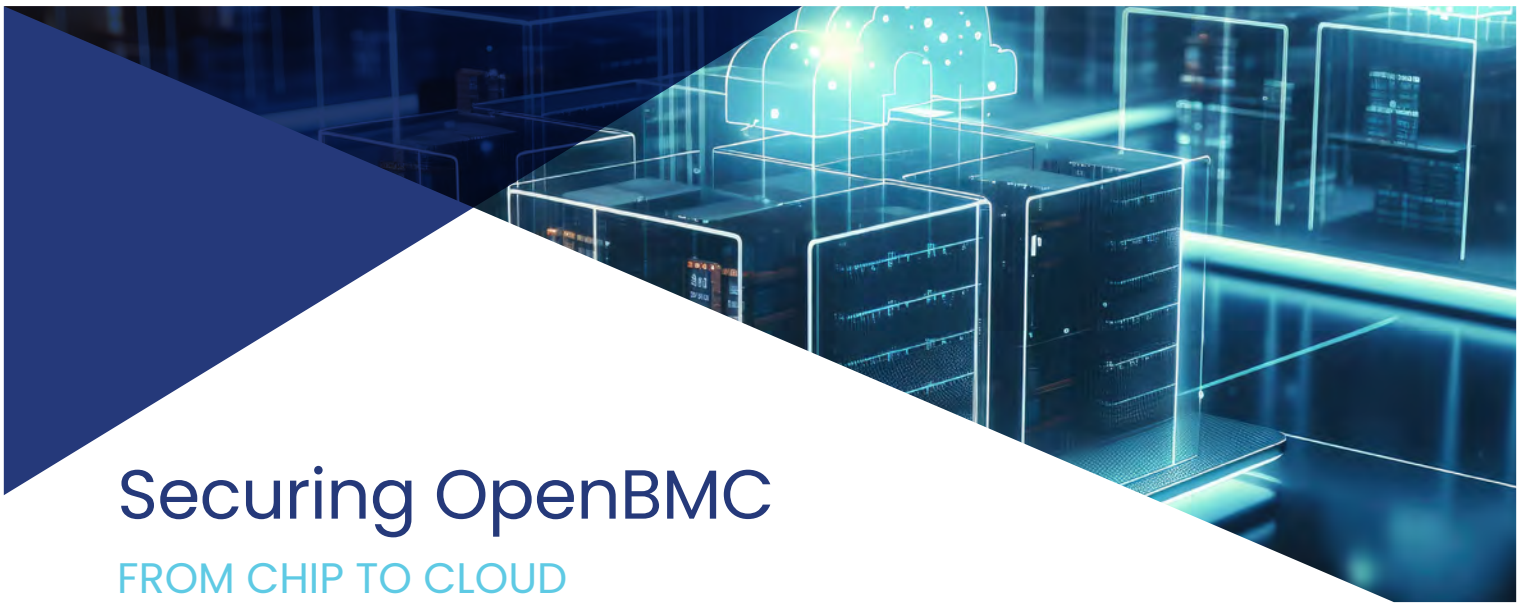


Securing OpenBMC

FROM CHIP TO CLOUD

INTRODUCTION

As enterprise Information systems and infrastructure expand to hybrid cloud environments, shifting administration and management from onite to to remote, the risk of cyberattacks for the data center server infrastructure is growing. As new protocols like OpenBMC from Open Computing Platform (OCP) standardize remote management and administration protocols, there is a stronger need to protect systems from the BMC chip all the way to the remote management systems, as we move from legacy IPMI to openBMC.

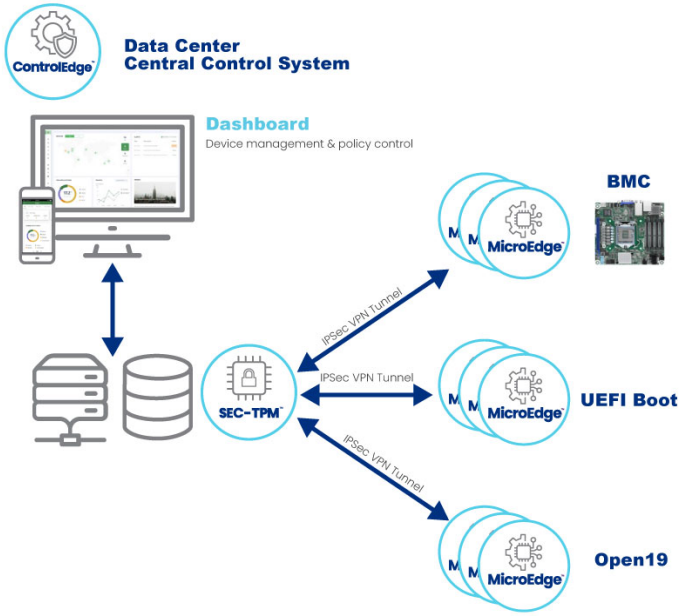
SecEdge's solution for OpenBMC is designed to protect server infrastructure:

- Securing the server device with with SecEdge' SEC-TPM, which is integrated with leading BMC processors like the ASPEED AST2600. This provides a root-of-trust and enables device authentication, secure boot & updates, and encryption key generation and storage. This protects the server from local attacks from the other malicious systems.
- Enabling secure communication tunnels with SecEdge' SEC-VPN. This solution enables multiple IPSec tunnels for device administration and management communication.

The solution brings a number of benefits, including:

- Strengthening OpenBMC's security and integrity, by offering an option of having a hardware root-of-trust anchored in the BMC Chip;
- Securing Remote Access to the Data Center server infrastructure by isolating BMC access;
- Securing lifecycle management with secure provisioning and change of ownership; and
- Protecting software and firmware updates by using a control plane isolated from the application plane.

SEC-VPN™ SECURE BMC SOLUTION



COMPLIANCE

- TCG 2.0 (Vendor ID:0X5ECE)
- NIST SP800-147: Secure Code Update
- NIST SP800-155: Strong measurement and remote attestation
- NIST SP800-164: Foundations in Root of Trust
- NIST SP800-193: For Protection detection and recovery
- PSA Level 1 Certified
- IOT Security Foundation certified

PARTNERS

ASPEED

METIFY

SEC eDGE™
Digital Security to the Edge

SecEdge™ (www.secedge.com) is a digital security leader for IoT and Edge devices, providing advanced security solutions for edge AI, compute, and control applications in a software as a service platform. Renowned for its award-winning AI Model protection, the SecEdge platform provides a complete chip-to-cloud solution including device-level security, zero-trust networking, and secure data control and management.

PO Box 201
Fall City, WA 98024
+1 425 654 2048
info@secedge.com
www.secedge.com