BLAZENT
CUSTOMER SUCCESS STORY

96% Reduction in Rogue Devices
Helps Managed Service Provider Deliver for Financial Client

CUSTOMER CHALLENGE

Our customer is a large managed services provider (MSP) that manages IT infrastructure assets for a Global 500 financial services company based in Europe.

Due to the complex compliance & regulatory environment of the financial industry, our customer was challenged to quickly & accurately identify the actual content of the financial organization's massive IT estate, and remediate assets considered to be high risk. For this account, high risk assets were defined as servers and PCs operating in the environment but not listed in the configuration management database (CMDB), or missing a core application like antivirus software or encryption functionality.

Service Level Agreements (SLAs) for the engagement required our customer to track and report accurate asset numbers for both server and PC populations, acquire asset lifecycle status, and use operational tooling to locate "active" assets not listed in the CMDB. Not only was our MSP customer required to provide trending scorecards for this critical information, our customer also needed to track billing accuracy and the deployment of key software applications.

HOW BLAZENT HELPED

Initially, Blazent worked closely with the account team during the discovery process to analyze 11 different raw data sources and the detailed reporting requirements for the engagement. This enabled the team to configure the necessary functionality into Blazent's Outsourcing Governance Solution.

The granularity of the reporting requirements is what makes this customer success story particularly interesting. Beyond Blazent's standard out-of-the-box reporting which identifies "Rogue Devices" (devices active on the network but not in the CMDB), "Phantom Devices" (devices listed in the CMDB but not active on the network), and software deployment coverage, this situation required the additional capability of being able to adjust the time frame in which an asset is considered "active" from 30 days to 60 days to 90 days.

After several weeks of collaboration, Blazent's integrated solution was configured to handle this extra level of needed customization and the project team started its work to optimize the environment.

RESULTS

Using output provided from Blazent's Outsourcing Governance Solution, our customer was able to deliver three very important results:

1) 96% Reduction of "Rogue Devices"
In six months, the Rogue Device count was reduced from 1,242 devices to 45 devices (96% reduction).

2) 300 Hours Eliminated from the Encryption Monitoring Process
By automating the encryption monitoring process using Blazent, our customer was able to save 300+ hours of manual work, and helped the organization avoid expensive audit penalties.

3) 94% Reduction of "Phantom Devices"
In six months, the Phantom Device count was reduced from over 1,341 devices to 80 devices (94% reduction).

BLAZENT IMPACT

96% Reduction
in Number of "Rogue Devices"

+

300 Hours Eliminated
from Encryption Coverage Monitoring

+

94% Reduction
in Number of "Phantom Devices"

Going forward, Blazent continues to be actively used in the day-to-day management of this large outsourcing engagement to ensure the initial data integrity improvements are not only maintained, but also improved.

About Blazent

Blazent is the world's most widely-used IT Data Integrity Engine. Built on patented algorithms developed over the last decade, Blazent's cloud-based engine aggregates, reconciles and consolidates IT data to guarantee continuous accuracy, and to optimize IT management & operations. Global 5000 executives rely on Blazent to ensure effective governance & compliance, mitigate risk, control costs and support major business transformation. As the gold standard for IT Data Integrity, Blazent empowers the business of IT. Headquartered in Silicon Valley, California. For more information, visit www.blazent.com or follow Blazent on Twitter @Blazent.