A Quick Guide to GDPR and Scale Computing Solutions

Introduction

Scale Computing is a market leader in IT virtualization infrastructure providing award-winning solutions around the world. As greater threats to data privacy and security emerge, new regulations like GDPR aim to protect both individuals and organizations from bad actors. This guide will provide insight as to what GDPR means for Scale Computing solutions.

What is GDPR?

GDPR (an acronym for General Data Protection Regulation) is a new law of the European Union (EU) that affects any entity around the world processing personal data originating in the European Economic Area[1]. The specifics of the GDPR are lengthy and largely relate to the processes of collecting, transferring, and retaining data. The regulations also cover the IT infrastructure systems housing the data and the actual data processing.

Like most regulations, GDPR does not get very specific when it comes to technology and implementation but rather provides more general statements regarding security. GDPR attempts to generally define higher standards by which data must be made private and protected and how an organization must react if there is a data breach. With the fast pace of technology innovation, these standards guide how IT vendors design solutions with data security in mind.

How does GDPR affect Scale Computing products and solutions?

Scale Computing provides IT virtualization infrastructure solutions which are a platform on which data storage and processing take place. Access to the infrastructure is a data security concern and the built in data protection features of the HC3 platform can be used to satisfy GDPR compliance. The inherent architectural security design considerations of HC3 places it well within both the spirit and the letter of GDPR.

HC3 Architecture Considerations

Single Vendor Solution

HC3 is a system that combines servers, storage, virtualization, and backup/disaster recovery into single solution. Because these solution components are not provided from different vendors, there are not separate authentication points for each component. Instead there is a single access and authentication point for administration. This significantly reduces the surface area available to unauthorized access attempts.

Restriction of Root Access

HC3 restricts root-level access even from administrators. As an appliance-based virtualization approach, administrators cannot access root functions but instead must contact Scale Computing customer support, further reducing the surface area for attack and adding an additional layer of access protection.

[1] The European Economic Area is comprised of the EU member states, as well as Iceland, Liechtenstein and Norway.

Network Access Isolation

Administrators can further restrict system access by isolating administrator access on a separate VLAN, preventing all other users from even accessing the access point. Users are then restricted to applications or guest virtual machine operating systems on the VLAN designated for those users.

High Availability

In the event of an outage or disaster, HC3 has redundancies and failover capabilities to allow data to be back online within minutes and with both administrator and user access. Even when failing over between on-prem and cloud instances, authorized access can be carried over seamlessly through L2 networking. Continuous replication ensures data is up to date locally or remotely.

Backup and Snapshots

Backups and snapshots can keep data protected against either disaster or attacks such as ransomware. Scheduled point-in-time backups or snapshots can be used to recover user data granularly as needed or to revert a virtual machine back to a previous point int time, before data corruption of malicious attack. For example, in the event of a ransomware attack against a virtual machine, the machine can be reverted to a snapshot before the attack, eliminating the ransomware. Additionally, backups and snapshots can be managed with retention policies to be eliminated after a certain period of time to remain in compliance.

Multi-Admin Auditing

With multiple admin accounts setup to manage HC3, the account activity is logged and can be audited to track administrator actions. This auditing can be used to monitor activities that could possibly compromise data security.

Development Processes and Design Goals

As Scale Computing continues to innovate with new technologies, we will continue to keep data protection and security a top goal. We will continue building in newer and better security measures as technology innovation advances, and further develop processes that ensure a more secure infrastructure platform.

Single Vendor Updates

As mentioned earlier, a single vendor has advantages in shrinking the surface area for attacks, but it also speeds the response time for correcting potential security risks. In a multi-vendor solution, an exposed security risk may be present in multiple solutions. With HC3 a single security patch covers the entire system from storage to hypervisor to server hardware. It also mitigates the risk that a patch on one vendor component breaks or exposes another vendor component.

Rapid Response Time

Our Agile test and development methodology helps shorten the time from development to release, getting critical security fixes to you sooner than later. Our development teams prioritize data security issues to deliver fixes as quickly as possible with quality peer reviewed and tested code.

Expert-Driven Delivery

Some of our updates are delivered directly through our user interface with a completely automated process that can be initiated at the user end. Others may be released through our support function and applied with the assistance of our expert ScaleCare Support Engineers. Either way, the updates are being applied by Scale Computing automated processes or our own experts, not by untrained administrators or third-party providers. As mentioned earlier, root-level access is restricted to prevent unwanted system changes that could jeopardize system integrity by non-experts.

Simplicity by Design

HC3 is a solution designed to shed the complexity and associated costs of traditional infrastructure solutions. Simplicity and ease-of-use include providing a secure system design that doesn't require a security expert to maintain. We will continue to develop toward the design goals of simplicity and ease of use as we continue innovating to provide a secure infrastructure platform for nearly any organization.

More information on security features can be found in our *HC3 Information Security whitepaper*.

How does HC3 help your organization comply with GDPR?

As an infrastructure platform, HC3 can be used to store and process data in compliance with GDPR but your business processes and operations, running on the virtual machines and applications you create and install, fall under different areas of the GDPR regulations. HC3 acts as a stable and secure platform onto which you can install and run whatever virtual machines and applications are needed to properly handle user data in compliance with GDPR.

In addition to the applications needed to execute your business processes and operations, you may also deploy other third party tools to further secure data within your applications. We've worked with one of our technology partners, *WinMagic*, to help our customers use SecureDoc for additional encryption to secure data. Other HC3 users have looked at F5 BIG-IP APM to provide enhanced access policy management for their HC3 systems. HC3 is a virtualization platform that supports nearly any x86 operating system or application, making it flexible enough to use nearly any security tools needed.

Summary

GDPR is merely one of many regulations that will be passed to protect data around the world during this century. As data is an increasingly valuable commodity, threats will continue to emerge and technologies will advance to continue to counter these threats. The unique design of HC3 along with the development processes and commitment to excellence will continue to put HC3 and Scale Computing ahead of the data protection curve. With HC3, IT administrators can confidently build secure environments that meet the increasing data privacy expectations of users, including those required by GDPR.

Corporate Headquarters
525 S. Meridian Street
Suite 3E
Indianapolis, IN 46225

West Coast Office
360 Ritch Street
Suite 300
San Francisco, CA 94107

EMEA B.V.
Europalaan 28-D
5232BC Den Bosch
The Netherlands

www.scalecomputing.com

1-877-SCALE-59 (877-722-5359)