SOLUTION BRIEF

Public Sector
Client Computing

Archon ZV: Secure Mobile Computing

Powered by the Intel vPro® platform and secured by the INTEGRITY operating system (OS), Archon ZV is redefining "secure" by providing an easy-to-use mobility solution with zero vulnerabilities[1]

Achieving security in an insecure world

Widespread use of the Internet and the proliferation of mobile devices have created a world in which individuals, businesses, and nations are more connected than ever before. The Internet of Things (IoT), backed by edge computing, machine learning, data analytics, and cloud technology, is accelerating and amplifying those connections. Currently, the number of IoT-connected devices worldwide is expected to reach 41.6 billion by 2025.[2]

As the world becomes more connected, however, it also becomes less secure. With each new connected device, vulnerabilities multiply, resulting in a rapid increase in the number of successful cyberattacks and serious data breaches worldwide. In 2019, the total cost of cybercrime is expected to exceed USD $2 trillion—a four-fold increase since 2015.[3] Globally, malicious hackers, cyberterrorists, and other cybercriminals are a growing threat to consumer finances, business operations, and public safety. According to the January 2019 edition of the *U.S. National Intelligence Strategy Report*, "Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices."[4]

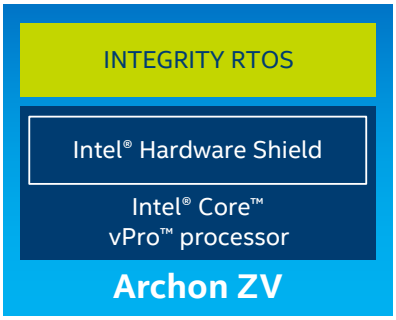
U.S. government organizations and individuals who routinely handle classified information and safeguard national security—from military and intelligence services to designated national leaders in the executive and legislative branches—require highly secure access to mobile resources in diverse locations. Increasingly, the same is true for law enforcement and many enterprise organizations that must ensure data security, protect critical infrastructure, and guard against attacks by cybercriminals and cyberterrorists. Unfortunately, many high-security or encryption solutions are expensive, complex, inflexible, difficult to scale, and hard to manage and maintain.

Introducing Archon ZV from ID Technologies

Designed by ID Technologies, Archon ZV (the ZV stands for "zero vulnerabilities") is one of the world's most secure laptop computers. It is the first-ever turnkey mobility solution that meets Commercial Solution for Classified (CSfC) program requirements. Developed by the National Security Agency (NSA), the CSfC program is an important part of the U.S. government's strategy to more quickly deliver layered cybersecurity solutions by leveraging emerging technologies and commercial products to meet rapidly evolving customer requirements.

The Archon ZV client is built on a high-performance Intel® Core™ vPro™ processor-powered laptop, which provides both an excellent end-user experience and sufficient performance to operate efficiently in diverse locations and under often challenging conditions. Intel vPro® technology provides the highly secure platform foundation for the Archon ZV, which is further secured by the INTEGRITY operating system (OS) from Green Hills Software and the INTEGRITY Separation Kernel,

ARCHON | ZV
ZERO VULNERABILITIES



which has been certified for the highest levels of safety and reliability in the INTEGRITY-178B Operating System.

The INTEGRITY Separation Kernel is the first and only separation kernel to be evaluated by the NSA and certified by National Information Assurance Partnership (NIAP) to EAL6+ High Robustness under the international Common Criteria standard (ISO/IEC 15408). This security rating certifies that the product is suitable for the protection of classified information and other high-value resources against well-funded, sophisticated attackers. INTEGRITY-178B is the only software product ever to achieve the EAL6+ High Robustness rating.

Hardware-enhanced security capabilities powered by the Intel vPro platform

Today's cyberattacks are moving down the computing stack—from software to hardware—making it increasingly difficult for the legacy model of software protecting the system to cope and keep pace with rapidly advancing threats to digital security, safety and privacy. Intel builds hardware-enabled security capabilities directly into its silicon to help protect every layer of the compute stack, including hardware, firmware, operating systems, applications, networks, and the Cloud.

For the Archon ZV solution, ID Technologies chose the Intel vPro platform for its hardware-enhanced security technologies. In addition to providing hardware-enhanced security features, the Intel vPro platform is the best for business, offering the performance, manageability, and stability of Intel® architecture while aligning with a future-proof roadmap.[5] The platform is optimized for managed IT environments and enables the enforcement of corporate policies.

In developing the Archon ZV solution, ID Technologies built on the hardware-enhanced security foundation that Intel makes available to all its partners. "When we began the challenge to build the world's most secure personal security appliance, we started with the most secure platform," says Dylan Conner, Chief Technology Officer at ID Technologies. "Many of the security capabilities we needed to make Archon ZV one of the world's most secure laptops were already built into the Intel technology. Having that level of hardware-enhanced security made our impossible task possible."

ID Technologies, using the INTEGRITY Real Time Operating System (RTOS), made extensive use of Intel hardware-assisted virtualization and security technologies to build a secure and trusted virtualized environment. The foundational technology building blocks are Intel® Virtualization Technology (Intel® VT including VT-x & VT-d) and Intel® Trusted Execution Technology (Intel® TXT), all part of the Intel® Hardware Shield suite of technologies.

Intel VT and Intel TXT are built into the hardware of the Intel vPro platform and enable the hypervisor to secure operating systems, applications, and data by keeping them isolated on their own Virtual Machines (VM), running in their own virtual hardware environment. Each VM is prevented from accessing another VM's OS, applications, data and input/output (I/O). Intel TXT enables a dynamic root of trust to ensure VMs are running on trusted hardware with trusted software, by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. This creates the ability to verify the security of installation, launch, and use of the hypervisor and operating systems.

These technologies provide a highly scalable architecture that is specifically designed to harden platforms against hypervisor and BIOS attacks, malicious root kit installations, and other firmware- or software-based attacks. Archon ZV and the Green Hills INTEGRITY Global Security software use these technologies on the Intel vPro platform for the multilevel, integrated software- and hardware-security separation capabilities they provide. Intel vPro technology helps to ensure more secure platforms and greater application, data, or virtual-machine isolation while providing a foundation for more advanced solutions as security needs continue to evolve.

Key takeaways

- With near-zero vulnerabilities, Archon ZV is one of the world's most secure laptops; it is powered by the security-enhanced Intel vPro platform and further secured by the INTEGRITY operating system from Green Hills Software and the INTEGRITY Separation Kernel.
- Archon ZV benefits from the hardware-enhanced security capabilities that Intel builds directly into its silicon and makes available to partners in the Intel security ecosystem.
- Archon ZV is a turnkey mobility solution that provides an excellent end-user experience and operates efficiently in diverse locations and challenging conditions.
- With its security features, Archon ZV helps government agencies, law enforcement organizations, and enterprises protect data and critical infrastructure against attacks by cybercriminals and cyberterrorists.

Leading benefits of Archon ZV

With Archon ZV, ID Technologies has redefined "secure" by creating a highly secure mobility solution, powered by the Intel vPro platform, which is:

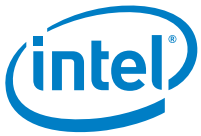
- **Flexible** – Archon ZV runs any common client operating system or application, including native applications that are compliant with Windows, Linux, Android and POSIX
- **Mission-ready** – The client hardware runs any client applications and is ready to handle any mission
- **Exceptionally mobile** – Depending on the capability package specified, Archon ZV can be deployed and operational anywhere on the planet and on any network, enabling true global mobility
- **Scalable** – The NSA CSfC capability packages create secure connections and data at rest for one or multiple environments
- **Not dependent on connection** – Archon ZV works beyond the internet connection, offering a variety of frequency support for the true tactical edge—including disconnected operations
- **Easy to use** – Archon ZV is easy to use and requires little user training; the laptop interface runs all current applications, providing a seamless user experience
- **Free from configuration challenges** – The factory-installed, use case-specific security policy means zero vulnerabilities from improper configuration. Archon ZV cannot be configured improperly, and there is no hardware-configuration management. Once the security policy is defined, there is no ability to deviate from it.

The entire Archon ZV system is designed to make security invisible to end users and sustainable for IT support teams, without compromising functionality or ease of use.

Additional information

For more information about the Archon ZV and Intel vPro platform security technologies, see:

- **Archon ZV and ID Technologies** https://www.idtec.com/archon/
- Intel vPro Platform https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-platform-general.html
- Intel Trusted Execution Technology Whitepaper https://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html



[1] The Archon ZV employs Green Hills Integrity RTOS, rated with "zero- vulnerabilities" per the National Vulnerability Database, National Institute of Standards and Technology, U.S. Department of Commerce (https://nvd.nist.gov/vuln/search). No product or component can be absolutely secure.

[2] The Internet of Things is Expected to Generate 79.4ZB of Data in 2025, According to New IDC Forecast, IDC, June 18, 2018 (Reference: https://www.idc.com/getdoc.jsp?containerId=prUS45213219)

[3] The Future of Cybercrime & Security: Threat Analysis, Impact Assessment & Mitigation Strategies 2019-2024, Juniper Research, August 27, 2019 (Reference: https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security)

[4] National Intelligence Report of the United States of America, 2019 (Reference: https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf)

[5] Based on a comparison (as of September 11, 2019) of features in the following categories: manageability, security, stability, and processor performance, between Intel vPro®-enabled platforms and other selected x86 architecture-based platforms marketed for use in business PCs.

Selection of manageability, security, stability, and processor performance features are based on a 2018 web-based survey, conducted by Intel of more than 500 IT decision-makers, to assess desired features when purchasing PCs for business use.

Printed in USA 0120/MM/MIM/PDF ♻ Please Recycle 341849-001