CASE STUDY

Mitigating Insider Risk at Leading Telecommunication Operator

Safeguard for Privileged Sessions

As a semi-government organization, the Cyprus Telecommunications Authority (CYTA) is the incumbent telecom operator in Cyprus. It was established with the aim of providing, maintaining and developing a comprehensive telecommunications service, both nationally and internationally. CYTA is considered to be the leading provider of integrated electronic communications services in Cyprus. It owns and operates a nationwide fixed and mobile network and provides a broad range of services for the consumer and business sectors including fixed and mobile telephony, fixed and mobile broadband Internet access, IPTV and other multimedia services, data center hosting and cloud services.

Learn more

- Safeguard homepage
- Request callback

The Challenge

Like most major telecommunication operators, CYTA's operation is also characterized by strict data security measures. The protection of customers' personal data, such as Call Detail Records (CDRs), from insider threats was particularly important for CYTA.

In addition, new internal security policies were introduced which mandated the monitoring of user access to internal systems storing the customer data. To minimize the risk of insider threats, CYTA searched for a solution which could meet the following criteria:

- ✓ Able to monitor and record all privileged access to remote systems which store customers' personal data
- ✓ Provides visibility into encrypted communication channels (such as SSH and RDP) used by administrators accessing data servers

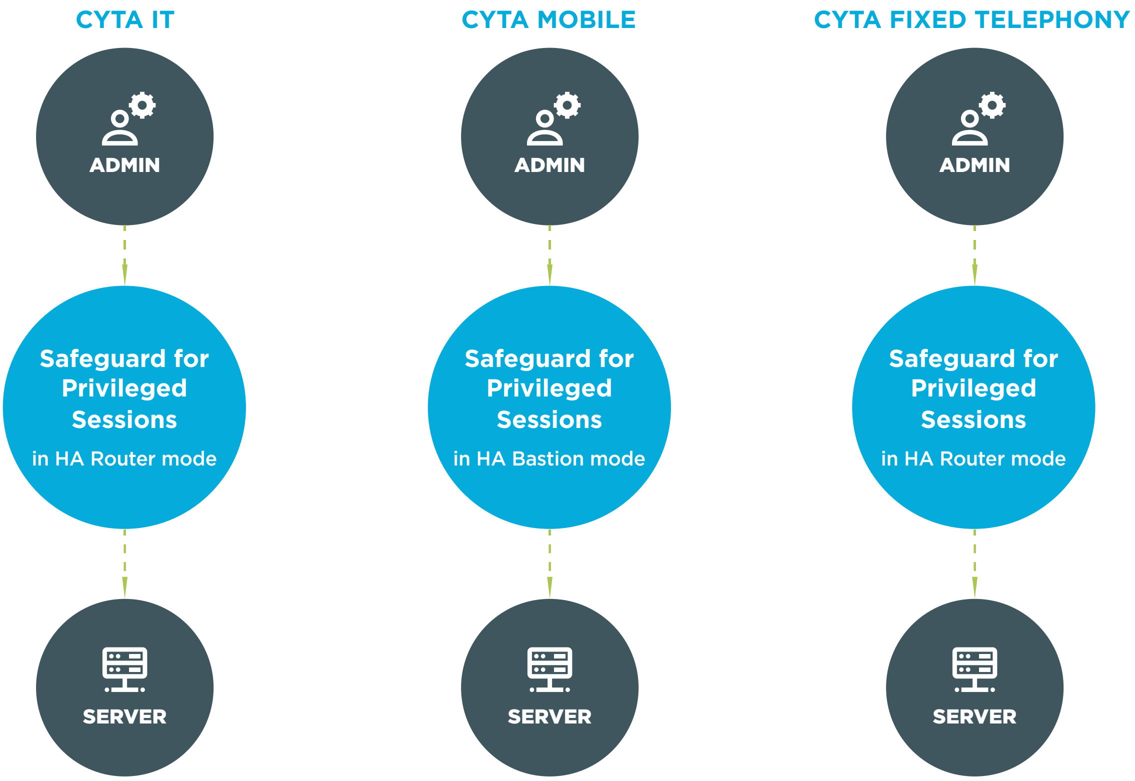
The Solution

To meet the above requirements, CYTA chose One Identity's Safeguard for Privileged Sessions appliance (Safeguard for Privileged Sessions).

"We directly selected this system because it was the only solution which could decrypt and monitor multiple communication protocols such as SSH and RDP" – explains Charalambos Charalambous, Security Engineer at CYTA.

The Safeguard for Privileged Sessions system has been in productive operations at CYTA. The solution consists of three high availability clusters (six appliances in total) located in three locations. The solution controls access of around 30 system administrators and protects 15 server hosts. The implementation took around 2 weeks.

> "ONE IDENTITY'S SAFEGUARD FOR PRIVILEGED SESSIONS IS A RELIABLE AND FEATURE-RICH PRODUCT THAT HELPS THE SECURITY DEPARTMENT TO ENFORCE INTERNAL POLICIES AND MINIMIZE THE RISK OF FRAUD..."
>
> – Charalambos Charalambous, Security Engineer, CYTA.



High availability Safeguard for Privileged Sessions clusters in three data centers at CYTA

Benefits

Since implementing the One Identity Safeguard for Privileged Sessions solution, CYTA has gained visibility into encrypted network traffic of privileged users who access systems storing customers' personal data. Safeguard for Privileged Sessions has proved to be an effective deterrent against internal fraud.

The ability to search for specific strings in user's activity and to watch all activity that has taken place on the servers as a video is a particularly useful feature of Safeguard for Privileged Sessions.

"Since we have been using the One Identity solution, we've experienced a reliable and feature-rich product that helps the security department to enforce internal policies and minimize the risk of fraud and other insider threats. That's why we are extending the One Identity solution for the next 5 years by upgrading both the hardware and software to the latest versions," – concludes Charalambous.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com