CleanSlate

CASE STUDY

AUTOMATE YOUR PATCHING WORKLOAD WITH **RED HAT ANSIBLE**

CLARITY IN TECHNOLOGY

CleanSlate

CLARITY IN TECHNOLOGY

CLIENT **OVERVIEW:**
The Client is one of the largest U.S. manufacturers of residential and commercial consumer goods. It is a division of a larger corporation and manufactures three well-known brands. The company invests in ways to manufacture innovative solutions that increase functionality, while also utilizing improved manufacturing processes to reduce their ecological footprint.

GO **LIVE:** February 2020

CLIENT **PROFILE:**

LOCATION:
Indianapolis, Indiana

EMPLOYEES:
2,000 +

INDUSTRY:
Consumer Goods

SOLUTIONS:
Red Hat Ansible Tower

CASE STUDY: **AUTOMATE YOUR PATCHING WORKLOAD WITH RED HAT ANSIBLE**

CHALLENGE:
The client has hundreds of virtual machines in its data center that require constant care and feeding. Managing the application of security patches is a time-consuming process. There is a lot of demand creating a heavy workload on the IT staff. Due to this challenge, patching had taken a backseat. The client was looking for a way to automate this workload to save on time and resources.

SOLUTION:
The client chose CleanSlate because we had a preexisting relationship and the skills to get the job done. They trusted CleanSlate to take their solution to the next level. We helped implement the Ansible tool set (including Ansible Tower), ensured connectivity to the client's environment and worked with the client's team to develop playbooks to automate the application of security patches.

> **"The CleanSlate team was able to pick up knowledge (of our environment) and get to work very quickly. In addition, we were impressed with the quality in which the solution was delivered."**

RESULTS:
CleanSlate's solution helped the client to drive additional business value now that they are not focusing on their prior heavy workload. In addition, the client saw the following results:

- Patched server KPI before implementing the solution averaged 13-15% with a high water mark of 30%, during the monthly patching cycle
- In the first month, they saw an increase to 64% of servers being patched and last month they broke 70%
- Less than five support incidents were reported since the solution was put into place

These results yielded a huge time savings and a more secure and reliable server environment.