MARKETSANDMARKETS™

SAFEGUARDING DATA

IN MODERN BUSINESSES

SECURITY SCENARIO IN THE CLOUD AGE…

With a wider adoption of cloud computing and big data, data security and protection have become serious concerns. In recent times industry has witnessed disastrous cybersecurity attacks, which have led to severe data breaches and monetary damages. Several new server attacks and malware have shaken data security providers. These attacks have been aimed at accessing encrypted system files and critical data. For example, A. P. Mollar–Maersk, a container shipping company, faced a loss of USD$300 million due to NotPetya cyber-attack. Loss of security control in the cloud-based infrastructure is another critical security challenge. It is driving industry giants to improve their security infrastructure by enhancing runtime encryption, hardware-based security, and side-channel security. It will ultimately minimize data breaches.

CHALLENGES

Although cloud computing is widely adopted due to several benefits such as availability, flexibility, and economy, the cloud has been constantly witnessing severe security breaches. Cloud service providers are striving hard to keep their customer data safe. However, cloud security varies significantly, and various cloud service providers offer different levels of security. Therefore, enhanced security technologies are essential to protect the critical data. Developers require a trustworthy execution environment where they can run their sensitive application codes without exposing their data. The following are the top 3 challenges that need to be addressed for enhanced security:

REMOTE ATTESTATION

In the expanded cloud environment, the client-server infrastructure needs robust security. Server machines need to validate the hardware and software configuration of client machines. It is achieved through remote attestation. The key challenges of remote attestation are given below:

- At present, the remote attestation mechanism is not considered sufficient to spot and fix runtime data attacks. Establishing a protected client-server communication to handle runtime attacks has become a major challenge.
- Existing remote attestation sometimes fails to maintain a “whitelist” (a list of client machines that are supposed to be validated by the server machine). The regularly updated whitelist is a critical requirement to avoid data breaches while using remote attestation.

RUNTIME ENCRYPTION

Encryption is a classic method for data protection and is considered useful to grant access to privileged users. However, its usage is restricted to “data at rest” and “data at motion.” Data encryption is no longer an iron shield, as it has failed in the past to prevent advanced cyber-attacks, resulting in major data losses. For example, the Bitcoin trading platform “Bitfinex” was attacked in 2016 and the secure key-exchange architecture of the company was weakened. Consequently, the company lost USD$65 million. To avoid such failures, runtime execution of applications needs robust security solutions to safeguard secret keys from threats posed by network intruders, malicious internal users, and root users.

SIDE-CHANNEL ATTACK

A side-channel attack is a major challenge faced by security vendors. Side-channel attacks extract confidential data from systems by targeting the system operations instead of the flaws in the security software algorithms. System usage is observed by the attackers to create patterns to exploit critical data.

FOLLOWING ARE THE MOST USED METHODS TO EXPLOIT SIDE CHANNELS FOR HACKING:

- **CACHE ATTACKS:** Here cache activities in a shared physical structure are screened by attackers to hack the private data. As these attacks are based on abusing CPU architecture, mitigating them is a critical challenge for the security architects. Such attacks are frequently observed in cloud/virtual environments.

  National Cybersecurity and Communications Integration Center (NCCIC) has explored a set of system vulnerabilities called Meltdown and Spectre. These weaknesses are exploited to create cache attacks.

- **TIMING ATTACKS:** Attackers analyze the execution time taken by the cryptographic algorithms during the execution of applications/private codes. They leverage this information for creating patterns to get access to these applications/private codes. Different parameters, such as design of cryptosystems, system implementation details, and accuracy of the time measurements decide the value of secret data for attackers.

SOLUTIONS AVAILABLE TO TACKLE THE CHALLENGES

Secure architecture for executing applications and code is now a necessity for software architects and application developers. Industry giants have come up with cutting-edge security technologies to address the various challenges and attacks discussed above. FileFlex Enterprise™, developed by Qnext® Corp., is a 'hardened' silicon-to-silicon remote access, sharing and collaboration solution that can be integrated with Intel Software Guard Extensions (Intel SGX). It provides remote sharing and collaboration solutions that do not require the cloud. The following section explain how FileFlex Enterprise uses Intel SGX platform hardening in brief.

INTEL SGX

Intel SGX is a technology designed exclusively for application developers. The technology comprises a set of CPU and platform enhancements that enable application developers to execute their computations in an exclusive and safe environment. Using SGX, application coders can create a secluded area called an "enclave" (an isolated part of memory), in which selective code can be executed independent of any other system process and without any alteration. These enclaves offer runtime encryption by taking care of encryption keys and selective code and providing protection against various attacks.

SGX leads to an uninterrupted application execution despite compromised Basic Input/Output System (BIOS) or Virtual Machine Manager (VMM) and/or any malware with access to OS privileges. The following 2 figures explain application execution with and without Intel SGX.

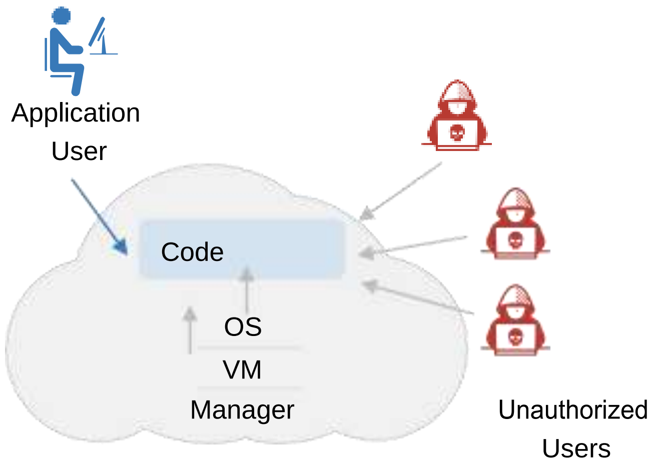


Fig. Runtime Encryption without Intel SGX

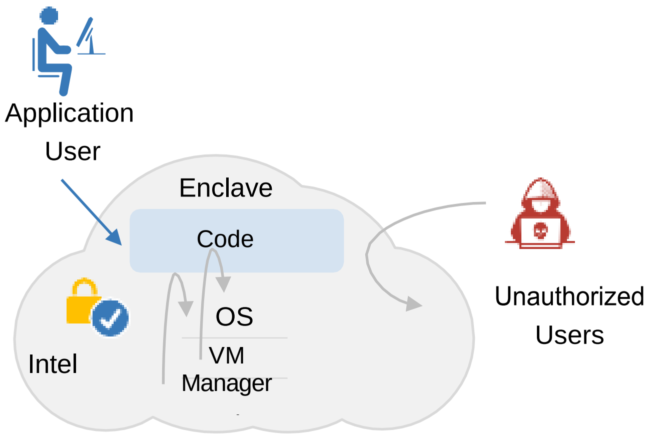


Fig. Runtime Encryption with Intel SGX

FILEFLEX ENTERPRISE WITH INTEL SGX

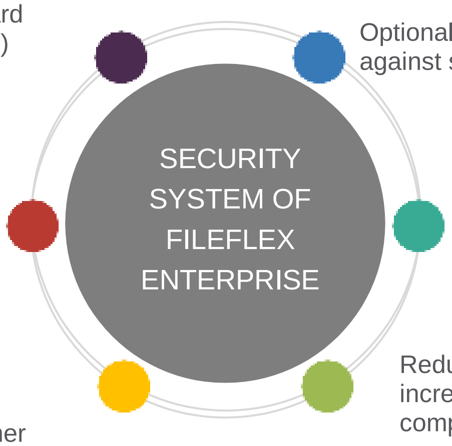
FileFlex Enterprise uses decentralized cloud or edge cloud technology that leverages the storage and CPU power of edge devices to allow users to access, share, stream, and collaborate data from source locations without using a traditional centralized cloud repository. When FileFlex Enterprise is combined with Intel SGX technology, it offers fully encrypted, silicon-hardened, hybrid point-to-point communication with no duplication and no uploads to third parties. Intel SGX technology provides hardened crypto-functionality using Intel Software Guard Extensions (Intel SGX) at the endpoint to provide added protections within the silicon itself against shared data being snooped or tampered with at any stage of access or transmission. FileFlex Enterprise uses the secure enclaves to provide added protection below the application layer, below the OS level, and below the BIOS. This enables secure file sharing at the deepest level, within the silicon itself.

With FileFlex Enterprise you get a reduced threat surface and simplified storage structure. Governance, risk management, and compliance are now back under organizational control - all of which translates into a lower risk posture. It includes version control, file locking, a unified workflow across devices, and a Content Collaboration Platform (CCP) which does not duplicate or sync content to a secondary location or third-party server. It supports two-factor authentication (2FA), device authentication, and AES 256 encrypted hybrid point-to-point communication for security. And it provides a real-time audit trail and user-controlled data residency to aid compliance to privacy regulations such as GDPR and HIPAA.

BENEFITS OF FILEFLEX ENTERPRISE WITH INTEL SGX

Intel SGX brings a fundamental change to security by providing hardware-level trusted execution of applications. FileFlex leverages Intel SGX to provide platform hardened generation of encryption keys. When used with Intel SGX, FileFlex can deliver enhanced integrity and enhanced security of all data that is accessed by a user and with improved prevention of man-in-the-middle, impersonation, snooping, and intercept attacks even on a system that is compromised (at the application level).

FileFlex Enterprise offers additional unprecedented improvements in security and benefits in file sharing and collaboration, such as:



Supports SSO by using SAML (Security Assertion Markup Language) open standard and OneLogIn (a custom version of SAML)

Optional double encryption brings extra protection against snooping and intercept

Two-factor and device authentication provide added protection in that only authorized users can access the storage infrastructure through FileFlex Enterprise, even if someone knows the password of one of your users.

Files are not copied or duplicated to third-party servers to improve protection of privacy of confidential documents and reduce possible secret exfiltration.

Reduces the organization’s attack surface while increasing governance, risk management and compliance (GRC) control

Aids compliance to HIPAA, GDPR and other privacy regulations

MARKETSANDMARKETS’ PERSPECTIVE

Combining Intel SGX technology with FileFlex Enterprise provides a solution that offers confidentiality, integrity, and high-grade security with a minimal impact on existing processes and infrastructure. It is a perfect example of an edge computing solution as it shows how processors with embedded applications can play a significant role as an alternative to existing cloud solutions. Intel SGX technology uses secure enclaves to provide additional security within the silicon itself against shared data being snooped or interfered with at any stage of access or transmission.

FileFlex Enterprise combined with Intel SGX addresses security challenges and strengthens the security of modern enterprises. The technology can be considered highly beneficial for data-sensitive verticals, such as Financial Services, Healthcare, Government, IT Services, and Defense.

ABOUT MARKETSANDMARKETS™

MarketsandMarkets™ is the world's largest revenue impact company, serving over 7500 customers. 80% of top 2000 companies globally rely on us for identifying new high growth and niche revenue opportunities.

In the face of constant technology innovation and market disruption, we help organizations plan and operationalize their future revenue mix decisions by identifying over 30,000 high growth opportunities ranging from $1B to $500B across 90+ industry trends and markets. Organizations choose MarketsandMarkets™ to stay ahead of the curve and accelerate their revenue decisions and implementations by 6 – 12 months, giving them a unique, first-mover advantage.

Our revenue impact methodology provides quantified and actionable insights on converged, granular and connected market eco-systems that result from disruptive technologies and high-growth markets. We provide an extended lens on not only what will impact our client's revenue but also what will impact their clients' revenues, continually uncovering latent opportunities.

We work across all major B2B industries with C-level executives in functions such as Strategy, Marketing, Sales, R&D, Product, and M&A. MarketsandMarkets™ brings exclusive high-growth markets intelligence generated by over 850 SMEs and analysts along with its proprietary Revenue Impact platform (Knowledge Store).

For more information, please visit: **www.marketsandmarkets.com**

Intel®, Intel Data Guard and Intel vPro are trademarks belonging to Intel Corporation. FileFlex, FileFlex Enterprise and Qnext Corp are trademarks of Qnext Corp.