ANOMALIX

ANOMALIX
CASE STUDY

Okta

Okta

Background – Large Energy Company

Anomalix was selected by a Large Energy company to provide a Workforce Identity solution that would protect and enable employees, contractors, and partners.
Anomalix helped the customer review the options, and chose the Okta Identity Cloud to provide the following services:

1. Single Sign-on (SSO)
2. Adaptive Multi-Factor Authentication (MFA)
3. Universal Directory
4. Lifecycle Management

The customer has around 15,000 employees that access upwards of 15 mission critical applications both hosted on-premise and cloud based. End users would have to log into many of the applications by going to separate login portals and using different sets of credentials for each app. This put a strain on the IT helpdesk due to the sheer number of password reset tickets that were generated on a daily basis due to users having to remember multiple sets of usernames/passwords for each app. With no real central authoritative source, provisioning of user access was manual, painfully slow, and prone to errors.

Also, there was no type of universally enforced Multi-Factor Authentication in place, which exposed them to the dangers of stolen credentials or weak passwords.

How We Helped

Anomalix worked with the Large Energy company to onboard their applications into Okta to enable SSO across the organization. Multiple Okta AD agents were installed and configured. An Okta IWA server was also setup which enabled Desktop SSO. This enables any domain user logged into an on-premise domain-joined computer with his or her credentials would be seamlessly logged into their assigned applications provisioned in Okta, thus eliminating the need for multiple credentials for end users. MFA was then activated for remote access users, using SMS and Okta verification. Universal Directory was also put in place and integrated with their existed AD Domain to serve as a central Identity source for all employees. A strong password policy was also put in place to further protect accounts from being compromised. The newly built Universal Directory enabled Lifecycle Management, greatly speeding up the provisioning process, while reducing errors through automation.

Conclusion

End result and Benefits

- Password reset tickets were greatly reduced which reduced strain on the IT Helpdesk
- Streamlined process for end-user application access
- Increased security by enabling MFA, reducing exposure and eliminating well-known attacks such as password spraying
- Reduced the risks associated with stolen credentials by using adaptive MFA to require multiple factors when assessing the risk of a user login
- Established a central Identity store by integrating with their existing AD infrastructure using Universal Directory
- Onboarded over 100 applications into Okta
- Automated user provisioning, creating a faster and more accurate turnaround for end users and reducing the load on IT administrators

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144