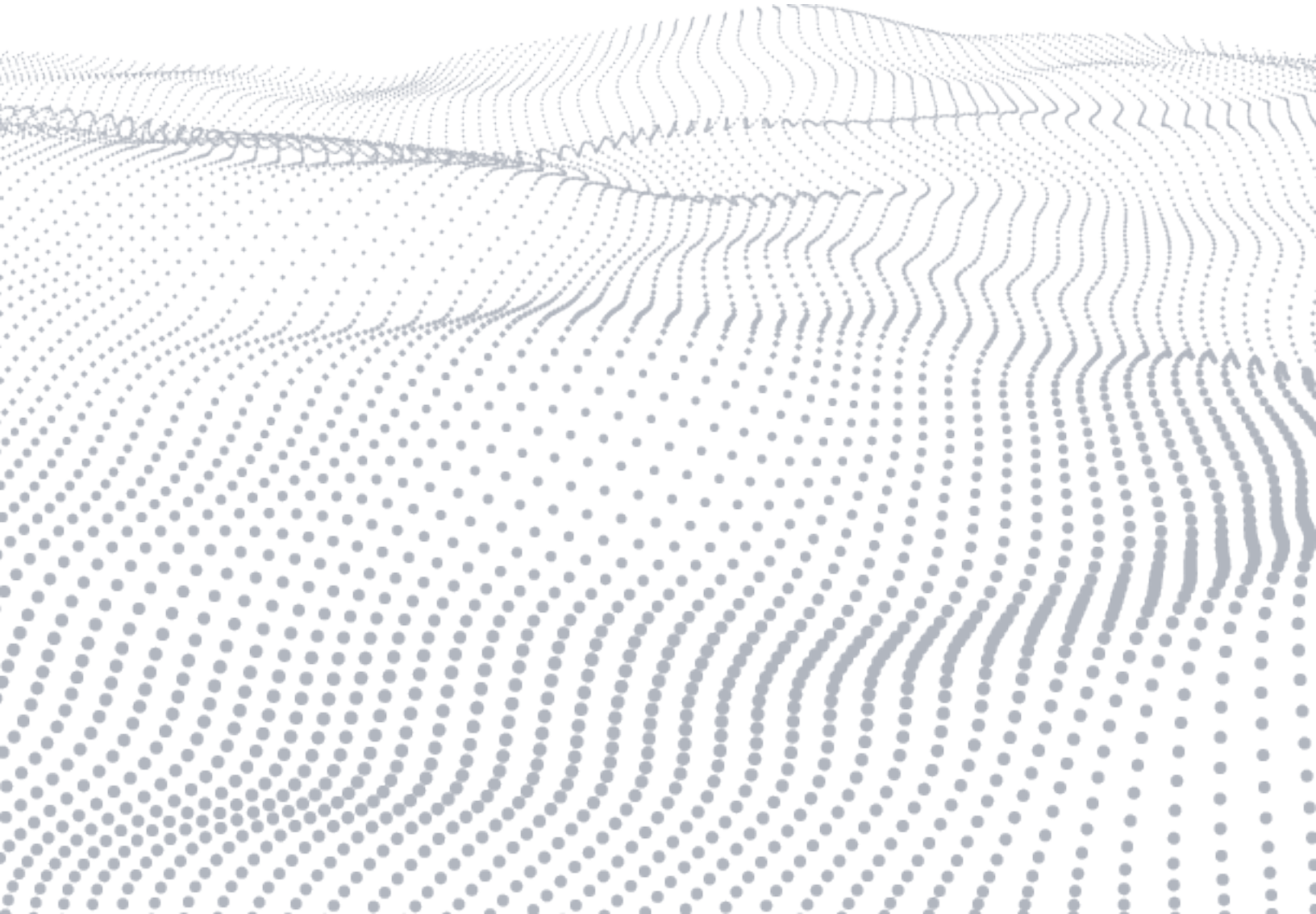
BLACKDUCK®

WHITE PAPER

Building a Comprehensive Multicloud Security Strategy: A Zero-Trust Approach



Introduction

The traditional, perimeter-based security model is no longer sufficient in today's dynamic, multicloud deployments. A zero-trust (ZT) security model, in which no user or system is inherently trusted, is becoming essential—it is a foundational capability that underpins security for multicloud strategies.

The ZT security model operates on the principle of "Never trust. Always verify." In this model, every access request is fully authenticated, authorized, and encrypted before granting access, regardless of the user's location or the network from which the request originates.

This white paper provides an in-depth overview of the essential considerations for building a multicloud security strategy based on zero-trust principles. Three questions about cloud security guide us.

- What cloud-specific security challenges do today's enterprises face?
- How can a zero-trust security model address these security challenges?
- What steps are involved in building a cloud security program using a zero-trust model?

Cloud Security Challenges

As enterprises adopt a cloud-first strategy, it becomes essential to understand the shared-responsibility model offered by cloud service providers (CSP). Each CSP has its own specific shared-responsibility model for architectures where components are hosted on multicloud environments. In this model, clients are fully responsible for specific security aspects, such as data and applications, and CSPs are responsible for physical security. These responsibilities vary from one CSP to another and by service model (SaaS, PaaS, IaaS, etc.). Clients must thoroughly understand the division of responsibilities and the boundaries with their providers.

The security threats and challenges enterprises face today require unique strategies and solutions within their cloud security program. A zero-trust security model can help mitigate many of these challenges by enforcing strict access controls, minimizing attack surfaces, and enhancing visibility into cloud resources. The threats include

- **Data breaches:** These occur in the cloud for various reasons, such as unauthorized access, account hijacking, misconfigurations, or weak security controls, leading to the exposure of sensitive data.
- **Account hijacking:** Attackers gain access to users' cloud services accounts, often through phishing, software vulnerabilities, or credential stuffing, which can lead to unauthorized activities.
- **Ransomware attacks:** These attacks use malware to encrypt a victim's files. The attacker then demands a ransom to restore access to the data.
- **Phishing and social engineering:** Attackers often use phishing and social engineering tactics to deceive users and gain access to cloud resources. Employee training and awareness programs are essential to counter these threats.
- **Cryptomining/cryptojacking:** Attackers can exploit cloud resources for cryptomining or cryptojacking, resulting in performance degradation and increased costs for the organization.
- **Advanced persistent threats (APTs):** Sophisticated and targeted attacks by APT groups can pose significant risks to cloud environments, as they often employ advanced techniques to infiltrate and persist within the targeted infrastructure.
- **Supply chain attacks:** These attacks involve compromising a trusted vendor to gain unauthorized access to their clients' sensitive data or disrupt their operations.
- **Malware attacks:** Malware designed to exploit cloud architectures can result in data breaches or service disruptions.

The challenges include

- **Identity and access management (IAM):** Compromised credentials or weak access controls can allow attackers to gain unauthorized access to cloud resources. Strong IAM policies can prevent such breaches. IAM issues include
  - Weak passwords and authentication: Weak or reused passwords and a lack of multifactor authentication can make it easier for attackers to gain unauthorized access.
  - Insider threats: These can be malicious (employees intending to cause harm) or nonmalicious (employees inadvertently causing security incidents due to lack of awareness or training).
  - Device and endpoint management: Identifying user identity and whether the user's device is registered can be complicated by lack of a centralized view, difficulties in user life cycle management, and keeping application integrations updated.
- **Misconfigurations:** Improper setup of cloud services can leave data unprotected, providing attackers with an easy path to

access sensitive information. Configuration issues include

  - Cloud resource misconfiguration: Cloud-based architectures comprise cloud resources (i.e., Azure) or services (i.e., AWS) that must be securely configured because each misconfiguration contributes to an attack path that can be exploited.
  - API vulnerabilities: APIs are often used to communicate between cloud services. If not secured properly, they can be exploited to gain unauthorized access.
  - Container and serverless security: Lack of proper isolation, insecure images, or misconfigurations can lead to breaches in containerized and serverless environments.

- **Cloud service provider vulnerabilities:** The cloud service provider might have vulnerabilities in its systems, which attackers can exploit to gain access to user data.
- **Insufficient visibility and control:** The dynamic nature of the cloud can lead to a lack of visibility into resources and weak control over data and services.
- **Inadequate training and awareness:** Employees may not follow security best practices without proper training, potentially leading to various security incidents.
- **Compliance:** Organizations must comply with myriad regulations like GDPR, CCPA, and HIPAA. Noncompliance can lead to legal issues and financial penalties.

Each threat and challenge requires a distinct strategy and solution within the cloud security program. A zero-trust security model can help mitigate these challenges by enforcing strict access controls, minimizing attack surfaces, and improving visibility into cloud resources.

How Zero-Trust Addresses Cloud Security Challenges

The zero-trust approach can address many cloud security challenges including data breaches and account hijacking, compliance and regulatory issues, insufficient visibility and control, and inadequate training and awareness. This approach emphasizes strong access controls, malware containment, secure configurations, thorough vetting of third-party vendors, continuous monitoring, secure authentication, and robust incident response strategies. The National Institute of Standards and Technology (NIST) zero-trust model provides an evolving set of cybersecurity protocols that focus on protecting users, assets, and resources.

Data Breaches and Account Hijacking

With the zero-trust approach, every access request is authenticated and authorized, significantly reducing the risk of data breaches and account hijacking. Using multifactor authentication (MFA) and strong identity and access management practices further ensures that only authorized individuals can access sensitive data.

Ransomware and Cloud-Native Malware

The NIST ZT model's continuous validation approach helps mitigate the impact of ransomware and cloud-native malware by verifying the legitimacy of users, devices, and actions. Controlling access to each resource can contain the spread of malware. Regular backups and disaster recovery strategies are essential to recover from such attacks quickly.

Supply Chain Attacks and Cloud Service Provider Vulnerabilities

Thorough vetting of third-party vendors and continuous monitoring of their activities helps mitigate supply chain attacks. In a zero-trust model, every access request from a third-party vendor is authenticated and authorized, providing an extra layer of security. Regular reviews and updates to service-level agreements (SLAs) with cloud providers help address vulnerabilities at the provider level.

Insider Threats

A zero-trust approach combined with user behavior analytics can help detect and mitigate insider threats. By continuously verifying access requests, unusual behavior patterns can be quickly identified and addressed.

Misconfigurations and API Vulnerabilities

The zero-trust model emphasizes the importance of secure configurations and regular configuration audits to help prevent security incidents enabled by misconfigurations. Secure authentication and authorization mechanisms for APIs, combined with vulnerability scanning and penetration testing, can help identify and patch API vulnerabilities.

Container and Serverless Security

Securing containers and serverless architectures with a zero-trust approach involves a combination of identity and access management, network segmentation, and vulnerability scanning to ensure these technologies are configured securely and monitored continuously.

Compliance and Regulatory Issues

The NIST ZT model encourages continuous monitoring and automated compliance checks to ensure that organizations maintain compliance with regulatory standards. Regular audits further ensure compliance requirements are met.

Insufficient Visibility and Control

The zero-trust model emphasizes the need for granular visibility and resource control. This is achieved through centralized logging, monitoring, and cloud security posture management tools.

Inadequate Training and Awareness and Weak Passwords and Authentication

Regular security awareness training and a strong security culture are essential to mitigate the risk of human error. The zero-trust model's emphasis on strong IAM practices, including MFA, helps prevent unauthorized access due to weak passwords and authentication practices.

CLOUD SECURITY CHALLENGES AND HOW TO ADDRESS THEM USING THE ZERO-TRUST APPROACH	
Complexity of Cloud Environments	Employing automated asset discovery and management solutions can help identify all assets and data.
Lack of Security Awareness	Regular training and awareness programs can ensure employees and stakeholders understand security best practices.
Lack of Clear Security Strategy	Developing a comprehensive cloud security strategy aligned with the zero-trust model and business goals can provide a clear roadmap.
Lack of Visibility and Control	Implementing cloud security posture management tools and centralized logging and monitoring solutions enhance visibility and control over cloud environments.
Securing Third-Party Applications	Robust IAM and API security measures can help in securing third-party applications and services.
Data Exfiltration Risks	Implementing strong data protection measures like encryption, and data loss prevention solutions, can mitigate the risk of data leakage.
Account Hijacking and Insider Threats	Regular audits, anomaly detection, and implementing least privilege access can mitigate these risks.
Compliance Complexity	Compliance-as-a-code tools can help automate and simplify compliance with various regulations.
Misconfigurations and Vulnerabilities	Regular vulnerability assessments and configuration audits can help identify and rectify potential weaknesses.
Lack of Integration and Interoperability	Adopting solutions that support integration and developing a unified security architecture can mitigate this challenge.
Scaling and Adapting Security Solutions	Choosing scalable, flexible security solutions and continuous improvement can help organizations adapt to changing threats.

Building a Zero-Trust Cloud Security Program

To build a security program in your organization using a zero-trust security model, you must understand ZT principles. There is no one-size-fits-all way to implement this—every organization is different, and their business objectives are unique. The ZT approach must be built carefully based on business and regulatory compliance requirements. The table below outlines core domains and initiatives for implementing zero-trust security.

DOMAIN	RECOMMENDATIONS
Asset Management	• **Identify data and assets:** Create an inventory of data and assets. Document metadata (tech stack, production/nonproduction environment, etc.) for these assets and determine ownership. • **Classify data and assets:** Identify what data and assets need protection. These could be databases, application servers, or sensitive files that, if compromised, could harm your organization.
Strategic Plan/Processes	• **Understand zero-trust principles:** Start by understanding the core principle of the zero-trust model: "Never trust. Always verify." This principle applies to every component of your organization, irrespective of its location. • **Use policy-based security:** Implement consistent, policy-based security and compliance where possible.
Network Access Management	• **Use microsegmentation:** Segregate the network into smaller, isolated segments. This limits lateral movement and contains attacks within a single segment. • **Implement cross-cloud infrastructure management:** Develop a cloud-agnostic process to manage infrastructure spread over multiple CSPs.
Identity and Access Management	• **Establish user/device identity management:** Implement a unique ID for each user and device. Identify a solution that can support different authentication models used by different CSPs and allows you to define user/service principal accounts, roles/permissions, and access policies, and manage these in a centralized way. • **Enforce a strong password policy:** Enable and enforce a strong password policy. • **Use multifactor authentication for all users:** This adds an extra layer of security, ensuring that even if credentials are compromised, attackers can't gain access easily. • **Implement privileged identity management:** Manage privileged users and break-glass accounts separately from general users. • **Establish a conditional access policy:** Grant access permissions not only by user and device identity, but also by geographical location of device, time of access, etc. to ensure that there is no unusual user access. This can also be extended to service principal's access to cloud resources. • **Enforce least-privilege access:** Limit user access rights, giving them only the privileges they need to perform their tasks. Regularly review and update these privileges. • **Practice vendor management:** Ensure that all third-party vendors adhere to your organization's security standards and can support the zero-trust model.

DOMAIN	RECOMMENDATIONS
Data Protection	• **Use encryption:** Encrypt data both at rest and in transit. This ensures that even if data is intercepted or accessed without authorization, it can't be understood.
Application Security	• **Secure the SDLC:** Ensure applications are developed securely, following the principles of a secure SDLC. Regularly update and patch applications to fix any vulnerabilities. • **Use automation:** Accelerate application deployment and automate application life cycle management.
Continuous Visibility and Incident Response	• **Continuously monitor and log activity:** Implement monitoring tools to continuously observe network traffic and log user activity. This can help identify any suspicious behavior and provide valuable information for incident response. • **Analyze user behavior:** Implement user and entity behavior analytics to identify abnormal behavior or anomalies that could indicate a security incident. • **Use automated response tools:** Utilize security orchestration, automation, and response tools for automated responses to security incidents, speeding up incident response and reducing downtime.
Internal/Third-Party Audit	• **Perform periodic audits and assessments:** Conduct regular audits and assessments to ensure the zero-trust model is working as intended, and identify any areas for improvement.
Security Training	• **Conduct security awareness training:** Regularly train employees on the principles of the zero-trust model, current threats, and safe online behavior. This helps ensure that everyone in the organization understands their role in maintaining security. • **Conduct secure development training:** Train cloud solution architects and developers regularly on security, since the cloud is a fast-growing area and CSPs are offering new services and resources every year. The cloud is an area of innovation, so CSPs are making changes in resource features that may affect architecture design decisions.
Continuous Improvement	• **Track metrics:** Measure process performance using key performance indicators and key risk indicators for risks that need remediation. • **Review/update/upgrade:** The zero-trust model is an ongoing process, not a one-time implementation. Regularly update your security measures based on evolving threats and business needs.

Adopting a zero-trust model is challenging. However, the challenges can be addressed with the right tools, techniques, and mindset. By following the steps we've outlined, organizations can build a comprehensive security program centered on the zero-trust model. It's important to remember that zero-trust is a journey, not a destination—it requires continuous evaluation and adaptation as new threats emerge and business needs evolve. This dynamic approach ensures that your security posture remains resilient and effective, even as the security landscape changes.

Case Study: Zero-Trust Multicloud Security Strategy

Opportunity

Our client, a global financial services firm, was undergoing a massive digital transformation. As part of this initiative, it adopted a multicloud strategy to gain the benefits of best-of-breed services from a variety of cloud providers (AWS, Google Cloud, Azure). However, it quickly realized that managing security across these disparate environments was complex. The traditional, perimeter-based security model needed to be revised, as the perimeter had essentially disappeared. The firm was also subject to strict data protection and privacy regulations. It needed a robust security strategy that could handle the complexity of a multicloud environment while meeting its compliance obligations.

Our Approach

We proposed a multicloud security strategy based on the zero-trust model. This approach included multilayer security controls that ensure defense-in-depth, identity-centric processes, and continuous visibility. It would require that everything trying to connect to its systems would be validated before gaining access—it would not automatically trust anything inside or outside its perimeters. The strategy included

- **Identity and access management:** We established strong IAM controls across all cloud platforms. This ensured that only authorized individuals could access specific resources. Adopting multifactor authentication added a layer of security.
- **Microsegmentation:** In a multicloud environment, network segmentation is complex. We implemented microsegmentation to create secure zones in its cloud environments. This ensured that even if an attacker compromised one part of the system, they could not move laterally to other parts.
- **Encryption:** All data at rest and in transit was encrypted, and key management was handled through a centralized system to ensure consistency and reduce the possibility of key mismanagement.
- **API security:** The client relied heavily on APIs to integrate services across cloud platforms, so we implemented API security measures, including regular scanning for vulnerabilities, and authentication and authorization checks for API calls.
- **Continuous monitoring and security analytics:** We enabled visibility of real-time network and application traffic across all cloud platforms using a unified security information and event management solution. This allowed for quick identification and response to any potential security threats.
- **Automated compliance reporting:** To address the client's regulatory requirements, we implemented a system for automated compliance reporting, including real-time risk assessments and audits.

Value

The shift to a zero-trust security model significantly improved the client's security posture.

- **Enhanced security:** The client reported a significant reduction in security incidents and breaches, as the ZT model effectively mitigated the risk of internal threats and reduced the attack surface.
- **Regulatory compliance:** Implementing automated compliance reporting simplified the process of proving adherence to multiple regulatory frameworks, saving time and reducing the risk of noncompliance penalties.
- **Operational efficiency:** Adopting consistent security controls and automation across all cloud platforms improved operational efficiency by reducing manual tasks and allowing the security team to focus on more-strategic initiatives.
- **Scalability:** The zero-trust model is highly scalable, allowing the client to securely add new services and capabilities to its multicloud environment as its business needs evolve.

The zero-trust model proved an effective solution for the client's multicloud security challenges. It provided a holistic, integrated, and proactive approach to security that was robust enough to handle the complexity of a multicloud environment while meeting regulatory obligations.

Conclusion

Building a comprehensive multicloud security strategy is a complex undertaking that necessitates a zero-trust security model. By addressing each of the considerations outlined, organizations can overcome the challenges associated with multicloud environments, ensure a consistent and unified security posture, and protect their valuable data and applications in the cloud. The zero-trust approach safeguards against current threats and provides a solid foundation for responding to future security challenges in the ever-evolving cloud landscape. Zero-trust is integral to any organization's cybersecurity framework.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.