Solution Brief

Entrust for a Secure Multi-Tenant IT Infrastructure

ENTRUST

SECURING A WORLD IN MOTION

A solution that delivers

In this paper, we examine the challenges IT organizations face within regulated environments, where encryption and compliance are necessities. Entrust provides a secure, multi-tenant infrastructure solution that delivers the performance, scale, and efficiency required of cloud and virtualized data centers – as well as the required levels of data protection and security controls needed to simplify regulatory compliance and safeguard against the risk of breaches and other attacks.

The business challenge

Regulatory compliance is becoming more and more commonplace in the market today, with GDPR in Europe, sovereign data controls in countries like Germany, and the client privacy requirements in the US, such as HIPAA in healthcare. IT organizations must understand and enact compliance on a much deeper level than ever before. There are several available solutions, although many of them require sacrifices and compromises to be made in terms of performance and data services.

Hardware solutions

Self-Encrypting Drives (SEDs) are the most common hardware solutions in the market, but they are often expensive and take a blanket approach to encryption. There is also the added performance penalty associated with the drives performing the encryption, reducing the overall performance of the infrastructure solution, with extreme latency potentially causing failures.

Software solutions

Other solutions require the administrator to encrypt the ESXi cluster and to ensure that every member of the cluster, and their associated datastores, are being encrypted. This results in several phases of the data path being encrypted and decrypted as data services are applied to the data when it passes through the IO Stack. While this is more granular, the risks associated with potential inflight data capture and the encryption/decryption process make it a less secure solution than the SED option.

Software solutions can also require many kernel changes are made to the VMs that are being protected, to install an agent that protects data inflight, leading to a host of interoperability headaches, and ensuring that only certain patches are applied to application servers to ensure continuing compliance and protection.

Additional considerations

It is often the case that not every piece of data in the environment needs to be encrypted, or is considered sensitive, which means that these blanket solutions are often unnecessary and drive the cost of the solution upwards, reducing the amount of budget available for expansion, or additional beneficial products.

The other major considerations in sensitive environments are key management and multi-tenancy, whether that is multi-tenancy through departmental division, or multi-tenancy in the truest sense, with multiple organizations securely housing data on the same infrastructure.

These challenges are exacerbated when you wish to take advantage of the new infrastructure developments that HCI offers, as SEDs are either not an option with the HCI solution or they are only available at a significant extra cost. One must also sacrifice several post-process data services, such as erasure coding, deduplication, and compression, as encrypted data can't be processed once it has been encrypted.

"Entrust provides a secure, multi-tenant infrastructure solution that delivers the performance, scale, and efficiency required of cloud and virtualized data centers as well as the required levels of data protection and security controls needed to simplify regulatory compliance and safeguard against the risk of breaches and other attacks."

The solution

Entrust provides a secure, multi-tenant infrastructure solution that delivers the performance, scale, and efficiency required of cloud and virtualized data centers as well as the required levels of data protection and security controls needed to simplify regulatory compliance and safeguard against the risk of breaches and other attacks.

Both products are managed through policies, meaning that system administrators can approach their environments in a workload-centric manner, simplifying and removing the need for complex hardware infrastructure and enabling a modular, fine-tuned approach.

By removing the requirement for blanket hardware encryption, organizations are able to take advantage of a simple, scalable and modular infrastructure. This facilitates a greater level of agility in the IT organization, enabling a more rapid deployment model, without the (often) long lead times associated with purchasing hardware-based encryption products. Costs are also removed as multiple hardware infrastructures for “Sensitive” and “Non-Sensitive” workloads no longer need to be designed and maintained.

Entrust workload security

Per-VM Encryption

Entrust works on a per-VM model, both in terms of protection and licensing. This gives an unprecedented level of granularity and control to an administrator, allowing them to only encrypt the VMs that they need for compliance or security reasons.

Entrust DataControl supports up to 5,000 encrypted workloads per Entrust KeyControl cluster. There are no limits to the amount of encrypted data other than those imposed by the underlying workload operating system. Customers can choose to protect entire workloads leveraging disk encryption, folder/directory encryption, or individual file encryption. Using disk encryption provides the highest level of workload protection.

Working at the block level, the entire disk is encrypted and any disk can be protected, including boot (C: on Windows or root on Linux). Policies may be set up in Entrust KeyControl to prevent a workload from booting up, or an encrypted data volume from being accessed, when specific conditions apply, such as changes in hardware signature, or even contingent upon hardware attestation, leveraging Entrust CloudControl and Entrust BoundaryControl. Regardless of disk size, disk encryption does not require downtime.

“Dynamic Rekeying” allows encryption to be applied with zero operational downtime, regardless of whether it is during initial encryption or when key rotation is required, a fundamental data security best practice. Note that when performing a rekeying operation with the Entrust Policy Agent, data is never decrypted to disk. From a performance perspective, when an encryption operation is kicked off, the Entrust Policy Agent encrypts data only when disk I/O is idle, preventing the encryption operation from affecting the applications running on the workload. Encryption operations take advantage of AES-NI, hardware cryptographic extensions found in modern Intel and AMD processors.

Key control –The key that ensures enforcement of policy via key issuance and revocation

Policy engine –Ensure appropriate controls with contest; enforces the right admins for creating/modifying encryption policies, identifies workloads and context for policies

Policy agent –Ties policy to workload and executes encryption and decryption

The Entrust Policy Agent detects whether the underlying hardware supports AES-NI and whether it is a virtual machine or physical system. In addition to disk encryption, Entrust DataControl provides folder-level encryption for Linux, enabling the encryption of all files within a specific folder/directory while retaining the high level of key management security. Encryption keys are generated and stored within Entrust KeyControl, delivered securely to only workloads that have been registered with the Entrust KeyControl cluster, while multi-tenancy policies still apply. The encrypted filesystems may also reside on a remote server (e.g., via NFS).

Lastly, file-level encryption can be used to share files securely without the need to directly share encryption keys. A file encrypted from a workload (e.g. server, workstation) that is part of the Entrust DataControl environment can be accessed from any other workload if it is allowed per policy.

"The Entrust Policy Agent detects whether the underlying hardware supports AES-NI and whether it is a virtual machine or physical system. In addition to disk encryption, Entrust DataControl provides folder-level encryption for Linux, enabling the encryption of all files within a specific folder/directory while retaining the high level of key management security."

Secure key management with host attestation

The Entrust KeyControl appliance provides encryption key management and policy definition for the environment. Entrust KeyControl manages keys used for encrypting data so that an administrator never has to handle keys directly unless they wish to, providing a much easier and more automated experience.

Entrust KeyControl is delivered as an OVA image, making it easy to deploy as a virtual appliance within a virtual infrastructure. Deploying the Entrust DataControl solution entails provisioning Entrust KeyControl appliances and deploying the Entrust Policy Agent. For production deployments, leveraging Entrust KeyControl high availability clustering is highly recommended, and multiple Entrust KeyControl appliances can be set up in an Active-Active cluster with up to eight nodes per cluster. Entrust KeyControl nodes within the cluster are kept in sync using TCP/IP ports 2525, 2526 and 8443, allowing deployments across datacenters.

Once the Entrust KeyControl infrastructure is in place, the Entrust Policy Agent is deployed on chosen workloads. The Policy Agent is unique in that it does not require the modification of any kernel drivers – a key difference in approach compared to other alternatives. This means you do not have to worry about updating your workload to a specific operating system or patch level. After the Policy Agent is installed, a mutual trust relationship is established between the workload and the Entrust KeyControl cluster by executing a registration command within the workload. This can be performed interactively by an administrator or unattended via scripting. The Entrust KeyControl appliance is built on a hardened, locked-down FreeBSD OS image. Access through open network ports, root-login, SSH, and other typical means of access are shut down and denied. Additionally, all OS data/files are whitelisted; if an OS file is modified on disk or in memory, it will be replaced with a pristine copy. All encryption keys are generated by Entrust KeyControl and stored within the Object Store. The Object Store is itself encrypted at rest with its own randomly generated Object Store Key, which is ultimately protected by the Administrator's key.

Workloads can move often, sometimes to hosts that may not be trusted. Entrust DataControl integrates with Entrust CloudControl to leverage Intel TXT (Trusted Execution Technology) to provide proof of a host's security state. With this capability, administrators can set policy and determine what to do if a workload is moved onto a host that does not have the appropriate level of security desired.

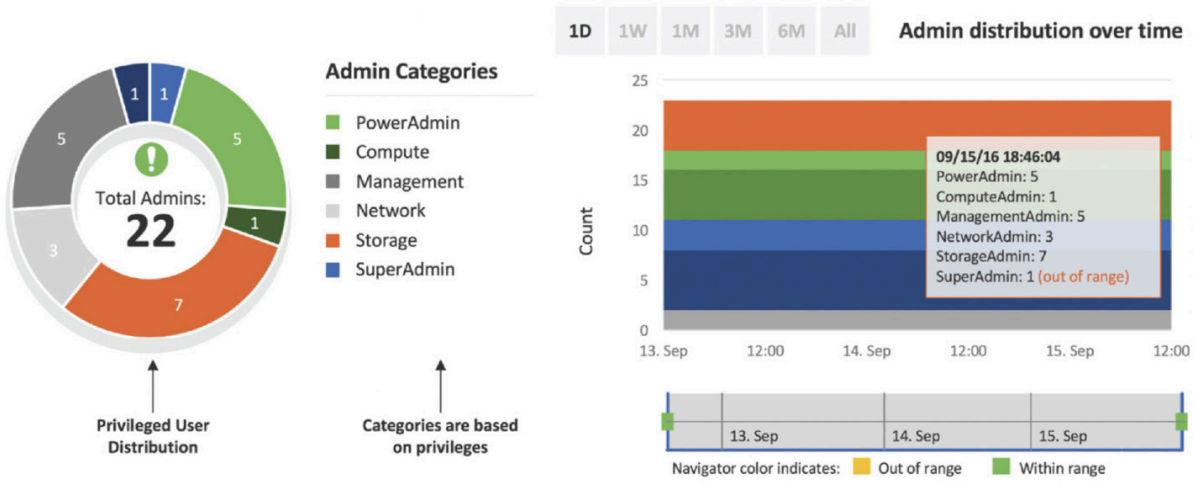
Role-based access controls/role-based monitoring (RBAC/RBM)

One of the most common breaches of secure desktops occurs when administrators have access to content that they shouldn't, by granting privileges designed to allow them to resolve issues and fix problems. This can be a problem where data is sensitive and the VDI solution, or support thereof, is outsourced.

By enabling RBAC, an organization can restrict the administrative privileges of a support engineer to only be able to access, fix, and view the necessary parts of the infrastructure to do their job. When combined with RBM, an organization can watch for "unexpected behaviors" and take appropriate actions. For example, an administrator for the EMEA team copying data from VMs in the USA to a datastore located in APAC, or migrating production VMs to an unexpected cluster, possibly used for test and development, would be flagged.

Tying this into data fencing, particularly in VDI and especially in healthcare, financial services and other industries handling sensitive client data, leads to a more robust and enforceable set of policies and reduces the potential for data breaches.

Beyond RBAC, most organizations also require an efficient and flexible way to:



1. Grant privileged users temporary permissions needed to perform infrequent duties.
2. Have greater control over the use of powerful privileges by users who need those privileges to do their daily jobs.

For example, a virtualization operations group needs ongoing authorization to create and delete VMs used for non-production applications, but management also wants the ability to approve or deny any attempt by this group to delete a production virtual machine.

"By combining Entrust host attestation (with Intel TXT) and data fencing controls, system administrators can ensure that sensitive workloads remain only where they are authorized to run, even in a global infrastructure, simplifying compliance at all times."

Because the VMware platform does not provide a viable way to enable one-time approval of a specific operation attempted by a specific privileged user, organizations have turned to Entrust CloudControl's Secondary Approval capability for both vSphere and NSX operations. From a workflow perspective, this feature allows authorized users to configure Entrust CloudControl to require additional approval before privileged users can perform sensitive or disruptive operations on specific virtual objects (e.g., delete or power off a virtual machine, edit a firewall, or create an edge services gateway). The process requires that a designated group of approvers authorize an operation attempted by a privileged user before that operation can proceed.

Summary

The Entrust Workload Security solutions allows IT organizations to leverage best-in-class solutions to create secure, modular infrastructure that provides the necessary levels of protection and performance where they are needed the most based on business priorities and requirements.

By combining Entrust host attestation (with Intel TXT) and data fencing controls, system administrators can ensure that sensitive workloads remain only where they are authorized to run, even in a global infrastructure, simplifying compliance at all times.

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust is dedicated to securing a world in motion by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com **entrust.com/contact**