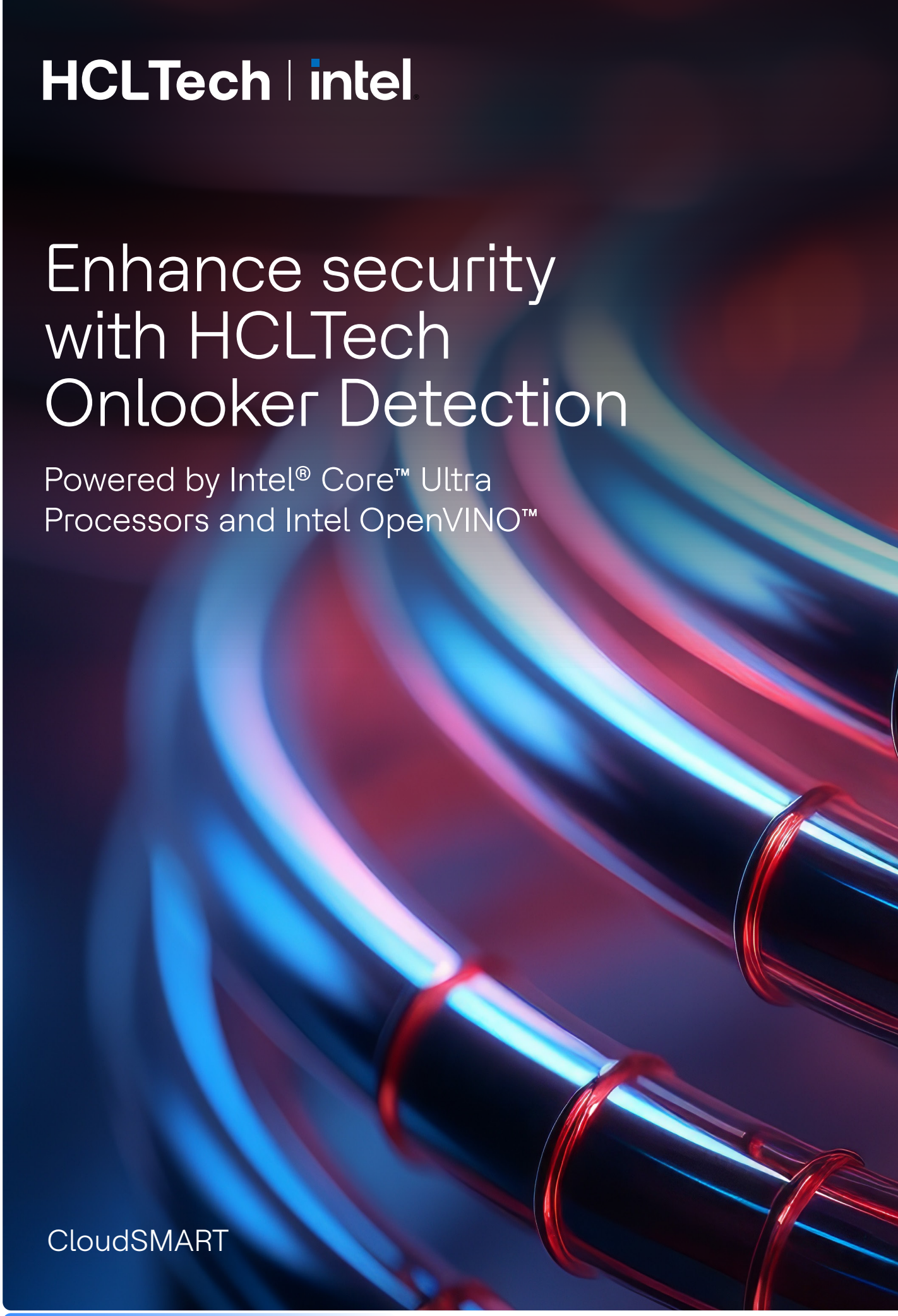
HCLTech | intel

Enhance security with HCLTech Onlooker Detection

Powered by Intel® Core™ Ultra Processors and Intel OpenVINO™



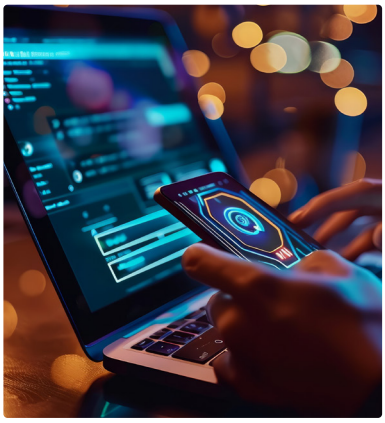
CloudSMART

Introduction:

Business in today's era requires organizations to adopt remote and hybrid work models. Safeguarding digital assets and ensuring the security of remote and hybrid employees has become imperative. HCLTech Onlooker Detection is a state-of-the-art security solution that Intel's Core Ultra processor powers. With Onlooker Detection, organizations can strengthen their defenses against evolving social hackers. This innovative security solution combines the power of Intel's Core Ultra processor with motion sensing and identity protection technologies to set new digital security standards.

Key Benefits:

HCLTech Onlooker detection offers a range of key benefits that can transform security and compliance measures in the hybrid workplace landscape and safeguard data while easily ensuring regulatory compliance



- **Prevents unauthorized access:** HCLTech Onlooker Detection utilizes AI-powered webcam surveillance to prevent unauthorized access effectively, safeguard company data and uphold security and compliance standards.
- **Visibility of machine location:** SecureSense provides clear visibility into device location, allowing for easy tracking in case of theft or loss and ensures device security.
- **Prevents data leakage:** Onlooker Detection's robust measures protect sensitive company data and prevent data leakage and unauthorized access.
- **Saves cost:** Maximize efficiency and reduce costs with out-of-the-box AI models and streamlined deployment.
- **Compliant solution:** HCLTech Onlooker Detection is designed to meet the stringent requirements of PCIDSS and GDPR compliance, ensuring that data is handled responsibly and securely. No data is stored in central servers unless a violation occurs, enhancing data protection and regulatory adherence.
- **Reduces overhead through AI:** Leverage AI-based solutions to optimize compliance and security management and improve operational efficiency.

Features and functionality:

HCLTech Onlooker Detection is designed to optimize workplace management and enhance employee experiences.

- **Identity protection:**

  Use webcam-based monitoring to verify that only authorized identities access the computer and bolster security against unauthorized access.

- **Motion sensing:**

  Leverage advanced AI models to detect motion behind the user, mitigating the risk of data loss through shoulder surfing attacks and ensuring your sensitive information remains protected.

- **HCLTech managed services**

  Enjoy comprehensive end-to-end support services from HCLTech for a seamless and consistent experience, ensuring that your security measures are always up-to-date and effective.

- **Detect prohibited devices:**

  Detect and block prohibited devices such as mobile phones and cameras to prevent potential data breaches and unauthorized access to sensitive information.

- **Imposter Detection:**

  Compliance with regulatory standards by implementing imposter Detection mechanisms, ensuring that only authorized personnel can access sensitive data and preventing unauthorized shoulder surfing incidents.

In addition to these core features, HCLTech Onlooker Detection offers:

- **Silent installation:** Enhance user experience with seamless and non-disruptive installation processes, minimizing downtime and maximizing productivity.
- **Engaging user experience:** Engage users at different levels with intuitive interfaces and user-friendly features, ensuring that security protocols are embraced and adhered to across your organization.
- **Flexible deployment options:** Choose from various options tailored to your needs, offering scalability and affordability without compromising security.

Use cases:

These use cases illustrate how HCLTech Onlooker Detection, optimized by the AI capabilities of Intel core ultra-processor and OpenVINO™, optimizes resource utilization, drives efficiency and delivers exceptional employee experiences within security measures.

Enhancing user onboarding, identity verification and user privacy:

- **Scenario:** To ensure secure access to the system, users must authenticate their identity for each login instance. This authentication process establishes a baseline of user identity, which is crucial for ensuring authenticity and preventing unauthorized access. Furthermore, users can rest assured that Detection mechanisms remain localized on their machines until a violation occurs. This approach preserves user privacy and data integrity while maintaining robust security measures within the system.
- **Solution:** Onlooker Detection enhances system security by implementing user authentication mechanisms for each login instance, ensuring only authorized users gain access. This is achieved through identity verification, which establishes a reliable baseline for access control and security measures. Additionally, Onlooker Detection

maintains Detection processes on the local machine until a violation occurs, effectively preserving user privacy and data integrity while upholding robust security standards.

- **Results:** Enhanced security is achieved through individual user authentication for every login instance, reducing the risk of unauthorized access and potential security breaches. This approach improves security by verifying user identities and providing enhanced protection against identity theft and unauthorized system access. Additionally, it fosters user trust and confidence by implementing privacy-preserving security measures. Moreover, it ensures increased compliance with regulatory requirements and industry data privacy and protection standards.

Unwavering smart IT:

- **Scenario:** Users require a comprehensive system check to ensure compatibility and optimal performance of the Onlooker detection application. Organizations seek to monitor user behavior through webcam-based surveillance to prevent security breaches effectively. Users also need clear visibility of their machine's location for tracking devices in case of theft or loss. The system must detect suspicious activities, such as talking on the phone or taking pictures, to prevent security breaches and maintain compliance standards. Additionally, it should track and flag violations for suspicious facial activities and detect unauthorized faces in the camera view to prevent unauthorized access and security breaches. Finally, users require the ability to lock the screen to prevent data loss or theft when the device is not in use.

- **Solution:** Onlooker Detection ensures smooth operation by conducting system checks for compatibility and functionality on user devices. It employs webcam-based surveillance to monitor real-time user behavior and detect suspicious activities. The application also provides clear device location visibility for effective tracking and employs algorithms to flag suspicious behavior, triggering alerts. It incorporates facial recognition technology for enhanced access control and auto-starts on boot for uninterrupted usage. Additionally, it offers tracking control features like screen locking to prevent unauthorized access or data breaches when the system is idle.

- **Results:** The Onlooker Detection application enhances user experience with optimized performance and automatic start-up, reducing errors and compatibility issues. It proactively monitors user activities for better security, improves asset management by accurately tracking machine locations and strengthens security posture by proactively detecting suspicious behaviors and facial activities. It ensures compliance with regulatory requirements for user monitoring while increasing efficiency and productivity, ultimately enhancing control and protection of sensitive information.

Tap on user behavioral aspects and protect the Organization's reputation:

- **Scenario:** Users require proactive Detection of external devices before sessions to mitigate potential security risks. Additionally, they must detect if the active screen is left unattended to prevent unauthorized access or data breaches. The system must capture activities such as taking photos of the screen to prevent unauthorized data copying. Furthermore, users must detect shoulder surfing by capturing background movement to prevent unauthorized access.

- **Solution:** Onlooker Detection enhances security by sending email notifications for multiple breaches, ensuring timely response. It detects unauthorized devices, unattended screens and suspicious activities like screen photos while identifying shoulder surfing attempts. Email notifications are sent to managers or HR in case of breaches.

- **Results:** Improved security posture is ensured by proactively detecting unauthorized external devices, reducing data breach risks. Real-time Detection of unattended screens and proactive prevention of unauthorized data copying bolster data security. Strengthened surveillance detects shoulder surfing attempts, reducing unauthorized access risks. Timely notifications of breaches enhance incident response, fostering accountability and adherence to security protocols.

Key Industries and roles that can benefit from HCLTech Onlooker Detection:

Onlooker Detection can effectively address the diverse needs and concerns related to user onboarding, identity verification and user privacy in various organizational settings.

Enterprise IT departments: IT administrators and managers responsible for managing system security, identity verification and user privacy within their organizations.

Compliance officers: Professionals ensure the organization adheres to regulatory requirements and industry data privacy and security standards.

Security professionals: Individuals responsible for implementing and managing security solutions to prevent unauthorized access, data breaches and identity theft.

End users: Employees and system users who require secure access to the organization's resources while maintaining their privacy and data integrity.

IT security consultants: Consultants and advisors who assist organizations in evaluating, implementing and managing security solutions to enhance their overall cybersecurity posture.

Regulatory bodies and auditors: Entities responsible for assessing and verifying the organization's compliance with data privacy regulations and security standards.

Industry associations: Organizations and groups focused on promoting cybersecurity best practices and facilitating knowledge sharing among professionals in the field.

Why HCLTech?

Experience the future of cybersecurity with HCLTech Onlooker Detection

Discover how our solution provides top-notch security, privacy and identity verification to keep your business safe and resilient

Embrace innovation and redefine cybersecurity for the digital age with Onlooker Detection by HCLTech

For more information, please write us at: IntelEBU@hcl.com / dwp@hcl.com

HCLTech | Supercharging Progress™

hcltech.com