token | Pixellot

CUSTOMER CASE STUDY

Pixellot secures *Non-Human Identities* at scale with Token Security

ABOUT PIXELLOT

Pixellot is a leading AI-powered sports production company that delivers automated video capture, streaming, and analytics solutions for sports organizations worldwide. Its platform leverages computer vision and artificial intelligence to transform raw video from sports cameras into real-time insights, highlights, and full-game coverage, without the need for human camera operators.

Pixellot operates a cloud-native infrastructure built on AWS, processing massive volumes of video data and analytics workloads. As an early cloud adopter, the company has scaled rapidly and is expanding through acquisitions and building a complex, multi-account cloud environment to support its global operations.

THE CHALLENGE

Securing non-human identities in a *complex cloud environment*

As Pixellot scaled its platform and infrastructure, managing non-human identities (NHIs) such as service accounts, API keys, IAM roles, and machine credentials, became increasingly difficult. Several key challenges emerged:

Massive identity sprawl
Thousands of identities across AWS accounts, with tens of thousands of non-human identities in total

Limited security resources
A lean security team responsible for securing a growing cloud footprint

Complex multi-account environment
Four acquired companies introduced fragmented AWS accounts and inherited identity risks

Legacy access risks
Residual access from former employees, long-lived credentials, and outdated permissions

Privilege escalation paths
Weak separation between development and production environments created potential attack paths

Lack of centralized visibility
Security teams were forced to navigate multiple AWS consoles without a unified view

> *"We had thousands of identities across multiple AWS accounts, but no clear way to understand what mattered most or where our biggest risks were."*

ERAN GUTMAN · CIO; VICE PRESIDENT OF MIS/IT AND CYBERSECURITY OF PIXELLOT

WHAT PIXELLOT NEEDED IN A SOLUTION

Pixellot was looking for a solution that could:

- → Provide **complete visibility** into all non-human identities across their AWS environment
- → **Prioritize risk** and highlight the most critical exposures first
- → Deliver clear **remediation guidance** without requiring deep knowledge of every workload
- → Enable a **small security team** to operate efficiently at scale
- → **Centralize** identity security into a single, unified platform

WHY PIXELLOT CHOSE TOKEN SECURITY

After evaluating Token Security, Pixellot quickly saw value during a hands-on evaluation period. Within a single **two-hour onboarding session**, Token Security provided full visibility into Pixellot's AWS environment and began surfacing critical risks.

Key differentiators included:

Rapid time-to-value
Immediate discovery and prioritization of critical risks.

Identity-centric risk graph
Clear visualization of attack paths and dependencies.

Actionable remediation
Step-by-step fixes without requiring deep system expertise.

Centralized platform
Eliminated the need to navigate multiple cloud consoles.

> *"Within just a couple of hours, we had a clear picture of our environment and where we needed to act. Token Security consistently surfaced the issues that actually mattered to us."*

ERAN GUTMAN

THE SOLUTION

How Token Security solved *Pixellot's challenges*

1 Eliminating Critical Attack Paths

Token Security identified and helped remediate privilege escalation paths between development and production environments.

- Removed attack chains that allowed movement from lower to higher environments
- Strengthened separation between dev and production
- Reduced risk of lateral movement across accounts

2 Cleaning Up Legacy Access and Credentials

Token Security uncovered long-standing security gaps, including:

- Residual access from former DevOps employees
- 5-year-old root user access keys that had never been rotated
- Long-lived, weak credentials across environments

Pixellot systematically eliminated these risks by rotating keys, removing unused access, and enforcing stronger policies.

3 Systematic, Account-by-Account Remediation

Using Token Security's prioritized insights, Pixellot conducted structured cleanup across:

- AWS accounts from acquired companies
- Database environments
- Key vaults and secrets management systems
- Kubernetes orchestration environments

The Token Security platform highlighted unused permissions and trust relationships, enabling precise and safe remediation.

4 Centralizing Identity Security Operations

Token Security replaced fragmented workflows with a single, unified interface:

- Consolidated visibility across all AWS accounts
- Centralized identity and risk prioritization
- Clear mapping of identity dependencies and relationships

> *"Instead of jumping between consoles, we now have one place with Token Security to understand risk, prioritize actions, and fix issues quickly."*
>
> ERAN GUTMAN

RESULTS ACHIEVED WITH TOKEN SECURITY

Pixellot achieved significant security improvements in a short timeframe using the Token Security Platform, including:

2hr	1	60%+	4 to 5
to full AWS visibility	remaining critical finding	of issues resolvable in under a week	month transformation timeline

- **Near elimination of critical risks**: Reduced to just one remaining critical finding 4–5 month transformation timeline
- **Improved environment separation**: Stronger boundaries between development and production
- **Accelerated remediation potential**: Greater than 60% of issues could be resolved in under a week with dedicated effort
- **Eliminated legacy access risks**: Removed outdated credentials and unused permissions

THE VALUE OF THE TOKEN SECURITY PLATFORM

Pixellot continues to realize ongoing value from Token Security:

Fast Integration and Immediate Visibility

- Full AWS visibility achieved in hours
- Rapid discovery of high-risk identities

Clear Prioritization and Risk Context

- Security Posture module surfaces the most critical issues first
- Identity graph highlights real attack paths

Actionable Remediation

- Guided fixes without requiring deep system knowledge
- Enables efficient automated remediation

Operational Efficiency for Small Teams

- Empowers a lean security team to manage large-scale identity environments
- Reduces manual investigation and console switching

“Token Security makes it easy to focus on what's critical and actually fix it. That's been a huge force multiplier for our team.”

ERAN GUTMAN

A STRONG & GROWING PARTNERSHIP

Pixellot and Token Security have built a collaborative partnership focused on continuous security improvements. Through regular working sessions, Pixellot is steadily strengthening its identity security posture while expanding coverage across more non-human identities.

As Pixellot continues to scale its AI-driven platform, Token Security plays a critical role in ensuring that its cloud infrastructure remains secure, resilient, and ready for growth.

To learn more about how Token Security can help you solve Non-Human Identity and AI Agent security challenges, visit:

www.token.security