Security Simplified™

Friday, August 8, 2014

Introduction

Trustifier Inc. is a cyber security company founded on the principle that everyone, everywhere has a right to digital security and privacy. We make products and provide services that ensure those rights are enforced and protected.

Trustifier technology has been used to protect some of the most sensitive financial, and military networks in the world.

Trustifier Cybersecurity

Trustifier cyber security suite is comprised of the following cyber security software and hardware systems that help protect against insider threat.

- KSE
- Fahrenheit
- HPCE
- ryu
- privatize
- CloudFort

Our cyber security solutions start with the assumption that the enemy has already gained access and is inside the network.

KSE

KSE security system makes sure that sensitive data cannot exist outside a defined boundary.

Basically, with KSE in place, even if an attacker is able to get into a system, or is already in the system, he (or she) cannot leave with sensitive data.

In addition,

- Attackers cannot see any data they are not supposed to.
- No one, including legitimate users, can piece together bits of information to gain more knowledge than their security clearance allows them to have.
- Users cannot use the data for unintended purposes, *and*
- Everyone is limited to the amount of data they can access, so no one can make mass copies of all sensitive information.

This security gets enforced on everyone including the so called *root* (system administrator) users.

KSE protects information on Windows, Linux, MAC OS X, Solaris, HPUX and other operating systems and provides new cyber security capabilities to these common off-the-shelf (COTS) systems.

KSE works on PCs, workstations, servers, embedded systems, cloud systems (*see Trustifier CloudFort*) and mobile systems (*see Trustifier ryu*).

Commercial and open source systems like Windows and Linux do not have advanced security capabilities, that are easy to use in complex networks. KSE greatly extends the security capabilities of these systems. KSE augmentations add the following security capabilities to Windows, Linux and Mac OS X:

Mandatory Access Control

- Bell—LaPadula Model
- Take-Grant Model

Mandatory Integrity Controls

- Biba Model
- Clark-Wilson Model

Roles-Based Access Control

User and group roles

Attributes-Based Access Control

Risk-Adaptive Access Control

- 2-independent stochastic engines: *Decider*™ & *Driller*™

KSE SECURITY STRENGTH

In 2009 KSE became the only system to provably defend a weak system against insider cyber attacks by elite NSA hackers.

Some Highlights.*Trustifier KSE:*

★ US Army sponsored a battle between DISA +NSA hackers (Red Team) and Trustifier KSE because US Army wanted to use KSE to protect weapons data.

★ The battle ground was Joint Integration and Testing Lab (JITC) cyber testing lab

★ Trustifier gave the hackers full insider access (system administrator access) to an unpatched and deliberately weak system that was only protected by KSE. they also had physical access to the system.

★ The Red team had 4 months to prepare and 2 weeks to attack the system.

★ The hackers completely failed to exploit the system or to get it to expose the sensitive data it was protecting.

★ As of July 2014, 5 years later, KSE is still proven un-hackable by them.

Learn more at https://trustifier.com/kse/

fahrenheit

Trustifier Fahrenheit (t°f) protects your websites and web applications from external attacks.

Fahrenheit uses a brand new break-through approach in security called Language-Theoretic design ensures that Fahrenheit understands *all* web languages completely, and can decipher web attacks without human help.

Normal web application firewalls need to be *individually* tuned and managed for *each* website or web-application that they are trying to protect.

Fahrenheit does not require configuration because it is completely self-adapting and self-configuring making it ideal for very large deployments.

Fahrenheit protects against these types of web attacks:

- Denial of Service
- SQL injection
- Code injection
- Buffer overflow attack
- Remote file inclusion attack
- Brute Force attack
- Insufficient Authentication attack
- Credential / Session Hijacking
- Content Spoofing Attack
- Cross-site Scripting Attack
- Format String attack
- LDAP injection attack
- OS commanding attack
- SSI injection
- Path traversal attack
- Cookie stealing attack
- Http Request splitting
- Mail command injection
- Null byte injection
- Predictable resource location
- Routing detour
- SOAP array abuse
- XML external entities
- XML attribute blowup
- XML entity expansion attack
- XML injection attack

Learn more at https://trustifier.com/f/

HPCE

Some information needs to be protected in all three stages:

- Data at rest (sitting on a drive)
- Data in motion (traveling over a network)
- Data in processing (being used by a user)

HPCE is the fastest commercially available encryption system, exceeding 1 terabyte per second AES256 encryption in sustained performance.

HPCE running on Trustifier CS10000Z servers is 100x faster than any other encryption engine.

The CS10000Z servers running HPCE sit between the secure data centres and untrusted or hostile public networks. They stop cyber attacks on the data centres and protect the information passing through.

HPCE is ideally suited for:

- Classified data, voice and messaging networks
- Data center mass encryption
- Encrypting e-Government systems; *and more…*

Learn about HPCE at https://trustifier.com/hpce

ryu

Trustifier ryu (*pronounced ree-oo*) is the complete mobile and smart device security solution.

ryu combines the functionality of KSE and fahrenheit with an artificial-intelligent Mobile Device Management (MDM) — all working together to provide a unified security environment

ryu device security ensures that smart devices remain secure even on insecure, rogue, or hostile networks

ryu network security ensures no insecure, rogue, or hostile mobile devices can contaminate a secure network

ryu can be used to trace hidden communication networks for law enforcement and national security agencies, using its data mining systems that perform deep pattern recognition.

ryu data mining systems (RDMS) a powerful tool for providing advanced cyber intelligence and signal intelligence support to national intelligence agencies.

Learn more at https://trustifier.com/ryu

privatize

Trustifier privatize virtual server software provides the bridge between physical servers and the cloud infrastructure.

privatize virtual servers are prebuilt turn-key servers that enable organisations to deploy secure web, email, file-sharing, databases and other informatics services protected by using using KSE, Fahrenheit and HPCE.

privatize servers are secure without any help.

privatize servers are designed to house sensitive, compartmentalised, secret and top-secret information

They are used for rapid deployment systems that can be up and running in a few minutes on Trustifier CloudFort (*see next section*).

Privatize servers have complete template support that enable users to create customised virtual servers for any application without worrying about security settings.

Find out more at https://trustifier.com/privatize

CloudFort

CloudFort is a complete system to build private clouds for large multi-organisation and multi-agency data centres.

CloudFort is capable of managing thousands of servers and peta-bytes of storage for true exponential scalability.

External and internal cyber attacks don't work against CloudFort because its infrastructure is built on top of Trustifier KSE, fahrenheit and HPCE security systems.

Sharing and collaboration on CloudFort systems is easy and straightforward and yet it does not compromise security. CloudFort secure file-sharing is used by sensitive organisations to host secure and private collaborative environments.

CloudFort is also able to provide cyber-security defence to existing data centre and cloud infrastructures.

Savings in electrical power usage is a key feature in CloudFort-based data centres — CloudFort provides sophisticated algorithms for migrating processes to ensure savings in power consumption.

Find out more at https://trustifier.com/cloudfort

About Trustifier

Trustifier Inc. is a cyber security company founded on the principle that everyone everywhere has a right to digital security and privacy. We make products and provide services that ensure those rights are enforced and protected.

Trustifier — Security Simplified™

For more information

Call us at 855.543.5434

International callers: +1 301 500-0084

Or email us at **info@trustifier.com**

or visit us on our website at **www.trustifier.com**

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

Produced in United States of AmericaJuly 2014