COCA-COLA EUROPACIFIC PARTNERS

CASE STUDY

CYBERARK®

Company: Coca-Cola Europacific Partners

Coca-Cola Europacific Partners was formed in May 2021 by Coca-Cola European Partners' acquisition of bottling company Coca-Cola Amatil. The entity is the world's largest independent Coca-Cola bottler, based on net revenues. In addition to Coca-Cola beverages, brands include Diet Coke, Fanta and Sprite, as well as an extensive range of hydration and ready-to-drink coffees, teas and juices.

Industry: Manufacturing

Annual Revenue: €13.5bn (US$15.6 billion)

Employees: 33,000

CyberArk Product & Services:
CyberArk Privileged Access Manager Self-Hosted

"One measure of the effectiveness of CyberArk is that we now know how every privileged account is being used and there has been a dramatic drop in the opportunity for someone to inflict damage to our environment."

Mukesh Kapadia
Global Deputy Chief Information Security Officer
CCEP

Coca-Cola Europacific Partners Steps Closer to Becoming the World's Most Digitized Bottling Operation with CyberArk

One of the most recognizable brands on the planet, Coca-Cola Europacific Partners (CCEP) is the largest bottler and distributor for Coca-Cola and associated beverages in Europe and the Asia Pacific region. A major aspiration for CCEP is to be the world's most digitized bottler. The company has launched multiple initiatives in pursuit of this objective, such as MyCCA.com for managing retailer partnerships.

While digitization is increasing efficiency and significantly growing customer engagement, it also comes with several challenges, not least being the growing risk of cyberattacks.

This led the company's Australian, Pacific and Indonesian operation (CCEP API) to create a three-year roadmap for developing and implementing enhanced security measures. A key element of the plan has been to improve existing privileged access management processes and gain heightened oversight and control over the use of elevated credentials.

PRIVILEGED ACCESS MANAGEMENT IS CRITICAL FOR MITIGATING RISK

Mukesh Kapadia, global deputy chief information security officer for CCEP, said, "Privileged access management is key for any organization wanting to protect systems and data. We needed to make sure we could implement enhanced control over access requests and provision them in a 'just-in-time' manner to reduce opportunities for abuse. The plan focuses on mitigating the risk of both unintentional and malicious harm."

Reinforcing compliance to standards such as PCI DSS (Payment Card Industry Data Security Standard) and adherence to the NIST (National Institute of Standards and Technology) framework were also important drivers for change.

To select the optimal privileged access management solution, CCEP API brought together stakeholders to ensure cross-business alignment and streamline adoption once the new solution was selected.

KEY BENEFITS

- Defends against modern threats and advanced attacks
- Provides 360-degree oversight of privileged access management
- Replaces manual, trust-based practices with rigorous, automated security processes
- Increases efficiency and reduces time and resources needed to manage privileged access
- Ease of integration with existing technology stack components
- Satisfy audit and compliance with standards like PCI DSS and NIST
- Sets the standard for global, group-wide privileged access management

SOLUTION

- Coca-Cola Europacific Partners API has used CyberArk to build a comprehensive and robust privileged access management solution that delivers complete oversight and increases protection against attacks.

CyberArk was one of a small number of vendors invited to provide in-depth proposals and, after receiving high scores in all evaluation criteria, was subsequently selected as the solution of choice. Additional factors included CyberArk's global operations being coupled with a very strong local presence. The decision was further validated through conversations with other customers and CyberArk's endorsement and prominent positioning by industry analysts.

CCEP API rolled out CyberArk Privileged Access Manager Self-Hosted – a hybrid on-premises and cloud solution that utilizes Microsoft Azure and other cloud services such as Amazon Web Services (AWS) and Google Cloud Platform. One important feature was how the CyberArk solution tightly integrates with complementary security tools – for CCEP API, this included SailPoint and Qualys – to enable developers to create seamless protection across multiple attack vectors.

CCEP API managed the implementation with support from CyberArk to help ensure that best practice guidelines, as defined by the CyberArk Blueprint methodology, were followed. CyberArk auto-discovery DNA scans were leveraged to support the deployment, and despite being at the peak of the COVID-19 pandemic lockdown, protection was quickly rolled out to several hundred admin accounts and almost 1,000 local admin accounts throughout the CCEP API region.

CYBERARK IS SIMPLE, ADDRESSES RISK QUICKLY

CyberArk has enabled CCEP API to build a solution that delivers a 360-degree view of privileged access activities and, more importantly, create a robust defense against attack.

Kapadia commented, "One measure of the effectiveness of CyberArk is that we now know how every privileged account is being used and there has been a dramatic drop in the opportunity for someone to inflict damage to our environment. Previously privileged access was done on a best-efforts basis with manual reviews and relied on trust. Now it is based on facts. We know if someone wants to make a change and the ensuing control process is strictly governed by a disciplined set of rules."

CCEP API used to have a decentralized infrastructure where people in different countries had the same level of access. CyberArk has limited the number of users with privileged access and when needed, enforces a consistent way of provisioning. This makes processes more repeatable and predictable, and in keeping with group practice and policy. Having better control and visibility to ensure adherence to standards like PCI has resulted in improved audit performance. These advances also take less time to track down items like ticket references, documents, and procedures.

Andy Chambers, information security architect for CCEP API, added, “Because of the inherent simplicity of CyberArk and the intuitive interface, we can action projects on our own and address risk very quickly. The support and online documentation make it really easy to be self-sufficient.”

“The local CyberArk team is very professional and knows the products inside out.,” said Andrew Ko, security program manager CCEP API. “Every time we reach out, the team knows intuitively what needs to happen. We never have to wait for a response: this has been directly helpful in speeding up the implementation.”

“The local CyberArk team is very professional and knows the products inside out. Every time we reach out, the team knows intuitively what needs to happen. We never have to wait for a response: this has been directly helpful in speeding up the implementation.”

Andrew Ko
Security Program Manager
CCEP API

CYBERARK DRIVES EFFICIENCY

“Deploying CyberArk means there are no gaps or inconsistencies in our approval process because we now have a common way of provisioning privileged access. That is a very important step forward because not only is it more secure, but it drives efficiencies,” outlined Kapadia. “It’s much less of a burden and far more flexible because we don’t have to reach out to ten different people to hear how each of them performs their process.”

Now other business units within the CCEP organization have seen what CCEP API has achieved and are anxious to replicate the successes in their own environments. Over the next year or so, Kapadia and his team are set to lead the expanded CyberArk implementation across the whole group.