Zero Trust Framework for Virtual Infrastructure

Enhanced security controls and compliance automation

Overview

As organizations progressively adopt Zero Trust models to secure an increasingly perimeter-less environment, one area that cannot be overlooked is the security of their virtual infrastructure. To ensure the security of the organization, only authenticated and authorized administrators should have access to the resources they have been allowed to control as part of a comprehensive Zero Trust framework.

The Entrust Zero Trust framework for virtual infrastructure uses Entrust CloudControl to extend security to the virtual infrastructure deployed across distributed private cloud environments. The model operates under the premise that no entity (human or machine) can be trusted by default, and that every request to access virtual resources across data centers and private clouds must be authenticated and authorized before access can be granted.

KEY FEATURES

- Protect against unauthorized access by defining and enforcing access rights and least privilege rules.
- Enforce role- and attribute-based access control (RBAC/ABAC) for virtual administrators by restricting what resources may be accessed and what actions may be taken on resources based on set roles.
- Segment what administrators can do based on their individual privileges.
- Monitor access to all virtual assets to ensure suspicious activity is quickly detected and remediated.
- Disable VMs if moved out of defined area, protecting computing resources from misuse and facilitating geo-fencing requirements.

Learn more about CloudControl at entrust.com

CloudControl - Zero Trust for Virtual Infrastructure

Benefits

The Entrust Zero Trust framework for virtual infrastructure provides comprehensive security to protect against modern threats. The technology suite extends Zero Trust, enabling organizations to enhance their control over the virtual environment, reduce risk of data breaches, and maintain confidentiality, integrity, and availability of critical assets. The components of the solution deliver:

Machine identity: In addition to users, applications, and devices, machines must also be repeatedly authenticated as part of the Zero Trust framework. With Entrust PKI as a component of the Zero Trust framework, the identity of applications, devices, and machines can be consistently and explicitly verified.

Keys and secrets management: Entrust KeyControl extends traditional key management and delivers an innovative centralized/decentralized security model, providing global compliance management and distributed vault-based storage for flexible deployment.

Certified root of trust: Entrust nShield hardware security modules (HSMs) deliver a FIPS 140-2 Level 3 high-entropy source for robust cryptographic key generation and a tamper-resistant environment for safeguarding root keys. Certification to FIPS 140-3 Level 3 is pending final validation.

Secondary approvals: Entrust CloudControl protects the virtual infrastructure by providing a means for defining specific actions that require secondary review prior to execution. This enables organizations to avoid potential costly mistakes.

Boundary controls: Entrust CloudControl enforces regulatory compliance by locking workloads into defined boundaries.

How it Works

Entrust CloudControl enables organizations to adopt a proxy-based approach to establish a control barrier between users and devices and virtual resources. The approach extends the Zero Trust model and enhances the overall security of the organization.

Zero Trust requires improved governance of identity, where access to resources is determined based on factors such as user, asset status, and environmental conditions like time and geolocation of the connection request. By facilitating the integration of a virtual infrastructure with an enterprise ID provider, Entrust CloudControl ensures that every access to virtualized resources undergoes thorough identification, authentication, and authorization.

Multi-factor authentication (MFA) is a prerequisite for implementing Zero Trust. CloudControl enables MFA by integration with an ID provider using standards-based Security Assertion Markup Language/ Open ID Connect (SAML/OIDC). This fulfills mandates that access to resources shall only be granted according to the principles of least privilege, separation of duties, and need-to-know.

CloudControl facilitates the implementation of these principles by providing centralized and granular role-based access management for accessing VMware resources. By leveraging RBAC/ ABAC, CloudControl ensures that users are granted access to resources based on their specific roles and responsibilities within the organization. Roles can

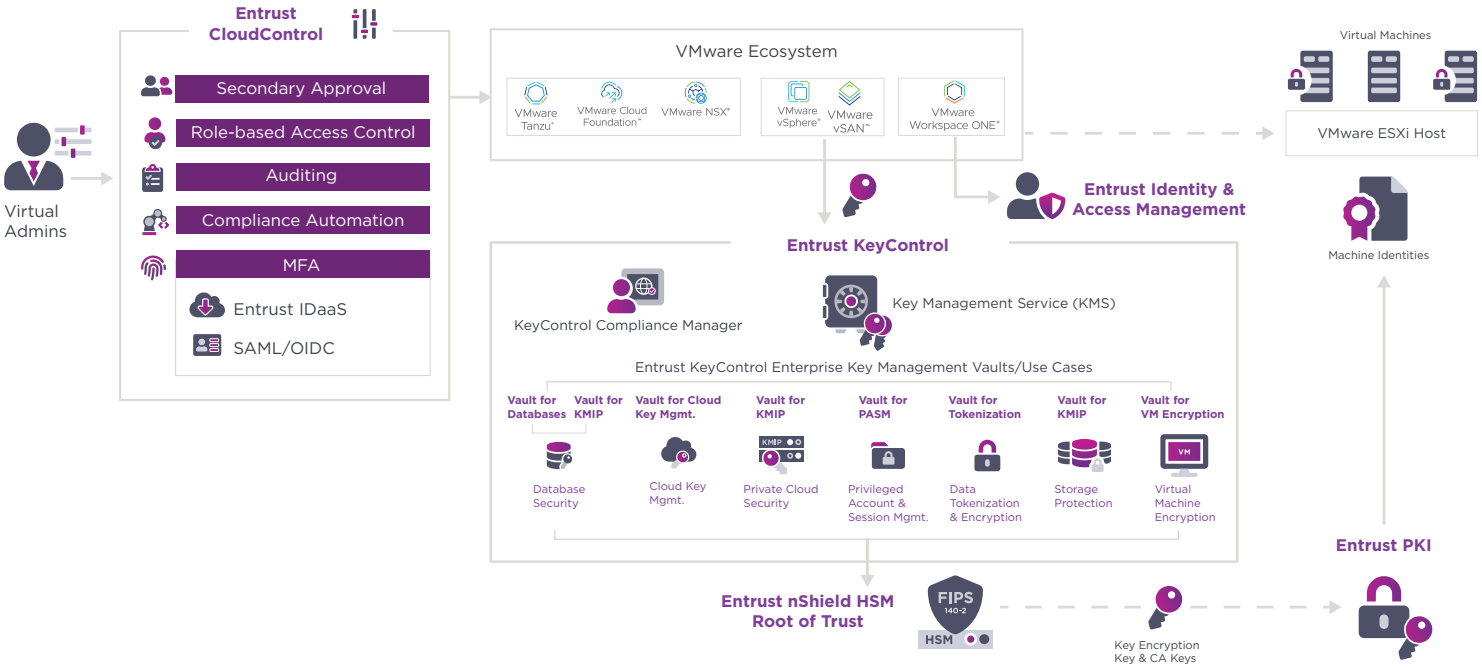
CloudControl - Zero Trust for Virtual Infrastructure

span across the entire VMware infrastructure and can include other components of the infrastructure. All requests for virtualized components are intercepted and assessed based on the role of each user or account making the request prior to granting approval. It is also possible to assign a role to a user based on their ID attributes.

Zero Trust requires the strengthening of detection capabilities; therefore, generated security logs must be accurately configured and centralized in a security information and event management (SIEM) system. CloudControl possesses reporting capabilities and provides intelligence to assist with forensic analysis and troubleshooting. All security events identified by CloudControl can be sent to the SIEM for centralized logging and analysis.

Zero Trust requires a state-of-the-art configuration regarding the security of the infrastructure. The CloudControl compliance engine ensures that the VMware infrastructure remains compliant with security requirements. Automated compliance verification and remediation allows organizations to allocate their staff to focus on higher-value tasks instead of continuously verifying compliance with regulatory or internal security requirements.

Beyond CloudControl's support for the virtual infrastructure, Entrust PKI services can support individual VMware deployments as well as infrastructure components. For individual VMs managed by VMware, the PKI can issue machine identity certificates for domain authentication, typically through Windows auto-enrollment. For VMware infrastructure components, the PKI can also issue and manage machine identity to/for ESXi hosts, TLS/SSL certificates to/for vCenter server nodes, VMware internal service certificates to enable SSO, and VMware SSO signing certificates and keys for signing SAML tokens. The extension of these offerings is illustrated in the figure below.



Learn more about CloudControl at entrust.com

CloudControl - Zero Trust for Virtual Infrastructure

MFA: Via SAML/OIDC integration, Entrust CloudControl provides MFA for VMware vCenter, ESXi, NSX, and SDDC Manager using Entrust Identity as a Service (IDaaS) or any SAML/OIDC compliant solution such as Okta, Ping, or Duo.

Least Privilege Access: Entrust CloudControl maintains a least privilege model by allowing security teams to define in one single document the roles and fine-grained privileges of virtual infrastructure administrators spanning ESXi, vCenter, NSX, and SDDC Manager resources. With its unique proxy approach, Entrust CloudControl transparently enforces privileges on all forms of access (via UI, API, and Command line and even ESXi/SSH) and maintains forensic-level logs with details of all allowed and denied access requests. Security teams can set up very sophisticated policies around what resources may be accessed by which administrators, and what actions can be taken on those resources.

Separation of Duties: Extends VMware controls for separation of duties by making all resources invisible that are not available to admins based on their role. This also provides secure multitenancy.

Encryption: Providing robust data encryption and key management capability for virtual machines protects against data exfiltration, ensuring that even if user or machine credentials are compromised, the attacker still cannot gain access to sensitive plain text information.

Micro-segmentation: Divides the network into smaller, isolated segments to prevent lateral movement by attackers. This means that even if a single segment is compromised, the attacker cannot easily move laterally throughout the network and access other resources.

Continuous monitoring: Uses advanced analytics and machine learning algorithms to identify anomalies and potential threats in real-time. Logging and auditing all activity, including denied requests, the solution delivers comprehensive logs compatible with SIEM platforms for correlation and storage for root cause analysis.

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