Highlights

- KSE™ Servers provably secure access to sensitive data and limit that access to authorized users
- KSE™ Servers ensure that users can only use the data and information for organization's intended purposes.
- KSE™ Servers can create and maintain boundaries to protect against abuse during and after the access to sensitive data
- Powered by Trustifier KSE™ authorization engine that enforces business rules in real-time, KSE™ can meet and exceed regulation mandates and compliances
- Trustifier KSE™ powered Servers stop rogue staffers and spies, including evil system-administrators from abusing access to your sensitive environments.
- Trustifier KSE™ cloud server provides complete private-cloud world for all your systems.
- Trustifier KSE™ Detect and stop malicious activities, including collusion, using Decider™ fuzzy human behavior monitoring system.

# Trustifier KSE™: Insider-threat protection best practices

*Trustifier KSE™ allows you to protect knowledge-assets in a way that creates trust between owners, employees, partners and customers, all the while keeping your most valuable assets safe.*

Security is not about safeguarding your IT infrastructure, it's about safeguarding your business and your organization! Today's attackers are more sophisticated and sinister than ever before and they are not after your computers, they are after the data that's residing on them. Random hacks, defacements and breaches of the perimeter are a thing of the past. Today your hacker may be inside your organization. You, as an owner, may be concerned about rogue or vengeful personnel, staff, or executives; or about spies planted by your competitors. You need security that can protect your digital assets across the board from both internal and external threats.

The express purpose of Trustifier KSE is to provide such protection..

**protect your environment with**

## Trustifier KSE™

The only security system that NSA's Red Teams could not hack even when given full insider privileges

# Overview: The KSE Model for Protecting Sensitive Data

Whether you are a small business or the largest enterprise, Trustifier KSE was designed to help you manage protection of digital crown jewels.

- Use a deny-by-default system that denies all access to everything, including to the originators of the information.
- Only grant access to those individuals and entities who need access to the information to achieve *tasks*.
- Only allow the type of operations on that are needed to get the task done. For example, if someone only needs to **read** then just grant that. The rest such as **write**, **copy** or **delete** etc. will be denied automatically because of Rule 1.

Trustifier KSE™ delivers precisely the ability to create and enforce these types of business rules.

# Implement all of the CERT Insider Threat Protection Best-Practices

Trustifier KSE™ helps you implement all 19 of the CERT Common Sense Guide to Mitigate Insider Threats best practices.

## Consider threats from insiders and business partners in enterprise wide risk-assessments.

KSE™ provides protection from both insider threats and the transitive trust issues that arise from normal working relationships with vendor or various partners, or customers. Where data or account privileges must be granted or provided and/or shared to accomplish mutual goals or projects, KSE™ contains the tools to reduce risk and provide peace of mind. This is done by:

1. Evaluating known rules using the KSE™ Limits Module. KSE™ Limits Module is an adaptive rules-based control system that can parameterize and configure any existing safety rules to identify threats and risks to the mission. These can be Mission-Specific, Operation-Specific or Environment-Specific rules;
2. Predicting suspicious behavior of humans, machines, networks and systems using the Decider Module — a Neuro-Fuzzy Artificial Intelligence automaton that predicts risks to sensitive information using behavioral analysis of users, machines and networks;
3. Providing a relative trust framework for sharing data. KSE allows you to enforce rules on a per-user per-group basis. Each group can be assigned ownership and security officers. Each can control their levels of trust granted to partners and KSE will automatically determine levels of access for directories, files, systems grants. In mandatory-access-control mode it can enforce domain separation as well as compartmentalization to protect against and eliminate risk of possible threats from the partner's own systems.

## Clearly document and consistently enforce policies and controls

KSE™ is able to mark, designate and list the security policies for organizations, groups, or individuals in terms of actual business rules.

KSE security syntax is designed to mimic business rule language constructs. This ensures that there is one-to-one mapping between security rules and business rules.

KSE™ is a real-time kernel level policy enforcer and an authorization engine to provide all necessary controls to govern all user end behaviors post-authentication. It is a true pro-active control system that whitelists user end behaviors in real-time with allowed actions and behaviors pre-determined for the purpose of enforcement. All unauthorized behaviors that are attempted are flagged and can be brought to the attention of a security officer as required.

All system, group, user, process and data activity is audited by KSE™ and all of it can be stored for in immutable and forensically defensible logging subsystem.

## Incorporate insider threat awareness into periodic security training for all employees

While KSE™ can be transparent to users with the exception of access denied notices, it can be configured to provide user-feedback so as to to help the users understand why an operation is denied in terms of business rules. This can be used to assist them to inform them as to why they may be attempting to do doing violates policy.

Since KSE™ is insider threat protection by design. The announcement, declaration, and reminder of the existence of immutable or tamper-proof logging through KSE™ mandatory access controls and mathematically verifiable separate logging domains will act as a deterrent for unauthorized or criminal acts.

## Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior

KSE™ can log attempted unusual and unauthorized behaviors actions by all individuals in real-time and flagged for group owners or security officers as required.

KSE™ enabled provisioning and positive security model means that potential security incidents are flagged only if abuse of privileges takes place, right from the start of employment. KSE™ Decider risk engines can also flag collusion by any number of staff personnel.

KSE™ provides forensically defensible immutable auditing that may not be tampered with or altered by anti-forensics tools used by any user (or external attacker), and KSE™ can quickly and easily determine any user activity, authorized or not.

## Anticipate and manage negative issues in the work environment.

KSE™ Decider module is able to assess unusual or new negative behaviors by individuals. KSE™ multi-level integrity can prevent deliberate acts of sabotage, such as a deliberate "accidental" data dump of a database. Ease of provisioning, least privilege and separation of duties with KSE™ rule setting greatly reduces opportunities for malicious behavior. These controls are in place to ensure that behaviors that are acceptable do not cross the boundary into unauthorized and unacceptable.

## Know your assets.

Group owners benefit from KSE™ implicit labeling of all data assets based on security labels derived from relative trust relationships within and between user groups. KSE™ tools and audit trails for user group member can inform group owners as to the directories users use regularly to perform their job duties, and use this as a basis for initial rule setting.

## Implement strict password and account management polices and practices

KSE™ can enforce all rules as required including event management for processes, such as using encryption before data transmissions. All pragmatic rules for system use such as automatic logging off, hours of available access to users are easily set up and enforced as needed.

## Enforce Separation of duties and apply principle of least privilege access control

KSE™ is a deny-by-default system. Its extremely fine grained access controls and natural-language like syntax rule language facilitates and enables rule setting to help tailor least privilege, provisioning and separation of duties possible for individuals or classes of users. For example, providing IT staff with all of that they require to maintain systems and networks but preventing them access to private client, staff or management data is possible with a few rules. KSE™ is unique in the ability to deny access to individual system calls or network commands and single files. Dual key (2 person) controls for highly sensitive systems or directories are easy to set up. KSE™ is the only technology that can selectively grant or withhold partial administrative privileges, or set specific limits for their use with the Limits Module of the KSE™ risk analysis engine

## Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

Businesses fear losing control over their data in the cloud. KSE™ is able to provide the finest grained rule sets as required for both users and cloud administrators. Once again, KSE™'s immutable, tamper-proof logging has a practical use to prove due diligence for cloud providers OR customer. Whatever compliance rules the business requires, KSE™ can enforce them and show proof of the fact. What is more, with KSE™ mandatory access controls and multi-level security, cloud administrators and staff can definitely be prevented from unauthorized access to business data, and the business notified with of unauthorized access attempts. KSE™ multiple domain separation can ensure business data access is never abused in multiple tenant situations.

## Institute stringent access controls and monitoring policies on privileged users

KSE™'s extremely strong capacity in this regard is unmatched. A trusted operating system may be defined as one that establishes a data processing system in which not even the system administrator can change or misuse its digital data in an unauthorized fashion. How better to control privileged users than with KSE™'s military grade trusted security? KSE™ provides controls to govern every action of every user, including administrators. Immutable, tamper-proof auditing is one of the strongest deterrents to insider abuse as time-stamped records of all unauthorized access attempts or other behaviors are recorded and flagged.

## Institutionalize system change controls.

KSE™ is used to enforce whatever rules are necessary to oversee processes and procedures in the enterprise. For instance, enterprise-wide rules that prevent tampering with application or system code. KSE™ military grade security will inform you if a user attempts to violate policy in any way.

## Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.

KSE™ can be used as an authorization and enforcement engine for all types of logging and correlation engine data fed into it. KSE™ risk analysis engine, the KSE™ Decider™ module, is able to predict suspicious behavior of humans, machines, networks and systems. KSE™ audit trails offer the advantage of providing better actionable logging information by virtue of the fact that it is framed as a positive security model. There is less needle searching in the proverbial logging haystack when the audit traces can be readily tied directly to users and business related activities.

## Monitor and control remote access from all end points, including mobile devices.

KSE™ mandatory access controls and labeled multi-level security can be placed wherever needed, extending the secure internal environment to remote users. KSE™ enforces and logs from all systems and devices as required. It is also in the process of being ported to Android devices, as well as other mobile and embedded platforms. Wherever KSE™ is, its' forensically defensible auditing with secure time stamping is available as a deterrent, proof of due diligence performed, or for evidence for legal prosecution of abuses.

## Develop a comprehensive employee termination procedure.

In a complex network environment, one common mistake is not to remove network and system privileges of dismissed employees. What could take hours to a time strapped administrator usually takes a few minutes with KSE™.

KSE™ can support termination procedures. You can set access control rules under the dates specified in the

contracts or the security officer can simply terminate all access using a single command across all systems.

All logs pertaining to a user in question can be inspected and checked in minutes. KSE™ forensically defensible audit traces assures that they have not been tampered with, and can determine authorized abuses have been used to attempt malicious or vengeful acts. Even acts of omission, or non-performance of duties could be determined. KSE™ risk analysis engines can be used to see if other staff persons had colluded with a insider suspected of malicious acts.

## Implement secure backup and recovery processes.

KSE™ allows separation of systems from system administrators.

KSE™ value in enforcing event management is important as mandatory access controls and multi-level integrity can ensure backup processes have been done when scheduled and without unauthorized tampering. KSE™'s immutable logging can be also be useful for recovery purposes when it combines operational with security events, providing historical event records of actions that can be rolled back in the event of network actions that possibly contributed to downtime.

Its backing up rules allow out-of-band verification of all data and ensures that back up content is encrypted using specially encrypted keys. This way back-up can only be used for restores on designated systems and with proper authorization.

## Develop a formalized insider threat program.

KSE™ is the strongest technology available to manage insider threat risks. It's specifically designed as a military grade, positive security framework to combat both the insider threat and digital espionage. As opposed to trying to make several different technologies and processes interoperate with each other, KSE™ facilitates fine grained access and auditing in one unified security platform: Securing everything from single mission critical servers, workstations, edge-devices such as embedded controllers and sensors as well as smart phones and tables, across multiple domains, for all requirements.

## Establish a baseline of normal network behavior.

The KSE™ positive security framework starts with predetermined, allowed behaviors. From the start, attempts to cross the boundary and perform acts that are not supporting business goals and activities can be flagged. The KSE™ Decider Module component of the risk engine will work to predict suspicious behavior of humans, machines, networks and systems.

## Be especially vigilant regarding social media.

While for the most part, data leakage through social media may not result from intentional motives, it is still leakage which is still potentially damaging.

KSE™ offer unique controls to help prevent data leakage directly, and indirectly. For example, not allowing copying of sensitive content across unprivileged networks.

## Close the doors to unauthorized data exfiltration.

KSE™ labeled security will not release data to systems/users unauthorized to access it by security label, or if the receiving system can not uphold enforcement of the caveat access privilege specified by the directory sensitivity label.

KSE™ risk analysis engines (decider) will not allow aggregate collection of data according to limits pre-set as acceptable, such as downloading entire database onto a device or laptop.

Between the previous two points, KSE™ will not allow an authorized user to access and collect data he is authorized to, and even collect, and use in conjunction

with a storage or media device, or allow a user to send the data to himself at a private Web email address.

KSE™ provisioning can enforce read-only rules for highly sensitive data, ensure they can only be viewed in presence of security officer or monitored environment/location, or under caveat conditions for viewing, such as in/not in presence of other persons, without mobile devices present, dual key controls requiring second person authorization, disallow use of media devices when accessing, e.g. printers, USB hub, burners, etc.

## References and Bibliography


[1] Internal review: The insider threat risk, SC Magazine, February 2011, http://www.scmagazine.com/internal-review-the-insider-threat-risk/article/WC7F4bzfUb0%3d/t/

[2] RSA 2013: User habits and behavior can denote a future insider thief, 2013-02-27, http://www.scmagazine.com/rsa-2013-user-habits-and-behavior-can-denote-a-future-insider-thief/article/282185/

[3] Common Sense Guide to Mitigating Insider Threats 4th Edition, George Silowash et. al. December 2012, CMU/SEI-2012-TR-012, http://www.sei.cmu.edu/reports/12tr012.pdf


trustifier




Trustifier Inc.
113 Barksdale Business Center
Newark, DE. 19711
U.S.A.

Produced in United States of America
July 2013