DESIGNING FOR RESILIENCE: LASTPASS PRIORITIZES SECURITY IN MOVE TO CLOUD

CUSTOMER SNAPSHOT

LastPass •••|

INDUSTRY	Technology – Software & Services
CUSTOMER	LastPass provides secure access solutions like credential management and monitoring to consumers and businesses worldwide.
SERVICES PROVIDED	Cloud Penetration Testing

"We didn't just lift and shift. We reinvented LastPass by modernizing our technology, elevating our security posture, and rebuilding a culture grounded in real accountability. Throughout this transformation, we've upheld commitments we've made to customers and, through our partnership with Bishop Fox, validated that our protections can withstand threats against a modern cloud architecture."

— MARIO PLATT, CISO AT LASTPASS

CUSTOMER OVERVIEW

LastPass provides secure access solutions like credential management and monitoring to consumers and businesses worldwide. The company's security model is grounded in architectural separation: customer master passwords and decrypted vault data never reach LastPass-controlled servers. Even in the event of infrastructure compromise, sensitive credentials remain protected by design.

When LastPass separated from its former parent company, the organization faced a defining moment: migrate legacy systems forward or rebuild from the ground up. Leadership chose to reconstruct its technology stack and security functions entirely in AWS, designing a cloud-native architecture intentionally aligned to its security model from day one. The transition introduced greater flexibility and scalability while redefining identity relationships, trust boundaries, and privilege governance across the environment.

THE CHALLENGE

The move to AWS reshaped the operational and risk landscape for LastPass. In a cloud-native environment, identity defines access. IAM relationships, cross-account trust configurations, infrastructure-as-code, and container orchestration controls collectively shape the attack surface. Each introduces operational flexibility, but also potential paths for privilege escalation or lateral movement if misconfigured.

With these changes, LastPass leadership sought independent validation that the architectural decisions made during the rebuild would withstand adversary pressure. That objective centered on the following security priorities.

SECURITY CHALLENGES

- **Containment**: Ensure the AWS design enforced strict blast-radius boundaries in the event of privileged account compromise.
- **Identity and privilege governance**: Manage complex IAM trust relationships and CloudFormation service roles capable of introducing unintended escalation paths.
- **Operational detection confidence**: Verify that malicious activity would generate timely alerts and appropriate response actions under adversary simulation.
- **Control assurance**: Provide independently validated evidence of adversary testing to support customer, auditor, and contractual review processes.

> "Designing the architecture was only the first step.
>
> We needed to see how it would perform under real conditions, knowing the identity and privilege boundaries we defined would shape our risk posture long term."
>
> — **PEDRO CORREIA, DIRECTOR OF PRODUCT SECURITY AT LASTPASS**

THE SOLUTION

Building on a multi-year application testing relationship, LastPass selected Bishop Fox to design and execute an adversary-led cloud penetration test aligned to the architectural priorities of the AWS rebuild. The objective was not to perform a routine assessment but pressure-test identity boundaries, privilege governance, and containment controls under realistic attack conditions.

LastPass chose Bishop Fox for its deep expertise in cloud exploitation, particularly within complex IAM environments where identity relationships, cross-account trust configurations, infrastructure-as-code, and service roles can introduce subtle but high-impact escalation paths. Evaluating these risks requires practitioners who understand not only how cloud architectures are designed, but how they are attacked.

Following collaborative scoping, Bishop Fox and LastPass defined clear goals for the engagement.

GOALS OF THE ENGAGEMENT

- Simulate compromise of a privileged developer account and assess architectural containment
- Identify and attempt to exploit privilege escalation paths within IAM, CloudFormation configurations
- Evaluate cross-account trust relationships and lateral movement controls
- Assess Kubernetes namespace segmentation and CI/CD access boundaries
- Validate detection, alerting, and escalation workflows under adversary simulation

The engagement was designed to complement existing cloud governance initiatives LastPass already had, including alignment with the AWS Well-Architected Framework and participation in the AWS Security Improvement Program. Those initiatives reinforced architectural best practices through structured review and continuous improvement, while the penetration test introduced an adversary's perspective, challenging those controls through active exploitation attempts rather than checklist validation.

"We didn't go to market looking for the cheapest option just to check a box. For something this important, quality and credibility mattered."

— MARIO PLATT, CISO AT LASTPASS

THE OUTCOME

The cloud penetration test demonstrated that the AWS architecture supporting LastPass performed as designed under adversary pressure, while identifying targeted opportunities to further strengthen identity governance and segmentation controls.

Under simulated compromise of a privileged account, escalation within a single AWS account was technically achievable in controlled conditions. However, attempts to extend that access across account boundaries were unsuccessful. This confirmed that the blast-radius controls embedded during the rebuild functioned as intended, while identifying targeted opportunities to further tighten identity and service role governance.

Within containerized workloads, adversary simulation evaluated Kubernetes segmentation and deployment guardrails. Testing identified a namespace-level refinement opportunity that LastPass promptly addressed in collaboration with Bishop Fox to strengthen isolation controls. At the same time, preventative container policies actively restricted high-risk configurations, and simulated malicious activity generated timely security alerts that were escalated through established response workflows.

Collectively, these results provided clarity on where incremental hardening would have the greatest impact and reinforced the architectural discipline underpinning the AWS environment. Most importantly, it validated that security and governance controls hold under realistic attack conditions.

KEY RESULTS

- Identified previously unknown attack paths enabling lateral movement and unauthorized access to PCI data, including decryption of cardholder records due to cryptographic weaknesses
- Eliminated systemic IAM misconfigurations by rebuilding shared server templates used across environments
- Strengthened PCI audit readiness through detailed remediation documentation and improved segmentation enforcement
- Increased customer confidence with clear evidence of risk reduction and corrective action
- Improved credential governance and access controls after demonstrating cross-domain Active Directory pivoting into the production PCI environment

"There's a difference between believing your architecture is sound and watching it hold under pressure. That process gave us confidence and clarity on where to keep strengthening."

— PEDRO CORREIA, DIRECTOR OF PRODUCT SECURITY AT LASTPASS

CONCLUSION

Rebuilding in AWS was a deliberate investment in architectural integrity. By pairing that redesign with adversary-based cloud penetration testing, LastPass ensured that its security model was not only well-constructed but proven under real-world attack conditions.

The engagement reinforced a disciplined approach to identity governance, containment, and continuous improvement, one that scales with the platform and supports the company's long-term security commitments.

For LastPass, validation is not a one-time milestone. It is an ongoing practice, embedded in how the platform grows over time.

The result is a cloud architecture built to scale without compromising the principles that define it: strong separation, enforced boundaries, and security designed to endure.