



UNITED SECURITY PROVIDERS

PROTECTING WHAT MATTERS.

USP SECURE ENTRY SERVER™



PREPARED FOR ALL THREATS.

Web applications allow innovative collaboration with customers, partners or within teams without the need for changes in media. Information can be accessed from anywhere by those who need it, including information critical to the company. However, the fact that Web applications are often produced under great time and cost pressure means that the data transferred is not always sufficiently protected. That's why the USP Secure Entry Server™ (SES) from United Security Providers guards not only the overall system, but also individual applications and even their content.

The quantity and complexity of Internet-based attacks is on the increase. A few years ago, these attacks were mainly the work of technologically gifted youngsters who saw it as a challenge. Today, however, the attackers have a financial motive and have the latest technology in their arsenal. Web applications are a particular target of frequent attacks and malware. Even when these applications are implemented by the book, underlying components provide vulnerable areas for attacks.

A further challenge is posed by the fact that user IDs and passwords are no longer sufficient for accessing Web applications, as they can be stolen or cracked too easily. For this reason, a changeover is taking place to tough authentication methods. In an increasing number of cases, authentication is a regulatory requirement. The SES is equipped with a wide range of popular procedures in order to satisfy these demands.



UNITED SECURITY PROVIDERS

PROTECTING WHAT MATTERS.

THE USP SECURE ENTRY SERVER™ STANDS THE TEST OF TIME.

Security you can bank on

You can put your trust in maximum security and exceptional features as used by leading banks. The USP Secure Entry Server™ protects each individual Web application and all related information and data. The server, which has been in operation since 1997, has not been breached to this day.

Highly complex, yet easy to use

The SES is user-friendly and provides transparent operation, as it is simply installed as the single access point to your Web applications and successfully deals with all requirements, even in a complex, multi-application environment.

Prepared for the future

You receive a protected investment that can be scaled as you please, no matter how many new users and applications are added or how much the system load increases. What's more, the server already supports numerous, increasingly popular authentication methods including one-time password tokens, matrix cards, biometrics, SMS and combinations of these methods.

Increased availability

The server architecture has been designed in such a way that it boosts the availability and performance of your Web applications. The architecture speeds up applications for users, and makes expensive load-balancing infrastructures a thing of the past.



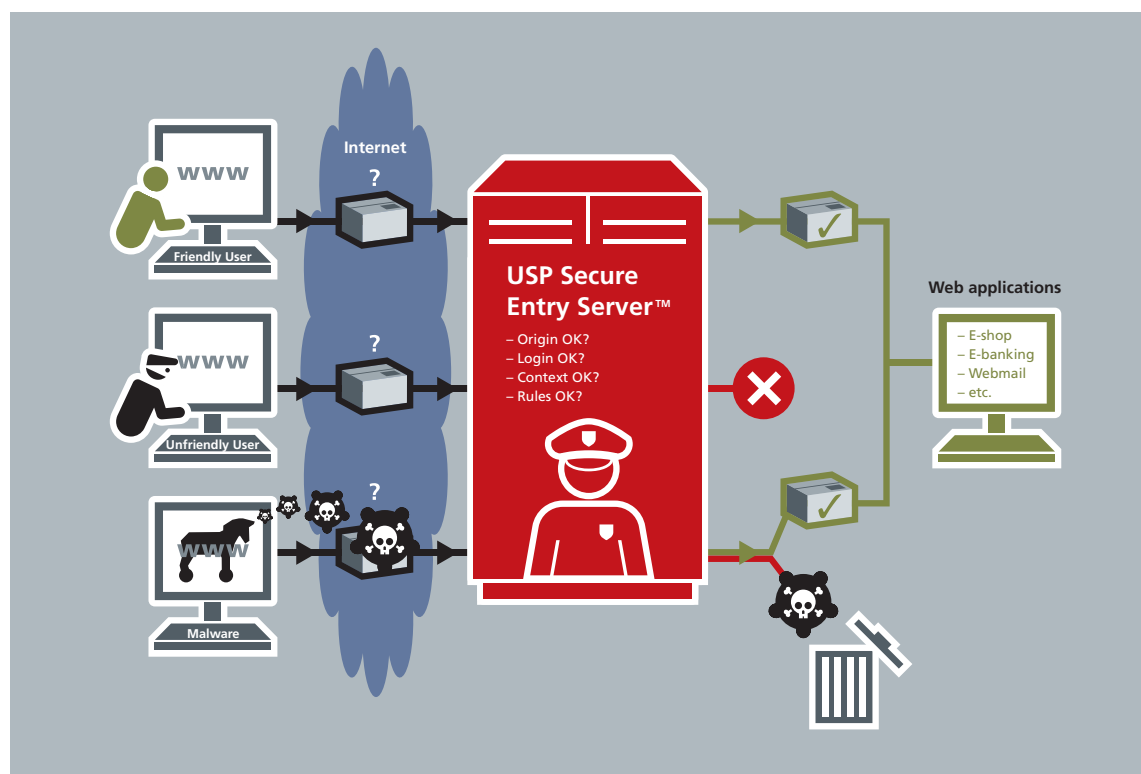
THE SES ALSO PROTECTS INDIVIDUAL CONTENT.

One access point

The tough USP Secure Entry Server™ provides one central access point to all Web applications. It securely identifies all users, and grants selective access to applications. Identification is performed through a special authentication method that can be physically separated. User-friendliness is also increased thanks to a Web Single Sign-On system incorporated free of charge, which means that users only need to log on once. Application developers are also freed of the task of identifying users and controlling access, which is one of the major weak spots and points of attack.

Seriously secure

The SES prevents direct connections between the Internet and your corporate network. It also internally checks the content of each query within the entire context. That's why the server can recognise and successfully fend off sophisticated attacks at application level, unlike conventional firewall and intrusion prevention systems (IPSs). And it protects not only the applications, but also the content being transmitted. This means that e-banking and online access to your ERP system remains secure, even if the end device being used is already infected with a Trojan horse.



The SES examines the content of data packets.
It releases to the application only those that are unsuspecting.





Traceable business processes

As the number of applications in use has soared in recent years, many companies are no longer able to consistently trace all transactions. These days, however, traceability is increasingly a legal requirement for core business applications. The central access point provided by the server enables you to chronologically search for and log all activities.

Managed service

The USP Secure Entry Server™ is available either as a software package at an affordable licence price or as a remote managed service. The software package can be easily integrated into your existing environment, processes and system administration tools. If you also opt for our system maintenance and operation service, the application will be monitored by security experts around the clock. This provides you with a clearly defined service at low, fixed calculable costs.

UNITED SECURITY PROVIDERS – PROTECTING WHAT MATTERS.

United Security Providers is a group of leading specialists in information security who have joined forces to close the gaps in network and application security. As the Swiss market leader in this sector with more than 80 highly qualified specialists, we now also handle this task on an increasingly international level.

Our efforts are centred on providing maximum security for your business processes in terms of both confidentiality and availability. Solutions from United Security Providers effectively protect your existing IT infrastructure, whilst also providing opportunities to simplify it. This gives you the freedom to align your processes with changing client needs and market requirements where necessary, thus strengthening your competitive position.

Since 1994, a growing number of clients have been placing their trust in United Security Providers. Our clients include renowned Swiss financial service providers, administrative organisations, multinational corporations and transport and logistics companies, all of whom demand first-class products and services. And that's just what we offer – 24 hours a day, seven days a week – by operating mission-critical network and security infrastructures at more than 200 locations across the globe.

Our carefully selected business partners help you to choose and integrate the perfect solution for you, meaning that United Security Providers is always at hand – wherever you are in the world.

USP SECURE ENTRY SERVER™

TECHNICAL INFORMATION.

Security

- Filters the HTML data stream and blocks known attack scenarios (injection attacks, cross site scripting, buffer overflow, etc.)
- Automatic validation of form-based user inputs
- Encryption of URL and/or parameters
- Protection against session/cookie hijacking, etc.
- Automated transaction signature
- Transparent encryption of application cookies
- Any required number of physically separate network zones can be supported
- Protects Web services (SOAP/XML filter)

Availability/performance

- Failover cluster
- Weighted load balancing of enquiries to the back-end systems
- Protection against DoS attacks
- Transparent data compression for faster website loading
- Faster SSL connections
- Multi-threaded architecture assures the best possible performance on modern processors

Operational advantages

- Central management of configuration data files
- Flexible monitoring and reporting
- Administration portal for direct access to running system
- Straightforward maintenance, e.g. by transfer of existing sessions to other systems
- Existing open source know-how can still be used
- Assists DMZ virtualisation and consolidation
- Attachment of external filter systems via ICAP interface (e.g. antivirus scanners)

End user benefits

- Single Sign-On via all Web applications
- Different authentication methods can be used simultaneously
- Simple integration of additional applications
- Protection against data loss for time-consuming forms by means of a special intermediate memory
- Entry-URL for all Web applications

Compliance

- PCI DSS (Payment Card Industry Data Security Standard)
- ONR 17700 (technical security requirements for Web applications)
- Audit logs

Supported standards

- SSL v3 / TLS (RFC 4346)
- ICAP (RFC 3507)
- SAML 2.0
- HTTP 1.0/1.1 (incl. "keep-alive" connection to back-end)
- SOAP 1.1/1.2
- WSDL 1.1
- Web Application Firewall Evaluation Criteria 1.0
- Apache 2.2

Authentication methods

- Certificate-based (X.509 V3)
- RSA SecurID
- Aladdin eTokens
- NTLM (Single Sign-On within Microsoft domains)
- GSM SMS (Simple Messaging Service) OTP
- Username/password on LDAP directories (incl. Microsoft Active Directory, Novell eDirectory, Siemens DirX, Sun Directory Server, etc.)

Authentication systems

- RADIUS (RFC 2865), RSA ACE Server, Aladdin TMS, Microsoft Domain Controller

Operating systems

- Sun Solaris 8/10 (Sparc)
- HP-UX 11iv23
- Linux (RHEL 5, SLES 10)
- TCSEC B1 and Common Criteria EAL4+ certified systems (Argus PitBull® Foundation)

United Security Providers
Bahnhofstrasse 4
P.O. Box
3073 Gümligen
Switzerland

Phone +41 31 959 02 02
Fax +41 31 959 02 59
www.united-security-providers.ch

United Security Providers
Förrlibuckstrasse 220
P.O. Box
8031 Zurich
Switzerland

Phone +41 44 496 61 11
Fax +41 44 496 61 99
www.united-security-providers.ch



UNITED SECURITY PROVIDERS
PROTECTING WHAT MATTERS.