Kron TECHNOLOGIES

CASE STUDY

A Large IT Consulting and Managed Services Company from North America chooses Kron to secure remote access to manage their customer ecosystem

Company Overview

- Founded in the 1990's
- 250+ Engineers
- Two 24/7 Operation Centers
- Named in 2020's Google Cloud Industry Solutions Partner of the Year for the Public Sector

The company is an IT consulting company with a unique company culture. Harnessing their experience of 20+ years in integration, cloud, cybersecurity, DevOps, and network, the company strives to be the best without sacrificing quality and integrity. It has more than 250 talented and expert engineers and two 24/7 operation centers.

Challenges

Access to customer systems requires tamper-proof reporting of all activities

The company uses the TACACS+ and SSH protocols to manage access control and privileges for changing network device configurations. Such critical responsibility weighed heavily on the company admins as they had to perform highly critical access management tasks when connecting to customer sites securely. Because the company admins work in customer environments, customers rightly want to know who, when, and why the company admins connected to their systems and what they did. From the slightest to the most significant, any changes in the customer's systems can stir up trouble unless both parties are able to present concrete evidence.

To empower their customers' security posture, the company needed a solution to prevent any manner of malicious usages.

The company needed a solution that supported TACACS+ and SSH protocols, eliminated unsupervised access and configuration changes on network devices, recorded and managed all activities based on least privilege principles, and generated reports for audit purposes. The company also needed a secure VPN-less solution, when connecting to customer devices in different locations and data centers.

Providing services to all customers on the same platform

Before Cisco announced the end-of-life for Cisco ACS, the company used it to manage TACACS+ devices. They were looking for other options as they didn't want to upgrade to Cisco ICE. In addition to the desired technical qualifications, it would make things a lot easier if they could find a solution to provide their services securely to different customers on the same platform.

Securing DevOps automation

The company employs Ansible, on which they developed automation scripts using various DevOps processes to manage customers' systems fast and detection-free. Authorized users connect to the customer devices for installation and configuration purposes. Therefore, they needed a PAM tool to secure this process with minimum or no extra work. They needed to retrieve the required credentials from the password vault, log all-access, and most importantly, allow privileged users to execute only the permitted commands.

Solution

Kron offered it's Multitenant PAM solution

Multitenant PAM allows defining customers as tenants and enables the company admins to securely access both customer devices and their own devices from a single platform.

The company also adopted the Tenant Connector and Direct Access Management (PAM solution for network elements supporting the TACACS+ protocol) modules. To end their search for a secure VPN-less solution, Kron helped by running the Tenant Connector module on the Multitenant PAM platform, reducing VPN costs without compromising security.

Logging all activities and the managerial approval mechanism improved the company's security posture.

The company now records all activities, configuration changes – each keystroke – as searchable log records, which allows them to answer where, when, who, and what questions regarding user activities. Kron's PAM solution also allows managing access control to devices through the approval of managers or customers.

The company managed the automation of SSH devices with various DevOps tools (Ansible Tower) and using multiple scripts. They wanted to maintain this structure while adding a security layer with a PAM system that supports DevOps automation and ensures secure access. In other words, they needed Kron's Multitenant Session Manager module. By using the Session Manager's SSH Proxy, users can use credentials from the password safe without exposing the password when connecting through Ansible automation. All sessions are now managed based on least privilege principles, video recorded for audit purposes, and are kept tamper-proof.

Result

The company provides IT managed services to its customers using a variety of technologies. Kron supported the company through a flexible and easy to integrate PAM solution that supports all technologies that the company avails itself of.

Thanks to Kron's Multitenant PAM solution, all its processes are now secure, traceable, reportable, configurable, and easy to manage from a single platform, while managing different tenants for each customer. The Multitenant module's unique ability to enable accessing multiple tenant devices simultaneously (On behalf Of Management) made life easier and much more productive for the company admins.