management approach, and user experience of the existing VPN-based solution. It is important to assess the scalability, performance, and operational overhead of the current model to identify areas that can be improved with BeyondCorp Enterprise.

During this assessment, organizations should consider factors such as the complexity of network configurations, the need for continuous updates and patching, the challenges of managing VPN client software on user devices, how the platform exists with collaboration tools used by the business, and the risks associated with a perimeter-centric security approach. A thorough understanding of these limitations provides the foundation for building a compelling business case for the migration and an understanding of the risks and their impact on the business if the existing VPN controls fail.

Identification of Pain Points and Limitations

Identifying the pain points and limitations of the current remote access model is crucial for emphasizing the need for change. Organizations should engage with key stakeholders, including IT teams, security teams, and end users to gather feedback and insights. Pain points may include user complaints about VPN connectivity issues, complex authentication processes, limited visibility and control over user access, the use of middle proxies, costs, and the potential security risks associated with compromised user credentials or unmanaged devices.

In addition, organizations should consider the limitations imposed by regulatory compliance requirements. If the current remote access model falls short in meeting industry-specific standards, such as HIPAA or NIST, this becomes a critical driver for migrating to BeyondCorp Enterprise.

Articulate Benefits and ROI

To build a persuasive business case, it is crucial to capture and communicate the benefits and return on investment that a zero trust security model using BeyondCorp Enterprise can deliver. These benefits can be categorized into three main areas: security, compliance, and user experience.

From a security perspective, BeyondCorp Enterprise offers a zero trust architecture that eliminates the reliance on perimeter defenses and instead focuses on continuous verification of trust for every access request. This approach significantly reduces the risk of unauthorized access, lateral movement within the network, and the impact of potential breaches. Organizations can highlight statistics and industry reports that demonstrate the effectiveness of zero trust architectures in preventing data breaches and reducing the attack surface. This was the main driver for Google to develop the security model and solution after it was attacked by a nation state in 2010.

Regarding compliance, BeyondCorp Enterprise provides robust security controls and integrates with industry-standard frameworks. By implementing BeyondCorp Enterprise, organizations can align their remote access solution with these compliance requirements, ensuring the protection of sensitive data and mitigating compliance-related risks. The in-depth capabilities of BCE provide more options to dial-in your organization's security objectives over a perimeter-based security model.

In terms of user experience, BeyondCorp Enterprise offers a seamless and frictionless access experience for users. With passwordless authentication methods, certificate-based authentication, and device attestation, users can enjoy simplified and secure access to resources from any location, on any device - all centrally managed by the organization. This improves productivity, reduces user frustration, and minimizes help desk support calls related to remote access issues.

To quantify the ROI, organizations can consider factors such as reduced operational costs associated with managing VPN infrastructure and middle proxies, decreased support and maintenance efforts, improved productivity due to simplified access workflows, and potential cost savings resulting from a reduced risk of data breaches and associated legal and regulatory penalties. Onix has seen both soft and hard costs reduced using Google BCE, especially when bundled with Google Workspace licensing.

By clearly articulating the benefits and ROI of implementing BeyondCorp Enterprise, organizations can effectively build a business case that resonates with key stakeholders and decision-makers.

Key Stakeholders Involved with BCE Projects

Successful implementation of Google BeyondCorp Enterprise requires the active involvement and collaboration of various stakeholders within the organization. Understanding the roles and responsibilities of these key personas is essential for effective decision-making, coordination, and execution of the project. We will explore the primary personas involved, with a specific focus on the Chief Information Security Officer (CISO) and Workspace Administrator roles.

Chief Information Security Officer (CISO)

The CISO (and his/her direct reports) play a pivotal role in the migration to Google BeyondCorp Enterprise. As the leadership team responsible for overseeing the organization's information security strategy and operations, the “Office of the CISO” - the group of decision-makers working under the direction of the CISO on special projects- provides the necessary leadership and guidance to ensure the successful implementation of a zero trust architecture.

The Office of the CISO's involvement begins early in the process, during the development of the business case. They contribute by providing insights into the organization's security posture, compliance requirements, and risk management strategies. This team helps articulate the security benefits of BeyondCorp Enterprise, such as improved visibility, reduced attack surface, and enhanced threat detection and response capabilities. They also ensure alignment with regulatory standards, industry best practices, and the organization's risk appetite. They are the primary drivers of changing the mindset early in the adoption process.

During the implementation phase, the Office of the CISO collaborates closely with other stakeholders to define security policies, access controls, and incident response procedures within the BeyondCorp Enterprise framework. They provide oversight and guidance to the security team responsible for configuring and managing the security controls offered by Google Cloud.

The Office of the CISO also plays a critical role in driving user adoption and change management. They communicate the strategic importance of the migration, address security concerns, and emphasize the benefits of BeyondCorp Enterprise to both executive leadership and end users. Additionally, this team ensures that security awareness and training programs are implemented to educate employees about the new security measures and their responsibilities within the zero trust environment.

Leverage the CISO role to affect change in the organization related to secure remote access and enablement. By thoughtfully using the Office of the CISO, complemented by the appropriate policies and procedures that support zero trust security, getting and maintaining buy-in will be easier to manage over the life of the solution.

Google Workspace Administrator

The Google Workspace Administrator and anyone involved in Workspace decision-making are key personnel responsible for managing and configuring Google Workspace services, including user accounts, access controls, and security settings. Their role becomes crucial during the migration to BeyondCorp Enterprise, as they undertake tasks such as:

- User Provisioning and Identity Management: The Google Workspace Administrator manages user accounts, creates groups, and assigns appropriate roles and permissions within Google Workspace. They play a vital role in ensuring that user identities are properly integrated with BeyondCorp Enterprise, enabling seamless access to resources based on user attributes and policies.

- Configuration of Security Policies: The Workspace Admin and his/her team configures security policies within Google Workspace to align with the principles of BeyondCorp Enterprise. This includes setting up password requirements, enforcing two-factor authentication, and configuring security settings such as session controls and device management policies.

- Integration with BeyondCorp Enterprise: The Workspace Admin collaborates with the security and network teams to integrate Google Workspace with BeyondCorp Enterprise. This involves configuring the necessary APIs, enabling secure Single Sign-On (SSO) for seamless authentication, and establishing trust relationships between Google Workspace and BeyondCorp components. Security and network teams may manage BCE. This depends on the org structure and roles and responsibilities in the organization.

- User Training and Support: The Admin and their team provide training and support to end users on accessing Google Workspace services within the BeyondCorp Enterprise environment. They assist with onboarding new users, addressing user inquiries, and ensuring a smooth user experience during and after the migration.

- Ongoing Management and Optimization: The Workspace Admin and team manage and optimize Google Workspace services within the BeyondCorp Enterprise framework. This includes monitoring user access, reviewing security logs, testing and validating new use cases, and implementing updates and patches to maintain a secure environment.

The Google Workspace Administrator collaborates closely with the Office of the CISO, security teams, and other stakeholders to ensure that the Google Workspace environment is properly aligned with the security principles and access controls of BeyondCorp Enterprise.

Effective coordination and collaboration among the Office of the CISO, Google Workspace Administrator, and other stakeholders are essential for a successful migration to BeyondCorp Enterprise.

Other Key Stakeholders and Participants

In addition to the CISO, several other key stakeholders and personas are involved in the migration to BeyondCorp Enterprise:

- IT Leadership: The IT leadership team, including the Chief Information Officer (CIO) and IT managers, provides strategic direction, resource allocation, and support for the migration project. They ensure that the migration aligns with the organization's overall IT strategy and objectives.

- Security Teams: The security teams, including security architects, analysts, and engineers, collaborate with the CISO to define security policies, configure security controls, and manage security incidents. They are responsible for implementing the technical aspects of BeyondCorp Enterprise and ensuring its alignment with the organization's security requirements.

- Network Teams: The network teams, including network architects and engineers, work closely with the security teams to design and implement the network architecture required for BeyondCorp Enterprise. They are responsible for network segmentation, access control configurations, and ensuring the availability and performance of the network infrastructure.

- Compliance Teams: The compliance teams, including compliance officers and auditors, collaborate with the CISO to ensure that the migration to BeyondCorp Enterprise aligns with regulatory requirements and industry standards. They provide guidance on compliance frameworks, assist with compliance assessments, and support the organization in maintaining and demonstrating compliance with relevant regulations.

- Application Owners: Application owners, such as product managers or business unit leaders, play a crucial role in the migration process. They provide insights into the specific requirements and access needs of their applications and collaborate with the security and network teams to ensure a smooth transition to BeyondCorp Enterprise. Application owners are responsible for testing and validating the functionality of their applications within the new access model.

- End Users: The end users, including employees and contractors, are impacted directly by the migration to BeyondCorp Enterprise. Their feedback and cooperation are essential for a successful transition. End users may participate in PoC testing, provide input on user experience improvements, and receive training and awareness sessions to familiarize themselves with the new access workflows and security measures.

Effective collaboration among these key stakeholders is vital for a smooth and successful migration to Google BeyondCorp Enterprise. Clear communication, shared goals, and a coordinated effort will ensure that the implementation aligns with the organization's security, compliance, and operational requirements.

By engaging and involving the CISO and other key stakeholders, organizations can leverage their expertise and perspectives to make informed decisions, address security concerns, and foster a culture of security throughout the migration process and beyond. The involvement of these personas ensures that the migration project considers all relevant aspects and positions the organization for long-term success in the zero trust era.

In the next section, we will delve into the critical decisions that need to be made during the migration project, which will further shape the implementation of Google BeyondCorp Enterprise within the organization.

Critical Decisions and Considerations

During the migration to Google BeyondCorp Enterprise, several critical decisions need to be made to ensure a successful implementation. These decisions shape the architecture, policies, and workflows within the zero trust framework. Additionally, various considerations must be taken into account to address specific organizational requirements and challenges. We will explore some of the key decisions and considerations that organizations should carefully evaluate.

Architecture Design Decisions

- Network Segmentation: One of the fundamental architectural decisions is how to segment the network within the BeyondCorp Enterprise framework. This decision involves determining the appropriate network boundaries, defining trust domains, and establishing access policies based on user roles, device attributes, and contextual information. Considerations such as scalability, ease of management, and the organization's specific security requirements should guide the design of network segments.

- Access Control Model: Organizations need to decide on the access control model they will adopt within BeyondCorp Enterprise. The two common approaches are attribute-based access control (ABAC) and role-based access control (RBAC). ABAC leverages user attributes and contextual information to determine access decisions, while RBAC uses predefined roles and permissions. The choice between these models depends on factors such as the complexity of access policies, the level of granularity required, and the organization's existing access management processes.

- Device Trust and Management: Organizations must determine how they will establish trust in user devices and enforce device management policies. This decision involves considering factors such as the supported device platforms, device attestation methods, and integration with existing mobile device management (MDM) or endpoint security solutions (including Google Workspace). Organizations should carefully evaluate the trade-offs between security requirements, user experience, and the complexity of device management processes.

Policy and User Experience Considerations

- Policy Definition and Enforcement: Organizations need to define access policies that align with their security requirements and compliance obligations. This includes determining policies for user authentication, authorization, and session controls. Considerations should be given to factors such as multi-factor authentication methods, granular authorization rules, and adaptive access policies based on risk assessment. It is crucial to strike the right balance between security controls and user experience to ensure seamless and frictionless access.

- User Experience and Productivity: The user experience is a critical consideration in the success of BeyondCorp Enterprise. Organizations must carefully assess the impact of the migration on end users and take steps to optimize user experience and productivity. This includes providing clear communication and training on the new access workflows, ensuring minimal disruption

during the migration, and designing intuitive self-service portals for managing access requests and permissions.

- External Collaboration: Organizations should consider how external collaborators, such as partners, suppliers, and contractors, will be granted access to resources within BeyondCorp Enterprise. Decisions need to be made regarding the onboarding and authentication of external users, the enforcement of security policies for external entities, and the provision of secure collaboration tools to facilitate external collaboration while maintaining a zero trust approach.

Compliance and Regulatory Considerations

- Data Protection and Privacy: Organizations must consider how BeyondCorp Enterprise aligns with data protection and privacy regulations, such as GDPR, HIPAA, or NIST. This involves understanding data residency requirements, ensuring appropriate data access controls, and implementing mechanisms for data protection, such as encryption and data loss prevention (DLP) strategies. Compliance with regulatory obligations related to data handling and privacy should be a key consideration throughout the migration process.

- Compliance Framework Integration: Organizations operating in regulated industries must ensure that BeyondCorp Enterprise meets their specific compliance requirements. This includes integrating BeyondCorp Enterprise with relevant compliance frameworks such as HIPAA, FedRAMP, and control frameworks. Organizations should assess the specific security controls and safeguards required by these frameworks and ensure that BeyondCorp Enterprise provides the necessary capabilities to meet those requirements.

- Audit and Monitoring: Considerations should be given to how audit and monitoring activities will be performed within BeyondCorp Enterprise. Organizations must determine the logging and monitoring mechanisms to capture and analyze security events, as well as establish processes for conducting regular audits and security assessments to maintain compliance and identify potential risks or vulnerabilities.

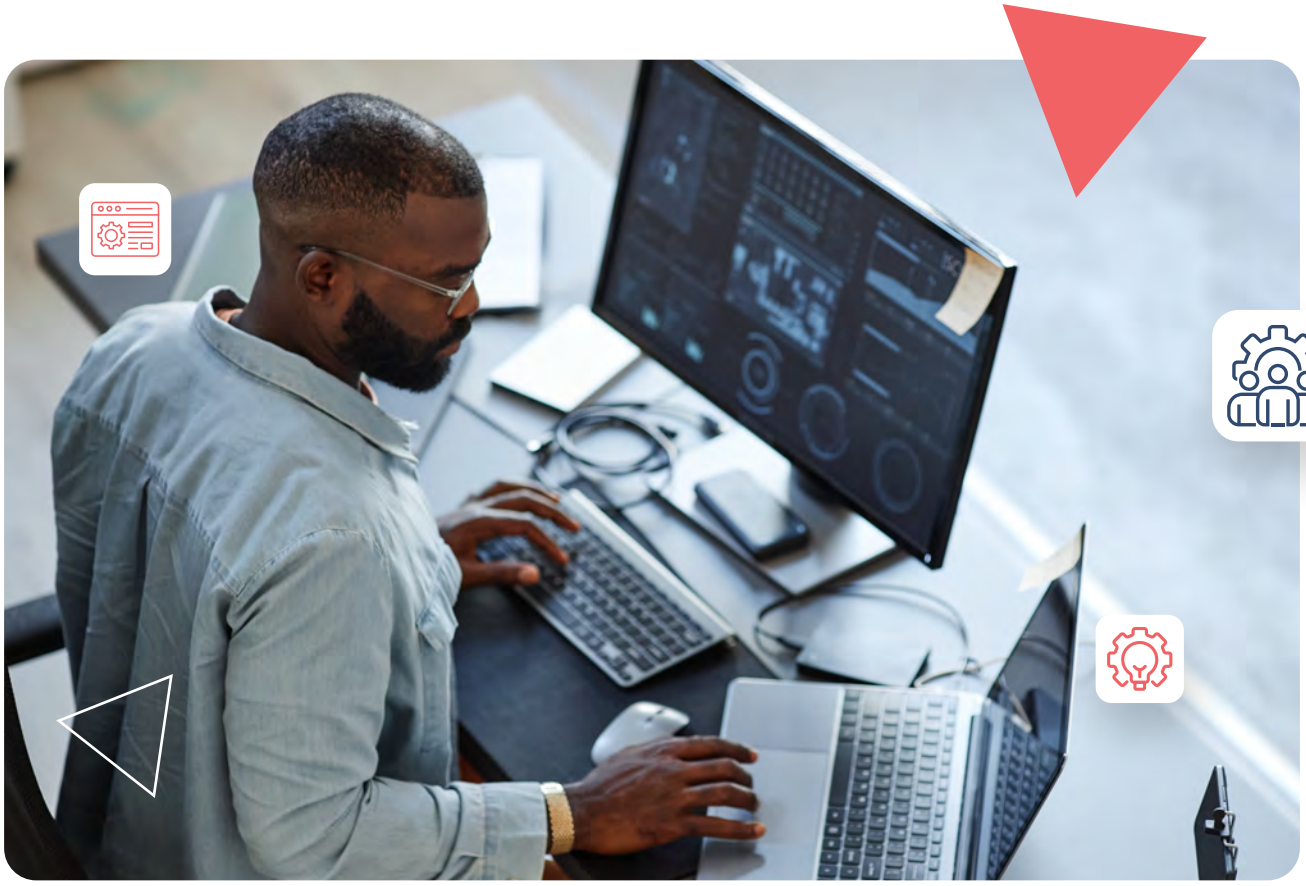
Change Management and User Adoption

- Communication and Training: Successful migration to BeyondCorp Enterprise relies on effective communication and comprehensive training programs. Organizations should develop a change management strategy that includes clear communication channels, regular updates on the migration progress, and targeted training sessions for different user groups. This helps users understand the benefits of the new access model, addresses concerns, and promotes a positive attitude towards the migration.

- User Feedback and Iterative Improvements: Organizations should establish channels for gathering user feedback and incorporating it into the ongoing optimization of BeyondCorp Enterprise. Regular feedback loops, surveys, and user sentiment analysis can provide valuable insights into user experience, identify pain points, and drive iterative improvements to the access workflows and overall user satisfaction.

- Executive Sponsorship: Executive sponsorship is crucial for driving user adoption and overcoming resistance to change. By securing buy-in from executive leadership, organizations can foster a culture of security and create a sense of urgency and commitment to the migration project. Executives can serve as champions, advocating the benefits of BeyondCorp Enterprise and encouraging widespread adoption across the organization.

In summary, organizations embarking on the migration to Google BeyondCorp Enterprise need to make critical decisions and consider various aspects related to architecture design, policy definition, user experience, compliance, and change management. By carefully evaluating these decisions and considerations, organizations can ensure a successful implementation that aligns with their security objectives, compliance requirements, and operational needs. In the section that follows, we will outline the high-level steps involved in implementing and migrating users from their VPN solution to BeyondCorp Enterprise.



Design Approach for Google BeyondCorp Enterprise

Effective design considerations are crucial for a successful implementation of Google BeyondCorp Enterprise. We outline key design principles and considerations that organizations should address during the planning and design phase of the migration.

Zero Trust Architecture

Zero Trust is the core principle of BeyondCorp Enterprise. Zero Trust has implications for network architecture, access policies, and security controls. It emphasizes the importance of continuously verifying trust and implementing least privilege access to ensure a robust security posture.

Identity and Device Verification

Strong identity and device verification mechanisms are essential components of BeyondCorp Enterprise. There are various methods for user authentication, including passwordless authentication, certificate-based authentication, and device attestation. Consider how continuous device health checks and access policies based on device posture are setup and configured.

Network and Service Segmentation

Segmentation is a key aspect of BeyondCorp Enterprise's network architecture. Network segmentation helps reduce the attack surface and mitigate potential breaches. It explores strategies for segmenting networks and services based on user roles, sensitivity of data, and security requirements.

Security Monitoring and Incident Response

Proactive security monitoring and incident response capabilities are vital for maintaining a secure environment with BeyondCorp Enterprise. This includes the tools and practices for monitoring user activity, detecting anomalies, and responding to security incidents. It highlights the importance of leveraging Google Cloud's security services and integrating them into the overall security operations workflow.

Steps to Implement and Migrate to BeyondCorp Enterprise

Successful implementation of Google BeyondCorp Enterprise requires the active involvement and collaboration of various stakeholders within the organization. Understanding the roles and responsibilities of these key personas is essential for effective decision-making, coordination, and execution of the project. We will explore the primary personas involved, with a specific focus on the Chief Information Security Officer (CISO) and Workspace Administrator roles.

Step 1: Assessment and Planning

The initial step is to conduct a comprehensive assessment of the organization's existing infrastructure, security controls, and access management processes. This assessment helps identify gaps, potential risks, and areas that need improvement. Key activities include:

- Identifying business-critical applications and their access requirements.
- Assessing the organization's compliance obligations and regulatory considerations.
- Evaluating the existing network architecture and security controls.
- Conducting a risk assessment to identify vulnerabilities and prioritize remediation efforts.
- Defining the migration strategy, including the timeline, resource allocation, and milestones.

Step 2: Designing the BeyondCorp Enterprise Architecture

In this step, organizations design the BeyondCorp Enterprise architecture based on the assessment findings and business requirements. Key activities include:

- Defining the network segmentation and access control model within BeyondCorp Enterprise.
- Establishing trust boundaries and access policies based on user roles, device attributes, and contextual information.
- Determining the integration points with identity providers, such as Google Workspace or Active Directory, to ensure seamless authentication and user provisioning.
- Configuring security policies, including multi-factor authentication, session controls, and encryption mechanisms.
- Designing the logging and monitoring mechanisms to capture and analyze security events.

Step 3: Proof of Concept and Testing

Before implementing BeyondCorp Enterprise across the entire organization, it is recommended to conduct a proof-of-concept program to validate the architecture and test the migration process. Key activities include:

- Selecting a representative set of applications and user groups for the PoC program.
- Configuring the access controls and policies for the PoC environment.
- Conducting user acceptance testing (UAT) to ensure that applications function correctly within the BeyondCorp Enterprise framework.
- Collecting feedback from PoC users and addressing any issues or concerns.

Onix has PoC solutions for BeyondCorp Enterprise available to customers for free or heavily discounted prices based on certain eligibility criteria.

Step 4: User Migration and Onboarding

Once the PoC program is successful, organizations can proceed with the migration of users from the existing VPN or remote access model to BeyondCorp Enterprise. Key activities include:

- Developing a user migration plan, including the sequence and timing of user groups to be migrated.
- Communicating the migration plan to users and providing training and support to familiarize them with the new access workflows.
- Configuring user accounts, access controls, and permissions within BeyondCorp Enterprise.
- Collaborating with application owners to ensure their applications are compatible with BeyondCorp Enterprise and assist with any necessary modifications.
- Conducting a phased migration of user groups, monitoring the process, and addressing any migration-related issues or challenges.

Step 5: Ongoing Management and Optimization

After the migration, organizations must establish processes for the ongoing management and optimization of BeyondCorp Enterprise. Key activities include:

- Monitoring and analyzing security events and logs to detect and respond to threats.
- Conducting regular security assessments and audits to ensure compliance with regulatory requirements.
- Providing ongoing user training and support to address any access-related queries or issues.
- Collecting feedback from users and continuously improving the user experience within BeyondCorp Enterprise.

- Staying up to date with emerging security threats and evolving industry best practices to enhance the security posture.

It is important to note that the implementation and migration process may vary depending on the organization's specific requirements and complexities. Organizations should consider engaging with experienced consultants or experts who specialize in BeyondCorp Enterprise to ensure a smooth and successful implementation.

Conclusion

The migration to Google BeyondCorp Enterprise represents a transformative shift in access management and security for organizations seeking to adopt a zero trust model. By embracing the principles of least privilege and continuous verification, organizations can significantly enhance their security posture, reduce the risk of data breaches, and improve compliance with regulatory frameworks.

Throughout this whitepaper, we have explored the key steps and considerations involved in implementing BeyondCorp Enterprise, focusing on the development of the business case, the personas involved, critical decisions, design considerations, and the steps for implementation and user migration. By following a systematic approach, organizations can successfully transition from traditional VPN-based remote access models to a zero trust architecture.

The development of a strong business case is crucial for securing executive buy-in and obtaining the necessary resources and support for the migration. Understanding the roles and responsibilities of key personas, such as the CISO and Google Workspace Administrator, helps ensure effective collaboration and decision-making throughout the project.

Critical decisions related to architecture design, policy definition, user experience, and compliance must be carefully evaluated to align BeyondCorp Enterprise with the organization's specific needs and objectives. By considering factors such as network segmentation, access control models, and user training, organizations can strike the right balance between security and productivity.

The implementation and migration process involve a series of steps, including assessment and planning, architecture design, developing a PoC and testing, user migration, and ongoing management. By following these steps, organizations can systematically transition users from their existing VPN or remote access models to BeyondCorp Enterprise, while ensuring a smooth user experience and minimizing disruptions.

It is important to emphasize that the migration to BeyondCorp Enterprise is not a one-time project but an ongoing journey. Organizations must continuously monitor, optimize, and adapt their security strategies within the zero trust framework to address evolving threats and maintain compliance with regulatory standards.

As you embark on your own journey towards implementing Google BeyondCorp Enterprise, it is recommended to seek the guidance of experienced consultants or experts who can provide in-depth knowledge and expertise. Their assistance can help ensure a successful migration, maximize the benefits of the zero trust model, and empower your organization to operate in a secure, agile, and compliant manner.

By embracing BeyondCorp Enterprise, organizations can elevate their security posture, enhance user productivity, and confidently navigate the ever-evolving threat landscape of today's digital world. Make the shift to a zero trust architecture and embark on a new era of secure access management with Google BeyondCorp Enterprise.

Onix can assist with all phases of a BCE project starting with a proof of concept to assess the capabilities and merits of the technology to ensure it’s a good fit for the organization. Depending on scope and availability of customer business and technical resources, this PoC can be completed in 4–6 weeks which positions a production migration for the organization within a few months.

Reference Information

Google Cloud. BeyondCorp Enterprise.
https://cloud.google.com/beyondcorp-enterprise

National Institute of Standards and Technology (NIST). Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800–53 Revision 5).
https://doi.org/10.6028/NIST.SP.800–53r5

U.S. Department of Health & Human Services. Health Insurance Portability and Accountability Act (HIPAA).
https://www.hhs.gov/hipaa/index.html

U.S. General Services Administration. FedRAMP Moderate Baseline.
https://www.fedramp.gov/moderate-baseline/

Google Cloud BeyondCorp Remote Access: Designing the Future of Security.
https://cloud.google.com/beyondcorp-remote-access

McKinsey & Company. Cybersecurity.
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cybersecurity

Deloitte. Cyber Risk Services.
https://www2.deloitte.com/global/en/pages/risk/solutions/cyber-risk-services.html

Gartner. (2022). Magic Quadrant for Cloud Access Security Brokers.
https://www.gartner.com/en/documents/4170760/magic-quadrant-for-cloud-access-securit-brokers

Cloud Security Alliance. Cloud Controls Matrix.
https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Open Web Application Security Project (OWASP). OWASP Top Ten Project.
https://owasp.org/www-project-top-ten/

SANS Institute. Critical Security Controls.
https://www.sans.org/critical-security-controls/

National Cybersecurity Center of Excellence (NCCoE). NIST Special Publications.
https://www.nccoe.nist.gov/publication/sp