National Healthcare Provider secures their Office 365 and Salesforce with Palerra

One of the largest national healthcare providers in US needed a robust cloud solution to secure their Office 365 and Salesforce deployments for their more than 5,000 employees across the country. Security of their communication service remains a top priority for the organization as they migrate to cloud services. It enables the organization to streamline operations with partners and vendors, as well as ensure communication privacy between patients and care givers.

ORGANIZATION
Nationwide Healthcare Provider

CHALLENGES
Monitor against external attacks

Monitor against possible insider threats

Secure against tampering of critical service configurations

Simple reports of organization's cloud footprint

Identify cloud service access from unapproved location

SOLUTION
Palerra's LORIC Platform for Office 365 and Salesforce

BENEFITS
Cost savings and efficient IT resourcing

Simplified Regulatory Compliance

Comprehensive and Predictive Security

Complete visibility across multiple cloud services

Single pane of glass alert and management

The Challenge: Finding the right security solution

The healthcare provider migrated from on-premise exchange servers and office applications to cloud services as part of their company-wide cloud adoption strategy. Unfortunately, due to large volume of performance-related helpdesk tickets, they had no other recourse but to follow Microsoft's recommendation and bypass the on-premise Web proxy for Office 365. Having to bypass existing security measures, the organization found themselves in dire need to secure their Office 365 deployment.

The healthcare provider also relied on Salesforce to house patient records as well as other sensitive data. They utilized custom objects extensively with access from various client applications. To secure the use of Salesforce, they defined specific company policies in which users must access Salesforce only from pre-approved locations. However, they lacked the ability to quickly identify access that did not adhere to their guidelines.

Based on their use of Office 365 and Salesforce, the healthcare provider had several key requirements:

- Secure against external attacks/hackers including use of compromised credentials
- Secure against possible insider threats/disgruntled employees
- Detect inadvertent or deliberate changes to critical configurations
- Quickly identify user access that does not adhere to company policy
- Simple reporting capability to address audit requirements

The healthcare provider initially employed a solution from a vendor known for their Shadow IT discovery capability but also offered security for sanctioned apps. Unfortunately, the healthcare provider identified several problems soon after deployment:

CONFIGURATION IT team uncovered a change to Office 365 configuration which bypassed the check for Personal Health Information on outbound emails. Operating in a heavily regulated industry, detection of such change remains a critical requirement for the healthcare provider. Unfortunately, the change was detected during a manual audit and not by the deployed security solution. All aspects of this incident from detection to remediation had to be handled manually.

PERFORMANCE Despite bypassing on-premise proxy, IT team started to again receive high volume of helpdesk tickets due to Office 365 performance. Although the security solution was cloud and API-based, it was also built on proxy architecture. The performance bottleneck had simply moved from organization's on-premise proxy to vendor's cloud infrastructure.

COMPLIANCE Although the security solution provided some insight into Salesforce access, it could not alert the IT team when the access originated from unapproved locations. IT team had to manually identify these scenarios which created a large gap in their ability to meet and document compliance.

VISIBILITY IT team was able to gain insight into select user activities but not application activities. With extensive use of salesforce objects, visibility into which client applications were accessing Salesforce data was critical. Unfortunately, the security solution did not offer the level of detail and visibility needed by the organization.

Unable to resolve these issues and not convinced of the overall threat detection capabilities, the healthcare provider decided to look for a new solution that is better suited to secure their cloud application environment.

> *"We decided to deploy LORIC based on its threat detection capabilities as well as its flexibility to support our unique security requirements."*
>
> *– CISO, Healthcare Provider*

The Solution: Palerra's LORIC platform for Office 365 and Salesforce

The healthcare provider assessed Palerra's LORIC platform as a replacement for their cloud security service. The initial onboarding was complete within a 30-minute meeting and the entire evaluation took less than 2 weeks to complete.

LORIC addressed all the deficiencies of the previous cloud security service as well as other challenges the healthcare provider had been struggling with:

- With LORIC architected to be 100% API-based, user experience was completely transparent with no performance issues.
- Whitelisting capability in LORIC enabled the IT team to easily enforce company policy requiring Salesforce access from approved locations only.
- Real-time dashboard and Key Security Indicators (KSI) enabled IT team to quickly identify the status of their cloud environment including activities from other client applications.
- LORIC, with its threat feeds and User Behavior Analytics, alerted IT team of suspicious activities and threats indicative of compromised credentials as well as access from risky locations.
- IT team was able to create custom alerts to be notified of any changes (inadvertent or deliberate) to critical configurations in their cloud environment.
- Built-in reporting capabilities covering multiple cloud services greatly simplified the task of generating consolidated and correlated report.

Satisfied with the evaluation, the healthcare provider decided to deploy LORIC platform to secure their cloud environment. According to the healthcare provider's CISO, "We decided to deploy LORIC based on its threat detection capabilities as well as its flexibility to support our unique security requirements. We spent a lot of resources to deploy and tailor our Office 365 and Salesforce environment. We needed a solution that complemented our environment and make it secure."

The Benefits: Advance Security, Cost Savings and Meeting Compliance

The business benefit of the LORIC platform included:

EFFICIENT USE OF IT RESOURCES With Office 365 performance-related issues completely resolved and LORIC continuously monitoring Salesforce environment including access by client apps, the healthcare provider was able to redistribute their IT resources. From as many as 10 administrators dedicated to supporting Office 365 and Salesforce, all the tasks are now managed by two administrators on a part-time basis.

SIMPLIFIED REGULATORY COMPLIANCE Several features in LORIC enabled the healthcare provider to address their compliance requirements. By creating custom policies, the organization was able to tailor alerts to specific activities, enabling the team to quickly address incidents before it can cause compliance issues. The built-in reports also enabled simple view of the organization's entire cloud environment.

PREDICTIVE SECURITY An unexpected benefit of the LORIC platform was its ability to offer predictive security. With continuous user behavior analysis, LORIC was able to alert IT administrators of users who were prime candidates for phishing and other attacks. By educating the users, the organization improved their overall security posture and likely avoided being the target of many attacks.

MULTI-CLOUD SERVICE VISIBILITY Already leveraging Office 365 and Salesforce with plans to adopt additional cloud services, LORIC's capability to provide security across multiple apps have proven invaluable. The IT team was able to easily identify several risky and non-compliant activities from select employees across multiple cloud applications.

In addition to addressing all of the healthcare provider's requirements, LORIC immediately paid for itself by detecting a routing configuration change that had previously gone unnoticed. The inadvertent change had routed the organization's emails to a gateway in another country. Routing of sensitive and private data outside the US could have resulted in HIPAA violations & financial penalties. LORIC was able to alert the IT team in time to avoid such consequences.