

CA Technologies maximizes productivity and minimizes risk with effective identity management

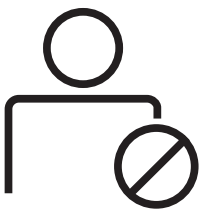
CLIENT PROFILE

Client Profile

Industry: IT

Company: CA Technologies

Employees: 12,000



70%

reduction in entitlements



4,000

resources secured with
CA Privileged Access Manager

Managing evolving access rights in a digital age

Enabling people to work faster and smarter while securing data is one of the greatest challenges of the digital age. And the scope and scale of the challenge keeps changing as teams, systems and privileges evolve.

"It's a delicate balancing act," explains Robert Primm, Director of Cyber Security at CA Technologies. "We need to ensure the right people are granted the right access at the right time across both on-premise and off-premise resources."

By utilizing its own Identity Management Portfolio, CA Technologies has enabled a step-change in how it grants, controls and revokes privileges to more than 1,000 users across 4,000 resources. "By strengthening and simplifying identity and access management, we have removed risk while also increasing agility and productivity," said Primm.

Reducing and controlling user privileges

Like many companies, CA Technologies applies a 'least privilege' rule to governing access to key IT assets, such as servers, networks and applications. To work effectively, this approach requires robust controls and seamless processes throughout the identity and access management lifecycle.

"As an IT administrator or power user progresses their career, they can amass privileges that exceed the remit of their role. If their credentials were stolen, this could expose a company to increased risk," comments Primm.

With CA Privileged Access Manager, CA Technologies can take a more consistent and controlled approach. For example, privileges are no longer issued for a single IT asset but for a business service, which has reduced the entitlement base from 200,000 to 60,000.

Regular reviews enable the cyber security team to identify and revoke any inactive privileges, which has contributed to superfluous rights being withdrawn from more than 400 users.

Enabling self-service and automation

Preventing unauthorized access, however, is just one piece of the identity and access management puzzle. CA Technologies also needs to ensure its people are empowered to work as productively as possible. And that means responding to new privilege requests efficiently.

"With CA Privileged Access Manager, we can automate key steps in the security value chain while safeguarding critical IT assets and datasets," said Primm.

"The CA Identity Management Portfolio enables us to empower our people by opening up the right doors and closing down potential threats."

Robert Primm

Director of Cyber Security,
CA Technologies

CA Technologies also plans to use the solution to establish a self-service portal for users to log and track their access requests.

"By granting new privileges in hours instead of days, we will be able to increase user productivity and satisfaction – especially when on-boarding new employees," said Primm. The identity portal will also provide a valuable audit trail of access rights per IT asset to support compliance efforts.

Multi-layer protection aids prevention

As part of its identity and access management framework, CA Technologies also uses multi-factor authentication. Privileged users authenticate with one-time passwords, which are generated by CA Advanced Authentication.

By combining this with threat analytics, Primm and his team can detect abnormal access by users and take immediate action. "With CA Advanced Authentication, we can do more than just protect core business and IT assets; we can prevent potential breaches," he said.

CA Advanced Authentication and CA Privileged Access Manager are just two of the Identity Management solutions being used by the cyber security team at CA Technologies. "Security needs to be strong but also simple; it needs to help not hinder the user. Deploying an integrated portfolio reduces both cost and complexity," explained Primm.

By taking a preventative and proactive approach to identity and access management, CA Technologies can safeguard security without compromising the user experience.

"To develop, sell and support our software, our employees need fast and secure access to different resources. The CA Identity Management Portfolio enables us to empower our people by opening up the right doors and closing down potential threats," said Primm.

Leveraging the CA Identity Management Portfolio, the security team is also currently working towards achieving a NIST (National Institute of Standards and Technology) Security Framework rating of 3.5.

For more information, please visit ca.com



CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

Connect with CA Technologies



Copyright © 2018 CA. All rights reserved. All trademarks referenced herein belong to their respective companies. This document does not contain any warranties and is provided for informational purposes only.

Any functionality descriptions may be unique to the customers depicted herein and actual product performance may vary.

CS200-346514_0418