

CASE STUDY

ASSET
MANAGEMENT
AND PCI
COMPLIANCE



As a Service Provider handling customer cardholder data (CHD), our client is required to validate compliance with the PCI DSS (Payment Card Industry Data Security Standard) annually through a formal external assessment, performed by a Qualified Security Assessor Company. The PCI DSS is a detailed and prescriptive set of security requirements for protecting customer credit card data that includes over 1000 individual data points and controls that must be validated in order to meet compliance with both the PCI Security Standards Council and Card Brands' requirements. PCI compliance is also a contractual obligation for many clients' customers; failure to comply with the PCI DSS could lead to security incidents, significant fines, and negatively impact our client's customer relationships and their bottom line.




THE CHALLENGE

Due in part to staffing and environmental changes, our client was found to be out of compliance with multiple significant technical, procedural, and time-based requirements. Some of the key areas identified that complicated meeting compliance with the PCI DSS were directly related to the client's scope and inadequately managed asset management processes. Issues included:

- > Client's relatively flat network architecture
- > Lack of overall definition of in-scope systems and applications
- > Inadequate asset management tools and system inventory (Client initially indicated that the scope of their network was between "three and five thousand hosts")
- > A lack of understanding and documentation related to payment system interconnectivity, dataflows, and critical system functions

THE SOLUTION

To address these problems, Online's Service Management team performed a comprehensive evaluation of the network and application environment that included both on-prem and cloud based systems, utilizing the BMC Discovery platform coupled with expert analysis from our team of consultants.



Ultimately, Online created a clear picture of the client's true asset inventory and connectivity.



TECHNOLOGY OVERVIEW

- > *Online was able to provide detailed information on the connectivity between systems and applications, down to the IP and service level, fingerprint operating systems and assets, and ultimately create a clear picture of the client's true asset inventory and connectivity.*
- > *Further analysis was performed to help them determine which systems should be isolated to reduce PCI scope; based on this analysis, the scope of the PCI environment was reduced from over 3000 to under 1800 systems in a matter of days, greatly simplifying future management and inventory concerns and increasing the client's overall security posture.*
- > *Online believes further scope reduction is possible, presenting opportunities for significant cost savings related to compliance management.*

THE RESULTS

ONLINE WAS PLEASED TO BE ABLE TO HELP THE CLIENT OBTAIN AN ATTESTATION OF COMPLIANCE FOR 2020, AVOIDING FINES AND POTENTIALLY COSTLY CONTRACTUAL ISSUES WITH THEIR CUSTOMERS.

Online estimated that this work could have taken 6 months or more for a similar organization; our team was able to help them reach this milestone in approximately 3 months, in large part due to the targeted scope analysis and reduction engagement that was performed.

OUR CLIENT HAS GREATLY IMPROVED THEIR SECURITY AND COMPLIANCE POSTURE AND IS WELL POSITIONED TO LEVERAGE THIS WORK TO CREATE A SUSTAINABLE AND OPTIMIZED PROGRAM IN THE FUTURE.

NEXT STEPS

To learn more about how Online Business Systems can help your business, visit **obsglobal.com**

 Results. Guaranteed.





Founded in 1986, Online Business Systems is North America's leading Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.