RESOLVING CROWDSTRIKE: BEHIND THE SCENES WITH BMC HELIX

On Friday, July 19, 2024, I was on a plane from Frankfurt to San Francisco, and I was one of the lucky few whose flight was not cancelled or delayed. On that day, what was supposed to be a minor software update had brought IT systems at major airlines, banks, and organizations worldwide to a standstill. It is a stark reminder that the impact of changes, if not properly assessed, can have a huge impact on our daily lives.

IT organizations around the globe must strike (pun intended) a balance between maintaining the speed of software delivery required to support the modern pace of business and effectively managing the risk that these changes can cause IT service disruptions. One of our customers was able to identify the risk of the CrowdStrike update and remediate it quickly with the BMC Helix platform.

How they did it

The customer, a large company in the food and beverage industry in the US, has been using BMC Helix products for a while now, including both BMC Helix IT Operations Management and BMC Helix Service Management, allowing it to effectively practice our ServiceOps approach (more on it below).

As the CrowdStrike patch issue started developing and affecting its systems, this company's command center was swamped with calls from its stores, warehouses, and manufacturing facilities. It was so intense that its IT team couldn't get "off queue" from taking calls to resolving calls. The

CrowdStrike issue was unique because the affected hosts needed to be patched manually. The company's BMC Helix Digital Workplace management team quickly spun up its BMC Helix Digital Workplace service so its stores could self-report issues, allowing the staff to focus on remediating servers and desktops. Within one day, hundreds of requests had been submitted.

BMC Helix helped this organization's IT team remediate the effects of the CrowdStrike patch and avoid the prolonged downtime that impacted—and is still impacting—so many people and businesses across the world. This was possible because the company's BMC Helix environment was not affected by the CrowdStrike issue.

Our ServiceOps approach helps IT teams manage risk

At BMC, we believe bringing together ITSM and ITOM while also embedding artificial intelligence and machine learning (AI/ML), is the answer to the increasing demand on IT teams to operate with no downtime and deliver high-quality services. ServiceOps is about eliminating information, technology, and organizational silos so cross-departmental teams can work collectively to deliver highly resilient services.

At the foundation of our ServiceOps approach is BMC Helix, our open platform with which IT teams can improve overall IT service quality by sharing data, predicting issues, automating workflows, and preventing outages. In our approach to ServiceOps, AI helps IT teams surface signals and eliminate noise so they can more quickly use data to correlate IT incidents and identify service problems. Combining ServiceOps with observability and AIOps helps IT teams increase the reliability of their services.

Improve IT resiliency with BMC Helix Discovery

In situations like the one facing the customer above, and other IT organizations around the world on Friday, it is more important than ever to understand in real time whether your IT assets are up to date and to proactively identify vulnerabilities.

This is where BMC Helix Discovery, a key component of our ServiceOps approach, can help customers improve IT resiliency. BMC Helix Discovery plays an essential role in proactively resolving vulnerabilities by providing comprehensive visibility and automated discovery of IT assets across an enterprise.

It continuously scans the IT systems to identify and catalog hardware, software, and their dependencies, maintaining a dynamic and up-to-date inventory of assets. By dynamically maintaining an accurate and current configuration management database (CMDB), BMC Helix Discovery allows IT teams to quickly detect vulnerabilities, assess their impact, and prioritize remediation efforts. The solution also neutralizes vulnerabilities faster by helping teams understand their business impact. In situations like the CrowdStrike update, BMC Helix Discovery customers would benefit from understanding which parts of the business service would have been affected by the update.

Also, BMC Helix Discovery's integration with security information and event management (SIEM) and vulnerability management tools enables automatic correlation of asset data with known vulnerabilities, facilitating efficient resolution and remediation of issues before they can be exploited. This approach not only enhances security but also minimizes downtime and operational disruptions, ensuring a more resilient IT infrastructure.

Interested in making your IT environment more resilient? Learn more about BMC Helix Discovery, BMC Helix Digital Workplace, and other BMC products at bmc.com/helix, or contact our sales team.