

Harden your security

Protect your entire IT estate with Microsoft Azure Arc-enabled infrastructure and Intel® technologies



Quickly identifying security threats is more important than ever.

Threats are growing in number and complexity:

- Ransomware and ransomware-as-a-service
- Botnets
- Cloud-powered attack techniques
- Nation-states harboring threat groups

It is getting more difficult to protect enterprises:

- 277** days to identify and contain a data breach¹
- 12.7%** year-over-year growth in total cost of a breach¹
- \$4.35M** average cost of a data breach¹

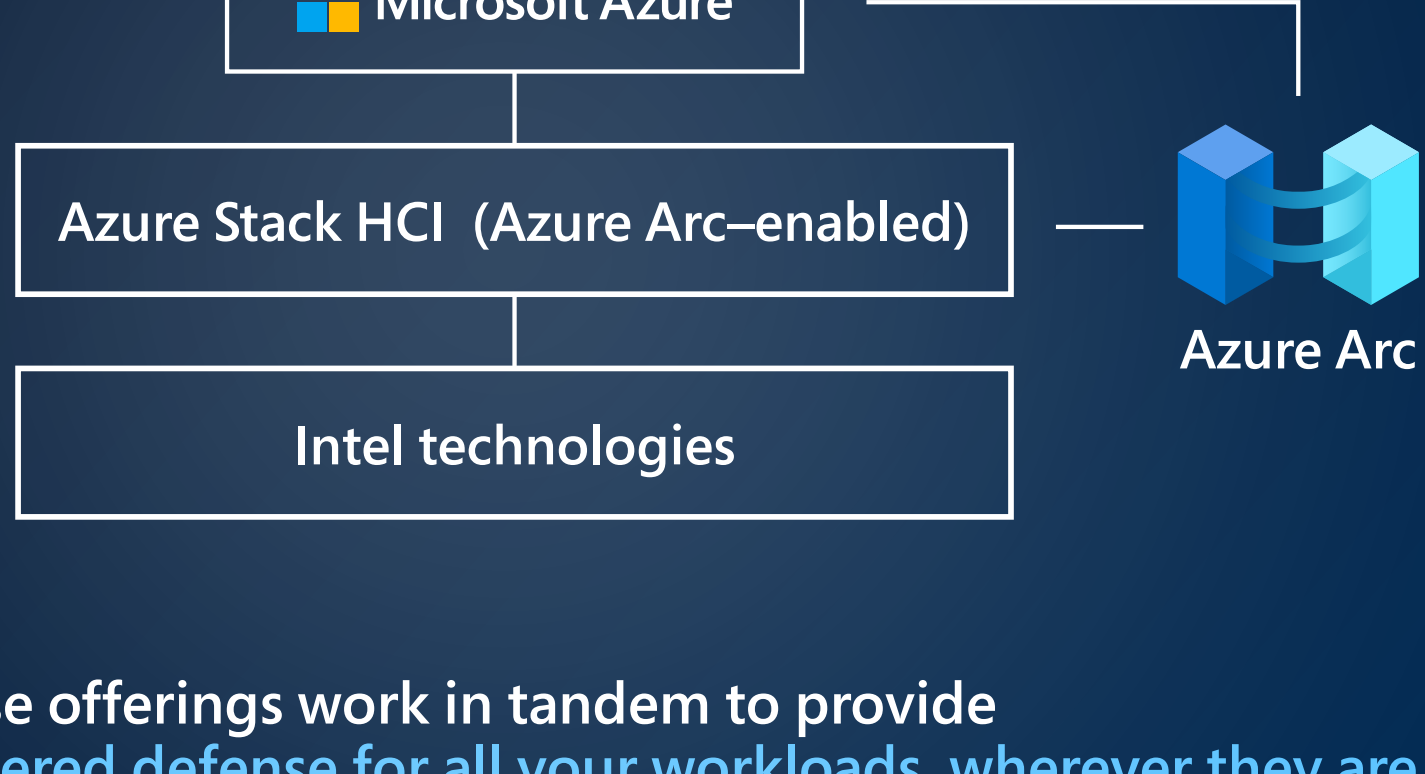
IT security professionals face additional challenges:

- Disparate security tools**
Security tools are increasingly complex and poorly integrated into the DevOps cycle.
- Too many tasks for under-resourced teams**
In some organizations, IT security admins might manage more than 20 security tools.
- Difficulty finding the signal in the noise**
The sheer volume of security signals means that attacks can “hide” in environments 50+ days before discovery.²

Attacks can span across many layers and organizational silos. As a result, security must be holistic.

Microsoft Azure Arc-enabled infrastructure on Intel technologies helps fortify your defenses across the stack.

Microsoft and Intel offer enterprises a comprehensive approach to security with built-in, modern, and holistic technologies.



These offerings work in tandem to provide a layered defense for all your workloads, wherever they are.

Together, Microsoft and Intel solutions help provide cohesive protection from silicon to cloud, including:

- Intel Crypto Acceleration**
Stronger encryption on Azure Stack HCI is built on Intel hardware acceleration for pervasive encryption.
- Full-memory encryption**
Intel Total Memory Encryption (Intel TME) helps protect platform memory against attack.
- Secured-core server**
A collaboration across Microsoft, Intel, and server OEM partners helps simplify security enablement and provide advanced protection.



Two visionary companies working to protect your business:

- Azure is the only cloud platform built by a security leader—Microsoft.
- 650K customers**
and 90 Fortune 100 companies trust Microsoft for security
- 24 trillion**
signals processed by Microsoft every 24 hours
- 9 billion**
malware threats blocked by Microsoft Defender in 2020 alone
- 12 studies**
in which Microsoft is a security leader (Gartner Magic Quadrant and Forrester Wave)

- Intel's security-first pledge aims to keep businesses safe with a defense-in-depth strategy:
 - Foundational security**—critical protection to help verify the trustworthiness of devices and data
 - Workload and data protection**—trusted execution for hardware-isolated data protection
 - Software reliability**—platforms that help protect against a range of cybersecurity threats

Protect your entire environment with hardened security.



Read the security white paper: [“Secure your Microsoft Azure Arc-enabled environment with Microsoft and Intel.”](#)

¹ IBM Security, “Cost of a Data Breach Report 2022,” July 2022, www.ibm.com/security/data-breach.
² Based on internal Microsoft customer research.
 © 2022 Microsoft Corporation. All rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.
 This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.