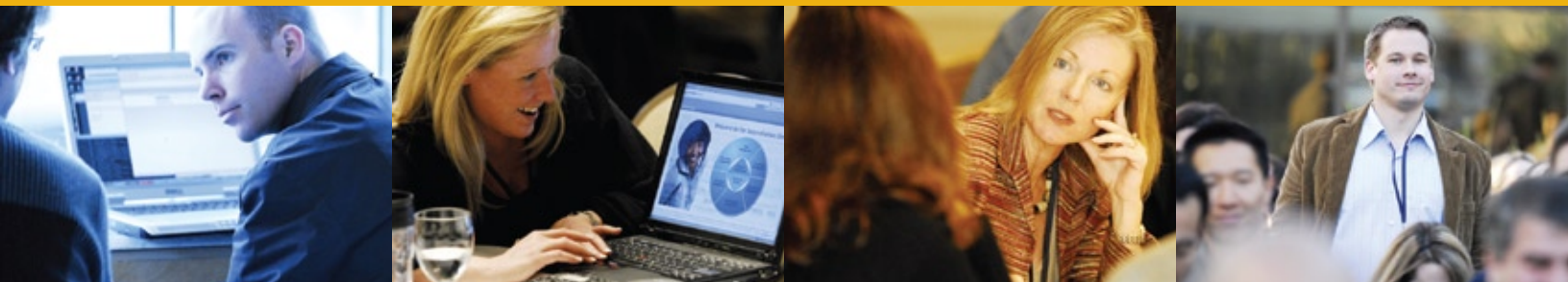


Security in a SaaS World

A SuccessFactors Overview



SuccessFactors
People Performance



Contents

- Abstract 3**

- Description 4**
 - PHYSICAL SECURITY 4
 - NETWORK INFRASTRUCTURE SECURITY 5
 - APPLICATION SECURITY 6
 - MAINTAINING EXCELLENCE OF EXECUTION 8

- What Our Customers Can Do 9**
 - IMPLEMENT SINGLE SIGN-ON 9
 - IMPLEMENT TLS FOR SECURE EMAIL 9
 - EDUCATION AND SECURITY AWARENESS 9

- Conclusion 11**

Abstract

The Software as a Service (SaaS) model is rapidly expanding to touch almost every aspect of IT.

Email, once a dedicated application built and maintained “in-house,” is now a commodity to be purchased based on user population. Enterprise tools once only in the realm of companies with deep pockets, capable of absorbing the massive upfront investments required are now available, not only to the Small and Medium businesses, but even to Sole proprietors looking to level the playing field against larger vendors. By utilizing the Internet to deliver SaaS applications, global access is immediately available. It is this same instant global access that creates a unique set of security requirements.

Anyone with an Internet connection can access the applications so SaaS providers must build a comprehensive multifaceted security program to ensure the security of their customers’ information. SaaS Security can be broken down into three basic categories: Physical, Network Infrastructure and Application.

This paper will review the standards that should be met by any SaaS provider as well as how Corporate IT teams can help create a highly secure environment. This paper will explore how the SuccessFactors solution meets the high demands of Security in a SaaS world.

Description

SaaS providers have the responsibility to provide a comprehensive multilayered approach to security their applications.

PHYSICAL SECURITY

The first layer in any security model is the physical. Data centers must deliver multi-level physical security because mission-critical Internet operations require the highest-level of security. SuccessFactors has chosen facilities that meet the highest demands. 24 x 7 x 365 onsite security, biometric hand geometry readers inside man-traps, bullet resistant walls, concrete bollards, CCTV integrated video and silent alarms are some of the features now deemed mandatory to properly secure facilities. Comprehensive and industry-leading security procedures protect equipment housed in the hosting center. Security personnel request government-issue identification from visitors, and record each visit. Security cameras monitor activity throughout the facility, including equipment areas, corridors and mechanical, shipping and receiving areas. Motion detectors and alarms are located throughout the facilities, and silent alarms automatically notify security and law enforcement personnel in the event of a security breach.

The massive investment required to build this level of security is the prime reason companies don't build their own datacenters, and why SuccessFactors has chosen to go with a world leader in co-location. On top of this they are able to benefit from the redundant power links into 2 different local utilities. This power is fed through additional batteries and UPS power sources to regulate the flow and prevent spikes, surges and brownouts. Behind this are multiple diesel generators ready to provide clean transfer of power in the event both utilities fail. In order to protect the physical investment the facilities environment is monitored 24 x 7. Heat, temperature, airflow and humidity are all kept within optimum ranges for the computer equipment housed there. All of this is protected by fire suppression systems, activated by a dual-alarm matrix of smoke, fire and heat sensors located throughout the entire facility. To avoid flooding the facility is located above sea level and has no basement and the structural systems meet or exceed requirements for lateral seismic design forces (earthquakes). These measures combine to provide a continuous and authenticated uptime of greater than 99.999%.

FROM BULLET-PROOF WALLS TO CAMERAS TO SOPHISTICATED POWER-OUTAGE PLANS, TODAY'S SAAS PROVIDERS NEED TO OFFER COMPREHENSIVE PHYSICAL SECURITY FOR APPLICATIONS.

NETWORK INFRASTRUCTURE SECURITY

Once a facility is built the next layer to be addressed is the infrastructure. All components from the point of entry on the network down to the final repository for information need to be meticulously configured, deployed, maintained and continuously tested and improved. Routers, switches, load balancers all must be configured to provide secure highly available access. SuccessFactors has chosen facilities with connections into multiple Tier 1 ISP's to provide highly available network access. All network equipment is redundant, providing seamless failover between devices. Web, application and database tiers must all be configured as secure devices while being tuned for maximum performance.

The internal networks are all configured to pass only the traffic required by the application. All internal traffic within the environment is isolated through the use of dedicated switchgear and segregated VLANs. This adds one more layer of defense within an already secure environment.

Companies not in the business of providing services tend to rely on in-house IT personnel to perform highly specialized functions. SuccessFactors has a team of specialist with years of industry experience assembled to create an environment that is secure while being optimally tuned and highly secure.

While building this level of reliability into the network is mandatory for SaaS providers so is monitoring it for both performance and security. SuccessFactors has employed the best of breed to address these requirements. Individual servers are monitored through Mercury SiteScope's remote agentless monitoring while AlertSite provides transaction-based monitoring from points around the world. This ensures the systems are monitored from the user's perspective. With respect to security monitoring SuccessFactors has chosen multiple solutions to ensure complete coverage. SuccessFactors utilizes two separate 24x7x365 security teams (IBM and SecNap) that monitor layered Network Intrusion Detection. TripWire's host based intrusion detection is also watching each individual server. Application vulnerability testing is performed regularly utilizing ScanAlert's HackerSafe and Whitehat's Sentinel. Operator logs and fault logging are used to ensure information system problems are identified. System monitoring is used to check the effectiveness of controls adopted and to verify conformity to SuccessFactors information security policies and standards.

ALL COMPONENTS FROM THE POINT OF ENTRY ON THE NETWORK TO THE FINAL REPOSITORY FOR INFORMATION MUST BE METICULOUSLY CONFIGURED, DEPLOYED, MAINTAINED AND CONTINUOUSLY TESTED.

Finally the user access controls for a secure environment require the same level of attention as the environment itself. RSA Two factor authentication to all critical components, redundant secure access points and monitoring of the usage is deployed to maintain a secure environment. In all cases, system access is based on the concept of least privilege. Users are limited to the minimum set of privileges required to perform the required function. All users have a unique identifier (user ID) for their personal use only. Capital costs and specialized personnel are key points to building this supporting infrastructure. SuccessFactors utilizes the highest quality tools to maintain their production environments. RSA SecureID, 3DES VPN access, and secure bonded on-site “Smart Hands” are some of the ways in which they protect the incredible investment made to build a secure and reliable application hosting facility. To ensure the reliability of the production environment, prior to introducing new systems into the environment, SuccessFactors insists all requirements for new systems be established, documented, and tested prior to acceptance and use of such systems.

APPLICATION SECURITY

All of the work and money spent to build a secure facility would be pointless without a secure application. As systems grow in complexity through years of configuration changes and custom code, they become less secure. SuccessFactors maintains a single code base regardless of the number of clients. The company’s unique and propriety XML schema is used to allow its customers to configure the system to suit their individual needs while never needing to write or maintain “custom code”. This methodology greatly reduces the chances of vulnerabilities being introduced through incompatibilities between custom installations and the test base. SuccessFactors is able to perform rigorous regression testing and deploy releases that are highly secure since every customer runs the same version of the code.

All interactions with the application are encrypted through a 128-bit SSL connection. The SuccessFactors application only delivers pure HTML and JavaScript to the customer, so desktops do not require any changes or special permissions. This also ensures the utmost security of the desktop environment. All administrative functions are accessed through a browser as well so there is no reliance on plug-ins or downloads. Data files can be loaded manually through the user interface or through SFTP. Files sent via SFTP must also be PGP-encrypted to ensure authenticity. Return communications from their environment are accomplished via secure messaging. All email is scanned for viruses prior to leaving the environment and TLS is employed by the outbound mail service to not only ensure privacy during transport by encrypting the email but to protect against spoofed or forged emails by authenticating the end points.

SuccessFactors also sends all email as plain text. In this way there is no chance for Phishers or Pharmers to send fake emails with secret links hidden in them, in an attempt to gather information from the users.

The overall goal is to reduce the complexity of the environment and the number of touch points in order to reduce the points of vulnerability, thus providing a higher level of security.

The SuccessFactors application itself implements an advanced security methodology based on dynamic data and encoded session identifiers. The application always requires the user to login, either interactively or through Single Sign-on (SSO). This is a requirement that cannot be disabled. Interactive logins require a username and passwords to be entered by the user and maybe configured to include mixed case, alphanumeric and minimum length. Passwords can, and should be, encrypted in the user database utilizing a one-way SHA-1 hash encryption. This is the encryption algorithm designed by the National Security Agency and published by the National Institute of Standards and Technology as a Federal Information Processing Standard (FIPS 180-1). The user's session is automatically logged out after 30 minutes of inactivity and accounts can be locked out after a predetermined number of failed logins.

If a customer is looking to further enhance the security of the application it can be integrated with the customer's Single Sign-on infrastructure. The trust mechanism between the client and SuccessFactors passes identity information through an encrypted token to SuccessFactors such that it can be interpreted, and trusted. This trust mechanism is based on pre-shared keys for encryption, system time stamps as well as usernames and passwords. The window for login is managed through system time synchronization with atomic clocks maintained by the military and the primary transport for this trust mechanism is HTTPS. SSO requires the user to be first authenticated via the customer's intranet and then be redirected to the SuccessFactors website. SuccessFactors then restricts access to the customer's instance of the application to the predefined IP address(es) of their proxy or gateway.

SuccessFactors also offers at rest disk level encryption. The Decru DataFort Encryption Appliance integrates with our SAN storage to provide a reliable safe, secure data storage environment. SuccessFactors uses AES 256bit encryption to secure data at the block level of our storage systems. Decru's key management has passed the FIPS 140-2 level 3 certification testing. Finally all data stored on backup tapes is encrypted using 128-bit encryption before it leaves the machine. These tapes are then transported and stored safely offsite with a bonded company.

***THE GOAL: REDUCE COMPLEXITY AND
THE NUMBER OF TOUCH POINTS IN
ORDER TO REDUCE VULNERABILITY
AND INCREASE SECURITY.***

MAINTAINING EXCELLENCE OF EXECUTION

Now that it's built what do you do? All the security in the world is useless without a properly defined and enforced policy. Procedures to control what and how changes occur within the environment, user education and security awareness are as, if not more, important than how many firewalls are in front of the data.

Strict procedures that provide checkpoints but do not impede the process are required to change anything in a production environment. Whether adding hardware, removing software or changes to existing configurations, there must be an auditable process that is followed every time. SuccessFactors has implemented a multi-tiered approach to ensure a balance between process control and ease of use. By ensuring the process is easy to follow there is no reason to find a way around it in order to get something changed. All changes to the environment are logged, approved and verified in a centralized on-line application. This is one of the reasons why SuccessFactors has been able to issue product releases into production every month for the last 70 months without fail.

User education on how and why to follow procedures is a critical component often overlooked by new companies, or those looking to move quickly. This is, more often than not, the reason of some of the most significant security breaches in both the SaaS arena and traditional Corporate IT. Without educating the people that support and control both the production and the back-office environments as to why the processes and procedures are in place there is no understanding of the potential outcomes if they are not followed. All employees at SuccessFactors are required to read and acknowledge they will follow the company's Security Policy. In fact we have used our own application to implement a secure delivery of the acknowledgement form and to capture the electronic signature from employees dramatically reducing the amount of time and effort required to complete the exercise.

***ALL THE SECURITY IN THE WORLD
IS USELESS WITHOUT A PROPERLY
DEFINED AND ENFORCED POLICY.***

What Our Customers Can Do

IMPLEMENT SINGLE SIGN-ON

The implementation of SSO between a customer and a SaaS provider only serves to increase the level of security of interaction with the application. By implementing SSO the customer is assured that the application is enforcing the exact same security requirements already established. There is no need to seek Security exceptions. End users are never given their application level credentials and the “interactive” login feature is disabled within the SuccessFactors application. This means that a user cannot login even if they knew the user names and passwords that were assigned to their account. When an employee leaves the company and their local account is disabled or removed they are automatically locked out of the SuccessFactors application as well. No more emergency calls to the application administrator to disable a users account. The application is also configured to only respond to the customer’s portal or gateway. Logins can only come from the customers pre-authorized networks.

IMPLEMENT TLS FOR SECURE EMAIL

SuccessFactors utilizes opportunistic TLS. This means if a customer’s mail server is configured with an SSL certificate and able to negotiate a TLS secure connection, SuccessFactors will use that secure connection. All companies should be encouraged to take advantage of this secure form of messaging communications.

EDUCATION AND SECURITY AWARENESS

In a world of ever increasing computing power and a greater reliance on information passing over the World Wide Web, one of the simplest and most effective ways to secure any application is user training. Periodic reviews of the company’s policies along with acknowledgements that the employees have read and understand them go a long way to keeping information security in front of everyone’s mind. Ongoing training to keep employees informed of the ever changing on lines scams such as “Phishing” and “Pharming” and occasionally randomly testing employees in the same way applications are tested for vulnerabilities.

Some of the biggest data leaks in recent months have been the result of social engineering or simple carelessness. Employees who unwittingly give access to confidential data, laptops stolen, or worse, left behind on airplanes or in cabs without encryption have resulted in some of the largest data leaks of all times.

In January of 2006 a laptop was stolen from a car containing information on 215,000 Ameriprise customers and advisors. In May of that same year an employee of the veteran's administration violated a simple security policy and copied information onto their laptop to work on at home. The employee's home was burglarized and the laptop stolen. The information that was lost contained personal information for 26.5 million veterans.

More recently an employee at a CRM SaaS provider fell victim to a phishing scam that allow a customer contact list to be copied. The criminals then used that information to target their clients with fake emails which eventually led to them gaining illegal access to hundreds of thousands of records.

CUSTOMER'S INTERNAL PROCEDURES AND BEHAVIOR ALSO HAVE A TREMENDOUS IMPACT ON APPLICATION SECURITY.

Conclusion

Security continues to be top of mind for organizations of all industries, as the malicious programs spread, identity theft increases and online system exploitation has become its own illegal industry. Governments are trying to legislate measures to protect citizens and businesses, customers are demanding higher levels of security to protect themselves, and many businesses are struggling to implement a sound security infrastructure that protects them from today's known threats and those that may emerge tomorrow. SuccessFactors has taken a comprehensive approach to security — at the physical, network and application layers — literally baking it into every aspect of its business. The company works with industry-leading, best-in-class technologies to ensure its customers' data is safe. Working together to secure communications and interactions, SuccessFactors provides a secure and highly accessible environment that many corporate “behind the firewall” implementations could not conceive or achieve. Due to the very nature of our business, SuccessFactors and many other SaaS providers, are leading the industry in offering applications that are affordable, configurable and secure.

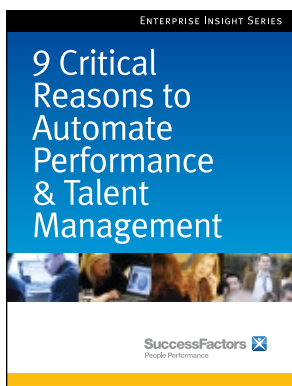
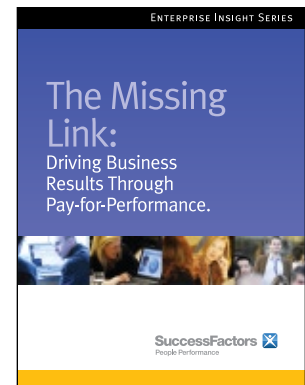
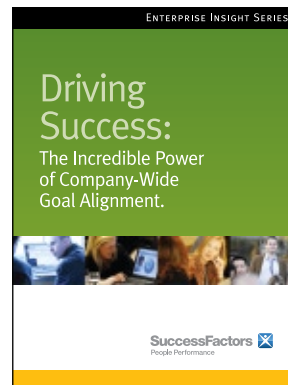
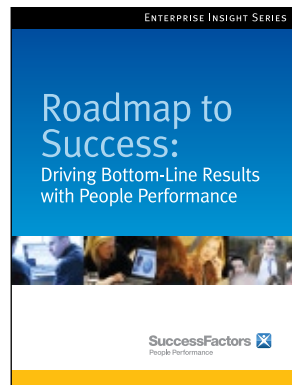
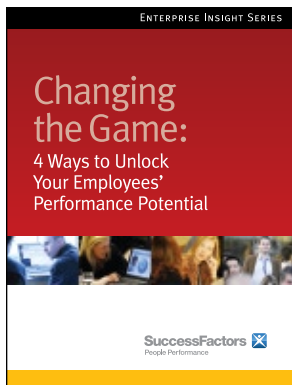
About SuccessFactors

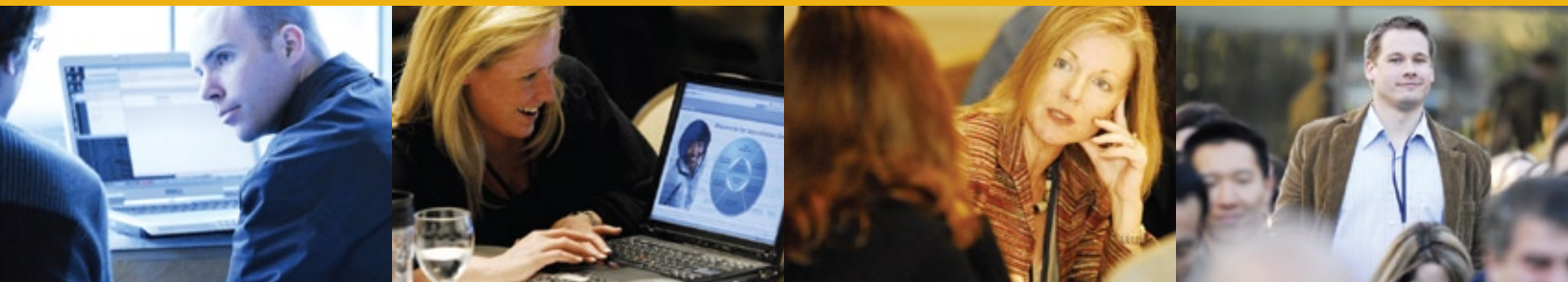
SuccessFactors delivers easy-to-use technology that helps businesses of all sizes align, develop and motivate employees. With a suite that includes solutions for goal alignment, performance management, compensation, succession planning, learning, recruiting, and workforce analytics, SuccessFactors offers the most innovative HR technology available today. Visit www.successfactors.com to learn more.

The Enterprise Insight Series

This ongoing set of guides is designed to provide HR professionals in large companies with insights and solutions that can be applied in everyday efforts. Contributing authors include HR experts, as well as leading companies that have improved business results by using the latest HR technologies.

Visit www.successfactors.com to download more of the Enterprise Insight Series:





SuccessFactors
People Performance

