Improving Business Focus, While Reducing Risk of Privileged Account Breach

CUSTOMER: A national provider of integrated clinical solutions for healthcare facilities.

CHALLENGES

- The security team had previously implemented a Privileged Access Management solution (CyberArk), to meet HIPAA compliance, but complete integration with critical infrastructure components had not happened due to competing priorities.
- The security team did not have sufficient expertise and available resources to expand the implementation, therefore leaving critical infrastructure elements unprotected and compliance requirements unmet.
- The security team was concerned about ongoing maintenance of the solution – new users, new applications and infrastructure elements, upgrades – given the lack of expertise in the team.
- Security leadership is concerned that they are not getting a return on the financial investment in the privileged access management solution and at risk for potential fines related to failing compliance audits.
- Security leadership is concerned that they are not getting a return on the financial investment in the privileged access management solution and at risk for potential fines related to failing compliance audits.

SOLUTION

- Optiv's team of certified CyberArk experts can provide privileged access management leveraging a state-of-the-art platform to monitor the solution 24X7X365 to detect, respond and recover from an incident.
- Leverage Optiv team to expand implementation and integration into environment to ensure that all critical application and infrastructure elements are protected, reducing the risk of a failed compliance audit.
- Rely on the Optiv team to deliver device health and performance monitoring, alerting and reporting, as well as upgrades, patches and ongoing maintenance to ensure maintained level of security and adequate return on investment in technology.
- Lean on Optiv's experience and expertise to help the security team consolidate its massive portfolio of security tools and outline a strategy for appropriately using resources.

RESULTS

Security leadership is no longer concerned about the risk of a breach related to privileged accounts and can be confident the organization is in compliance.

Security leadership has a **strategy for a critical element of their security infrastructure**, effectively reducing risk, and optimizing operations to ensure proper infrastructure management and long-term risk minimization.

The security **team feels confident that their privileged access solution is being monitored, maintained** and is retaining the appropriate security posture and ability to respond in the event of an incident.

The security team can **focus efforts on high priority issues and business objectives**, rather than tactical tool management.

With ongoing security measurement in place, the **security team is able to convey easy-to-understand metrics to the executive leadership team and board members**, enhancing communication between the two groups and elevating the security team's role in business strategy.

1144 15th Street, Suite 2900
Denver, CO 80202
800.574.0896 | optiv.com