

Dear Valued Customer,

We are writing to provide additional information regarding the cybersecurity incident Boston Scientific identified on August 25, 2026, and to share the attached final investigation summary prepared by CrowdStrike.

We appreciate the patience, trust and partnership you have shown as we conducted a thorough investigation and safely restored affected systems.

Investigation and findings

CrowdStrike completed its independent investigation and determined that the threat actor gained access to an external-facing network device and then to a limited portion of Boston Scientific's on-premises IT environment.

The investigation found no evidence of ongoing threat actor activity following Boston Scientific's containment measures implemented on August 25, 2026.

CrowdStrike found no evidence of compromise within Microsoft Office 365 applications (including email), other cloud-based applications or critical business systems related to manufacturing maintenance, product and software development, medical device maintenance, human resources and employee benefits systems or Boston Scientific's supervisory control and data acquisition (SCADA) environments.

CrowdStrike also found no evidence that the threat actor accessed, staged or exfiltrated data from those systems and applications, including customer or patient data.

Supporting previous assessments, based on the investigation and containment measures completed, customers and partners may safely continue normal business activities and system connections with Boston Scientific.

Containment and remediation

In parallel with the forensic investigation, Boston Scientific implemented containment, recovery and security-enhancement measures to harden against similar events, including:

- Disconnected and decommissioned the network device used for initial entry into the Boston Scientific IT systems
- Implemented firewall blocks for known IP addresses and domains used by the threat actor
- Performed password resets

Although the forensic investigation has concluded, Boston Scientific will continue monitoring its environment, completing longer-term security enhancements and applying lessons from this incident to further strengthen our cybersecurity program.

Our continuing commitment

We are grateful for your patience and partnership throughout our response and recovery. Again, please refer to the attached CrowdStrike report for additional information about the forensic

investigation, its scope and its conclusions.

For additional questions concerning this incident or the attached report, please review information available through our [website](#) or contact your sales representative.

Thank you,

Paudie O'Connor
Executive Vice President, Global Operations
Boston Scientific Corporation