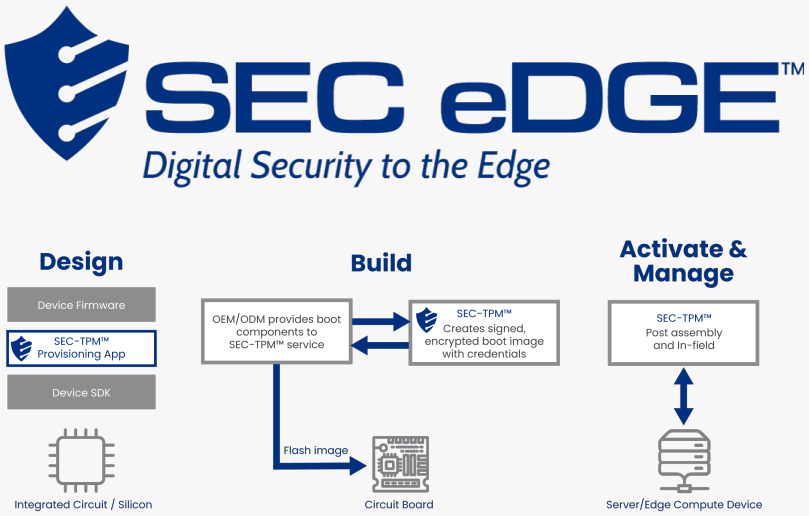
SecEdge™ Announces Collaboration with Insyde® Software to Enhance Server Security with OpenBMC Firmware

SecEdge SEC-TPM™ and SEC-VPN™ change the data center server administration landscape by enabling VPN Tunnels from BMC silicon to management systems

SEATTLE, WA, USA, May 30, 2024 /EINPresswire.com/ -- SecEdge, a digital security leader for Edge devices, announced today its collaboration with Insyde® Software, a leading provider of UEFI BIOS and OpenBMC-based systems management firmware. The alliance will deliver security enhancements to OpenBMC solutions by integrating SecEdge's SEC-TPM™ chip-to-cloud BMC security platform and Insyde Software's Supervyse® OPF OpenBMC firmware.



SEC-TPM™ is a TCG 2.0 Compliant, firmware TPM with turnkey provisioning service. It provides the security features provided by a discrete TPM, with crypto-agility and higher performance, without the need for additional hardware.

SEC-TPM is a turnkey solution providing a TCG 2.0 compliant fTPM with post-assembly provisioning service. It supports a range of Arm® TrustZone enabled secure hardware enclosures, including ASPEED Technology's AST2600 Secure Management Processor. Insyde Software's Supervyse OPF is a true OpenBMC-based solution that delivers reliable and secure systems manageability for today's enterprise, cloud and HPC servers.

The partnership provides several disruptive benefits for data center and cloud computing:

- 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.

> By working with Insyde Software, we provide the market a hardened and tightly integrated solution, thwarting threats targeting OpenBMC."
>
> *Sami Nassar, President & co-CEO, SecEdge*

Additionally, SEC-TPM provides a firmware TPM, anchored in the BMC Chip. This can be extended to the host OS, eliminating the need for a discrete TPM chip and providing flexibility for TPM provisioning as late as needed in the supply chain.

"By working with Insyde Software, we provide the market a hardened and tightly integrated solution, thwarting threats targeting OpenBMC," said Sami Nassar, president and co-CEO of SecEdge. "We believe this partnership will contribute toward creating a more secure data center infrastructure," added Nassar.

"We are thrilled to work with SecEdge to bring this innovative security technology to our server customers," said Tim Lewis, CTO of Insyde Software. "Our collaboration further demonstrates our commitment to platform security, and we believe that this combined solution will provide our customers with the secure remote management features they demand for enterprise, cloud, high-performance accelerated computing environments," added Lewis.

ABOUT SECeDGE, INC.

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.

Insyde and Supervyse are registered trademarks or trademarks of Insyde Software in the United States and other countries. SecEdge and SEC-TPM are registered trademarks or trademarks of SecEdge Inc. Other names and brands may be claimed as the property of others.

###

Jennifer Walken
Sec Edge, Inc.
jennifer.walken@secedge.com
Visit us on social media:
X
LinkedIn