Share Data While Helping to Protect User Privacy

An Intel and SAP solution enhances protection of sensitive data.

intel + SAP

Data insights delivered with privacy-preserving analytics

Organizations, businesses, and government agencies want to harness the benefits of cloud and software-defined infrastructure (SDI). They also want to be able to take advantage of computing at the edge to use business intelligence/machine learning (ML) and real-time analytics. But they must also protect the data in these systems, raising a difficult dual challenge. Data must be made available across platforms, applications, and environments. Yet data must simultaneously be protected from breaches and managed in strict compliance with local privacy laws and regulations, especially when it comes to personal health and financial information.

One approach to protecting healthcare data during a pandemic, when information needs to be shared for public safety, is the Pandemic Cohort Management Suite developed by Intel and SAP. Built on 3rd Generation Intel® Xeon® Scalable processors with Intel® Software Guard Extensions (Intel SGX) and SAP Business Technology Platform, the suite is an end-to-end digital solution that enables large amounts of data to be captured and accessed quickly by a large number of users, while keeping that data private during use. Data is normally encrypted at rest, in storage, and in transit, but there is a demand to ensure that it is always protected, even while it is being processed. The goal of the suite is to help individuals, businesses, city agencies, and governments manage in-person activities to help minimize the spread of disease while keeping personal data private.

Optimizing risk management for individuals and large groups

The Pandemic Cohort Management Suite is a risk-data-management solution that enhances the safety of activities during a pandemic by addressing both prevention and mitigation measures. Prevention measures are recommended based on individual and collective risk profiles and might include participation and distancing practices, in addition to guidelines that help safely conduct group activities. Mitigation measures are achieved through digitizing end-to-end test/trace/isolate/support strategies. By digitizing both prevention and mitigation measures, the suite can help businesses and governments avoid repeated closures and lockdowns, allow social and economic activities to occur, and reduce the risk of pandemic "pushes" (infection outbreaks).

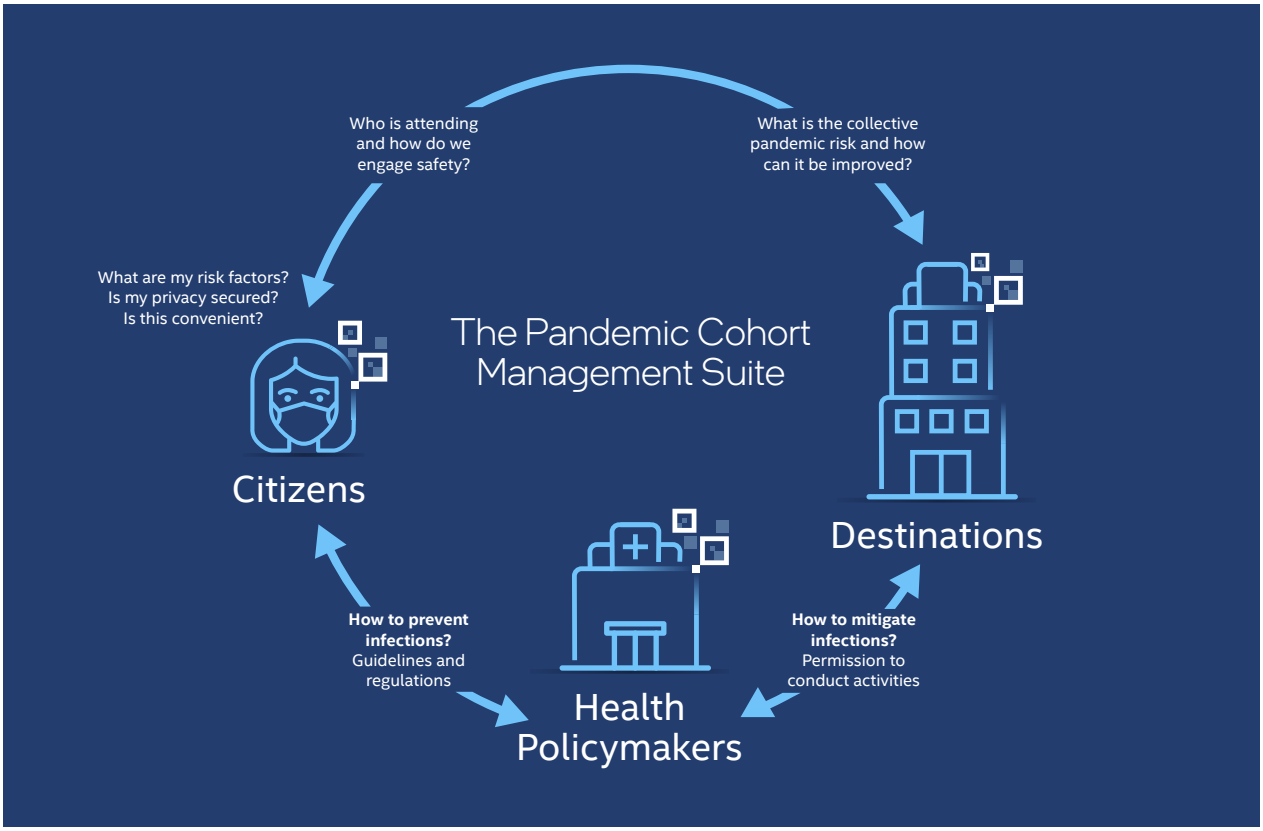


Figure 1. The Pandemic Cohort Management Suite gathers and shares data from citizens, destinations, and government health departments to support both prevention and mitigation measures during pandemics

How it works

The Pandemic Cohort Management Suite pulls together data from different sources to enable users (individuals, organizations, businesses, or government agencies) to better plan and execute in-person activities. It enhances the understanding of the risk of infection at events and workplaces, for example, and helps organizations decide how to minimize such risk for mutual safety. It scales from personal and small-business use up to enterprise and public-health-agency use in larger areas such as towns, cities, and states. The underlying concept for the suite is to offer an alternative to lockdown by digitizing the management of in-person activities from end to end.

> "We need the data and are all looking for tools that give us the needed security and privacy. And that's what the Intel and SAP solution is doing. "
>
> — Mayor Eckart Würzner, City of Heidelberg, Germany

In a typical group-event scenario, each individual attendee downloads a mobile app onto a smartphone that connects to a virtual machine (VM) with Intel SGX. Intel SGX creates security-enabled enclaves in memory where data and application code are protected and private while in use. This app is a virtual "pandemic wallet" that, like a real wallet, holds valuable, encrypted personal data (including name, address, testing, tracing, vaccination credentials, and current health and symptom details) that only the individual can view. The app's main function is to calculate the person's risk of being infectious or becoming infected during specific activities that the person is planning to do. This risk is based both on medical data, such as test results or symptoms, and the activities of the person during the past 14 days, stored in the personal pandemic-diary section of the app.

Managing personal risk is a convenient process. For example, by reading a Quick Response (QR) code before checking in to an event, an individual can see whether it is actually safe to engage at the event. The event organizer is also enabled to manage who can attend in person and who would do better to attend from a separated, safe area or participating virtually.

In a business meeting example, the event organizer can send each individual a digital invitation through a web-based meeting-planner app built on SAP Business Technology Platform. To attend the in-person event, invitees are required by the meeting planner app to provide health-survey data in their pandemic wallet that will help gauge the level of risk for the event. Invitees simply confirm attendance in the wallet after scanning a QR code or following a link in the invite.

The organizer can then view the status of attendee responses on a dashboard, but not any private health information from the attendees. At no point in time is any health information in the meeting planner system. The heart of the Pandemic Cohort Management Suite is the Confidential Compute Service built on Intel SGX that performs the confidential “in use” computing of collective risk calculations and creates recommendations on how to conduct the event.

“The solution encrypts that data in your wallet and on servers that perform the risk calculation at the CPU level, so data is never shared,” says Kai Wussow, head of digital transformation at SAP. “Typically, data is unencrypted at the CPU level to read the data. But with Intel Xeon Scalable processors with Intel SGX, the data remains encrypted while it is still able to be read.”

In addition to helping event organizers, the digitized solution helps public health officials investigate and isolate recent contacts of an infected person to break the chain of infection much faster than previously possible.

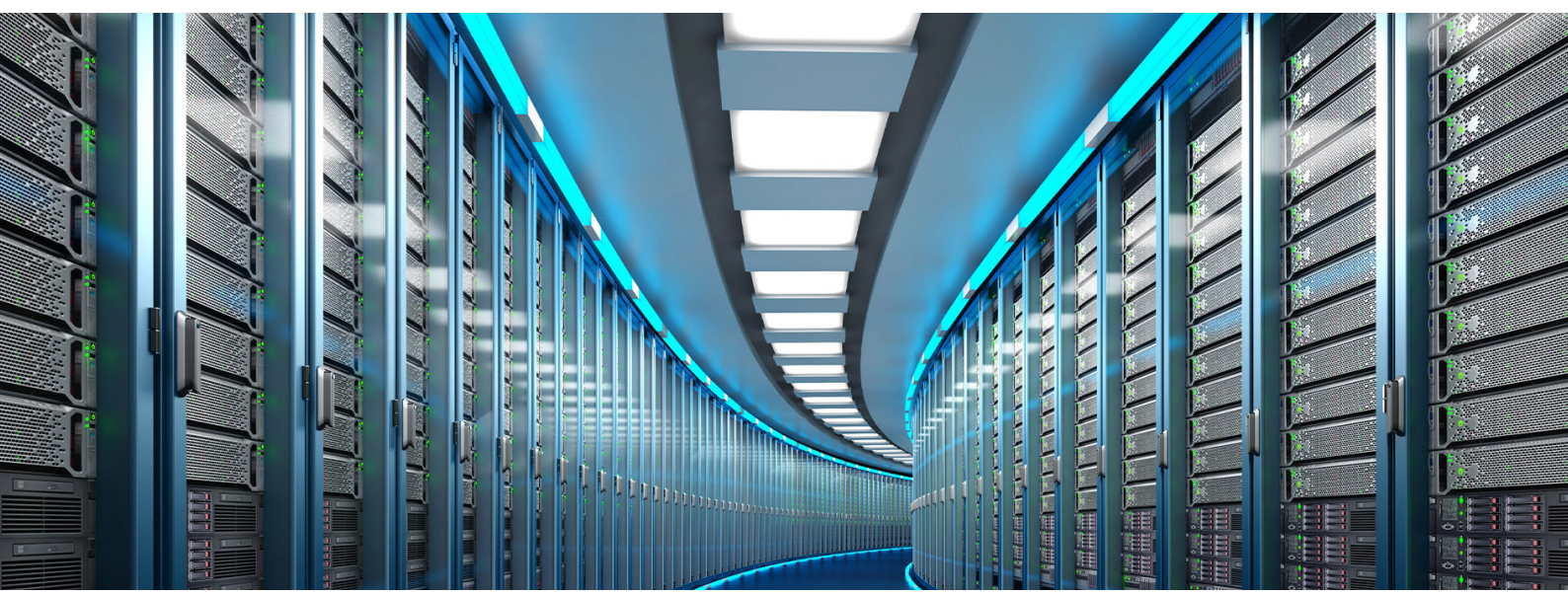
> "With Intel Xeon Scalable processors with Intel SGX, the data remains encrypted while it is still able to be read."
>
> — Kai Wussow, head of digital transformation at SAP

A solution with privacy built into the design

Any application, no matter how essential, will not be adopted widely unless users are assured that their most personal data is always protected and private. In addition, companies often do not want to store personal health data on their information technology (IT) systems. Government health departments want these types of data to be protected, but they still need to be able to mitigate any spread of infection. A critical component of the Pandemic Cohort Management Suite, therefore, is Intel SGX, which helps protect data and application code while in use.

Confidential Computing protects data in use by performing computation in a hardware-based Trusted Execution Environment (TEE). These isolated environments help to prevent unauthorized access or modification of applications and data while they are in use, thereby increasing the security level of enterprises that manage sensitive data and are required to compute on that private data. Intel SGX, which supports workloads with demands of up to 1 TB of memory, is one of the most tested, researched, and deployed TEEs in the data center, with a small attack surface within the system.[1] Intel SGX is designed to be regularly updated for continuous hardening against attacks. Ongoing collaboration with researchers and partners in the Confidential Computing Consortium helps Intel identify and mitigate vulnerabilities quickly.

Along with other Intel security technologies, Intel SGX can help protect sensitive data without compromising performance on 3rd Generation Intel Xeon Scalable processors. Intel Platform Firmware Resilience helps defend the underlying firmware layer to help protect against permanent denial-of-service attacks. And new crypto accelerators enhance performance for widely deployed cryptographic algorithms.



Use the power of data for safer activities

The Pandemic Cohort Management Suite is being tested in the real world at the global SAP Experience Centers, including the headquarters center in Walldorf, Germany. The Walldorf center is a state-of-the-art space for customers to collaborate with SAP engineers and innovate new solutions. When the pandemic started, these events went virtual, but since June 2020, the Walldorf center reopened with a hybrid approach of virtual and in-person attendance.

"We have to make customers and employees feel safe when they come to the center. They wear masks and practice good hygiene, and we have to be able to collect their data in a way that is GDPR [General Data Protection Regulation] compliant," explains Heather Morrison, Head of Global SAP Experience Centers.

The city of Heidelberg, in Germany, is also scheduled to pilot the solution. "This is exactly what we need," says Heidelberg mayor Eckart Würzner. "We need the data and are all looking for tools that give us the needed security and privacy. And that's what the Intel and SAP solution is doing."

> "This solution will help us host everyone on-site and determine what that on-site experience is like. Intel SGX allows us to have that data available to us but keep it safe and secure."
>
> — Heather Morrison, Head of Global SAP Experience Centers

A partnership that helps unlock the value of data today

The connected world exposes valuable data assets, and privacy concerns and regulations add to the challenges of finding the right solution. Intel and SAP are working together to help protect data integrity and personal privacy in powerful end-to-end solutions.

To learn more about Intel and SAP innovations, visit intel.com/sap.

[1] Intel. “Intel® SGX: Moving Beyond Encrypted Data to Encrypted Computing.” intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions-enhanced-data-protection.html.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Printed in USA 0321/VS/PRW/PDF Please Recycle 346525-001US