CROWDSTRIKE SERVICES

CROWDSTRIKE

Investigation Summary

PREPARED FOR

Boston Scientific Corporation

DELIVERED ON

September 22, 2026

services@crowdstrike.com

Investigation Summary

Background

On August 25, 2026, Boston Scientific Corporation ("Boston Scientific") identified system availability issues affecting certain segments of its network. Subsequent review determined the system unavailability was related to access by an unauthorized third party ("Threat Actor"). CrowdStrike Services ("CrowdStrike") was engaged to provide investigative services and to assess the scope and extent of Threat Actor activity within the Boston Scientific environment.

Findings

CrowdStrike's investigation began on August 25, 2026, and concluded on September 18, 2026. CrowdStrike determined that the Threat Actor gained access to the Boston Scientific environment through an external-facing network management device, with subsequent Threat Actor access limited to a portion of Boston Scientific's on-premises environment. Upon discovery of Threat Actor activity on August 25, 2026, Boston Scientific began implementation of the containment actions detailed below. CrowdStrike did not identify evidence of ongoing Threat Actor activity since August 25, 2026. CrowdStrike did not identify evidence that the Threat Actor caused encryption of data in any Boston Scientific environment. CrowdStrike did not identify any evidence of Threat Actor activity in Boston Scientific's Microsoft 365, email, collaboration and productivity platforms.

CrowdStrike did not identify evidence of interactive remote access to any of the following systems as identified by Boston Scientific:

- Human Resources and Employee Benefit systems.
- Medical device maintenance systems.
- Manufacturing and maintenance systems.
- Boston Scientific's supervisory control and data acquisition ("SCADA") systems.
- Software development systems.
- Product development systems.

CrowdStrike did not identify evidence that the Threat Actor authenticated at the application level for any of the following applications as identified by Boston Scientific:

- Internally developed and managed Boston Scientific manufacturing or medical device environments.
- SOX related financial systems, such as Salesforce or SAP.
- Software as a Service ("SaaS") and cloud applications.

CrowdStrike did not identify evidence that the Threat Actor accessed, staged or exfiltrated data from the systems and applications above, including any data identified as customer or patient data by Boston Scientific.

Containment Actions

Boston Scientific informed CrowdStrike that the below actions were taken to eradicate the Threat Actor from the environment, and harden against similar events:

- Disconnected and decommission of the network device used for initial entry into the Boston Scientific environment.
- Implemented firewall blocks for known IP addresses and domains used by the Threat Actor.
- Performed password resets.
- Additional hardening of the affected environment.

At Boston Scientific's request, CrowdStrike expanded existing security monitoring, threat detection, and response capabilities through the deployment of additional Falcon features. CrowdStrike continues to support Boston Scientific, providing monitoring and threat detection across the Boston Scientific environment with the assistance of Falcon Overwatch and CrowdStrike Active Defense Services.