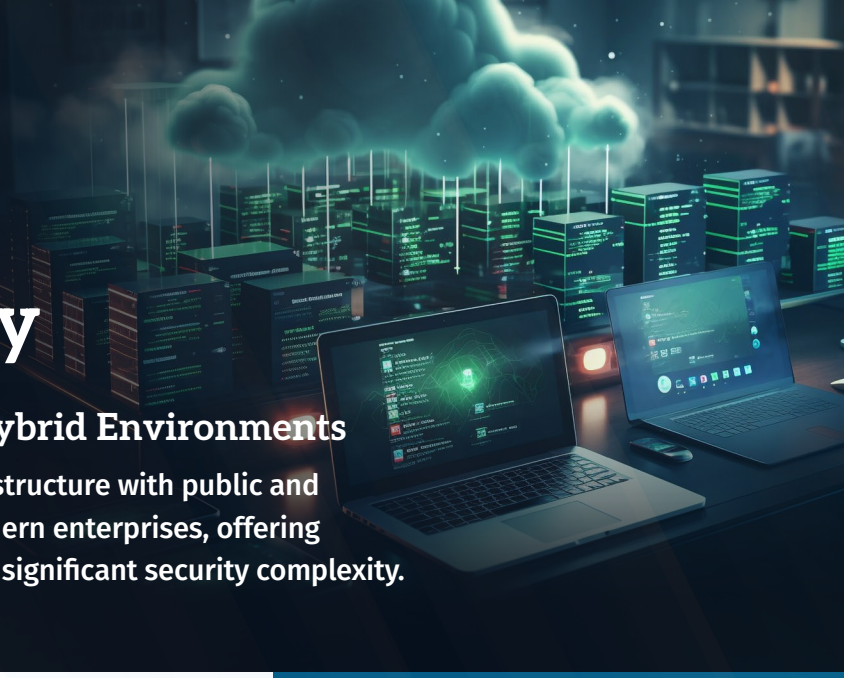
BROADCOM



Executive Summary

Navigating the Challenges of Securing Hybrid Environments

Hybrid IT environments—combining on-premises infrastructure with public and private cloud services—have become standard for modern enterprises, offering flexibility and scalability. However, they also introduce significant security complexity.

Integration and Complexity

Hybrid infrastructures are heterogeneous by nature. Integrating legacy systems with modern cloud-native platforms introduces interoperability challenges and increases the risk of misconfiguration. Fragmented responsibilities between cloud and on-prem teams often lead to inconsistent policy enforcement and delayed incident response.

Use Case: A financial firm implemented a unified endpoint security platform, resulting in a 60% reduction in response time through consistent policies and centralized visibility.

Data Governance and Compliance

Hybrid environments complicate data governance. Organizations must track data across dynamic boundaries and comply with multiple regulatory frameworks. BYOD, mobile access, and SaaS platforms introduce additional challenges for classification, monitoring, and access control.

Use Case: A government contractor implemented a hybrid security architecture that consumed cloud threat intelligence while ensuring sensitive data remained on premises, maintaining both compliance and protection.

Expanded Attack Surface

The hybrid model broadens the attack surface, primarily through endpoints and identities. In 2024, 60% of incidents involved compromised credentials.[1] Attackers exploit trust relationships to pivot laterally across hybrid systems, often undetected due to limitations in security tools.

Use Case: A healthcare organization integrated threat prevention across on-prem and cloud environments, automating detection and response to ransomware threats across both domains.

[1] "Top 10 Identity Attacks in 2024," https://socradar.io/top-10-identity-attacks-in-2024-protecting-credentials

[2] "40+ Cloud Security Statistics You Need to Know in 2024," https://adivi.com/blog/cloud-security-statistics

The Visibility Gap

A lack of visibility is one of the most pressing challenges in hybrid security. In 2024, 85% of organizations experienced a cloud-related security incident, and visibility issues comprise 82% of that majority.[2] Thus, security in hybrid environments requires shifting from perimeter-based models to real-time monitoring and identity- and device-aware access decisions. Organizations must unify their approach to endpoints, networks, and cloud assets while ensuring seamless policy enforcement.

Zero Trust and Endpoint Security

Zero trust architecture (ZTA) and microsegmentation ensure that trust is never assumed, and access is continuously verified. Endpoint protection is central to this model, requiring consistent, real-time threat detection, cloud-managed policies, and offline protection.

Use Case: A utility provider implemented a unified endpoint security platform across IT and OT assets, maintaining operational integrity and cybersecurity standards.

Conclusion

Hybrid environments offer powerful benefits, but also amplify security risks. Visibility, consistent policy enforcement, and real-time threat detection are non-negotiable. Organizations must move beyond traditional security models and embrace unified, adaptive strategies. By implementing zero trust, integrating automation, and reinforcing endpoint security, enterprises can protect their data and infrastructure across the hybrid spectrum.

SANS | Research Program

Best Practices for Hybrid Security

To effectively secure hybrid environments, organizations should:

Adopt Zero Trust principles
that continuously verify access requests based on identity, device posture, and context.

Encrypt and back up data
across all environments to protect against ransomware and accidental loss.

Strengthen identity and access management
using endpoint context and adaptive access policies.

Automate security operations
with AI and SOAR tools to reduce response time and analyst workload.

Conduct regular audits and compliance checks
to ensure alignment with frameworks like FedRAMP, GDPR, and CJIS.