SECUREITSOURCE

CASE STUDY

CYBERARK®

Delivery Partner: SecureITsource

SecureITsource was founded with the goal of raising the bar and changing the status quo in Identity Management Consulting and Professional Services.

Client: Confidential

Industry: Consumer Financial Industry

Employees: 10,000+

CyberArk Product & Services:
Endpoint Privilege Manager

Reduce the Risk of Attackers Gaining Access to Critical Systems, Implement Least Privilege.

A Frictionless Approach to Endpoint Protection

EXECUTIVE SUMMARY

A Financial Institution overwhelmed with the administrative privileges sprawled across their end-user environment needed a solution which would reduce the attack surface these network entry points exposed without affecting the strict Service Level Agreement's (SLA's) they have with their customers.

SecureITsource partnered with the institution to implement CyberArk's Endpoint Privilege Manager solution to take control of the privilege issue while allowing end-users to stay productive.

CHALLENGES

With thousands of applications in use, the company's immediate need was to remove local administrative rights from end-user machines. This was necessary to prevent end-users from granting themselves privileged access to applications they hadn't been authorized to use.. Since both Windows and Mac computers were being used to access applications, they needed a solution that would account for both operating systems.

Beyond reducing insider risk, the lack of controls around local privilege management could also make it easy for attackers to establish a foothold in the company through these machines, escalate privileges and move laterally across the environment until a jackpot of data is discovered that can be exfiltrated outside of the network.

To add to this, the institution needed to implement a simple process for their users to request access to the applications they may have had unrestricted access to previously, but are now being restricted by the solution. The goal was to keep the users with the minimum rights they needed to do their day to day tasks.

KEY BENEFITS

- Provide a critical layer of protection when an attack evades traditional perimeter and endpoint security controls
- A unique combination of technologies, to protect against, block and contain attacks on the endpoint, reducing potential damage to the business
- Strengthen the protection and detection capabilities of your existing endpoint security
- Enables the desktop team to easily implement security policy, with minimal impact on the business
- Prevents users installing unsanctioned applications and causing workstation instability, resulting helpdesk calls and increased support costs
- Enables removal of business users with local administrator rights without reduced user productivity and increased helpdesk calls
- Secure and rotate local administrator password regardless of endpoint location
- Easy deployment with automated policy creation, and OOTB policy templates eases the burden on the desktop IT team and standalone agent enables support on airgap networks
- Helps the desktop team to meet the requirements of the security / risk management team while reducing their workload

HOW SECUREITSOURCE HELPED

SecureITsource analyzed the company's requirements and recommended CyberArk Endpoint Privilege Manager as the solution of choice. After reviewing the functionality of CyberArk, the company realized that beyond controlling privilege escalation, the detailed device and application inventories would be a large improvement to their security operations.

During the implementation, the company's security engineers found that the Endpoint Privilege Manager's "monitor-only" mode was crucial to the project's success as they were able to deploy the solution into production while simultaneously testing policies. This allowed SecureITsource and the company to test the impact of the access policies without affecting anything in the environment, ultimately releasing a production-tested solution in a short time frame.

SecureITsource utilized its understanding of the CyberArk solution as well as role-based access control (RBAC) to design access policies for standard users, developers, desktop support users, and more. This granted the correct user's access to the applications they needed on day one and reduced the need for users to request access overall.

Moreover, SecureITsource worked to integrate Endpoint Privilege Manager with the company's existing SIEM solution – delivering another boost to the company's security operations by providing details logs and metrics of privileged activity throughout the organization.

RESULTS AND FUTURE PLANS

In three short months, SecureITsource completely removed local administrative rights from all the company's user-facing endpoints with minimal impact. The solution resulted in reduced calls to the helpdesk and the company was able to use the access policies SecureITsource established to continuously improve and adapt their policies going forward.

The company now has visibility into all their applications, something they did not have before, and are able to utilize that information to make policy decisions. With the solution deployed, the company hopes to continue using CyberArk to improve their advanced threat protection by implementing features like credential theft detection and blocking.