Tumbleweed®

WHITEPAPER

SECURE THE LINES OF COMMUNICATION: ACHIEVE PCI COMPLIANCE FOR EMAIL AND FILE TRANSFERS

Introduction

When customers give credit card information at a point of sale, over the Internet, on the phone, or through the mail, they do so based on the expectation that their account information is safe. When account information is compromised – whether intentionally or accidentally – the cost to consumers and merchants is significant, not only in dollars but also in negative impact to the merchant's reputation and to the future business relationship.

But the statistics show that credit card information is not safe. Almost 675,000 incidents of identity theft were reported to the Federal Trade Commission in 2006 alone, and credit card fraud is the leading form of identity theft. It's not just consumers who suffer when credit card data is compromised: The average security breach can cost a company between $90 and $305 per lost record, according to Forrester Research.

Security breaches exact a price beyond quantifiable losses. Data compromise is an increasingly visible problem, largely because of federal and state disclosure laws that require businesses to publicly disclose data loss. Failure to protect customer account information can cause customers and partners to lose faith in a company, leading to a tarnished reputation and loss of future revenue. After all, would you want to do business with a merchant that has experienced a significant data compromise? Likely not.

The State of PCI Compliance

The payment card industry created the Payment Card Industry Data Security Standard (PCI DSS) to enhance payment account data security. The Standard was created in response to industry and consumer concerns about the potential for large-scale theft of card data from merchant databases as well as actual security incidents. The PCI Security Standards Council, which maintains the Standard, was founded by American express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International.

The PCI DSS standard is based on a set of security and privacy best practices that should be familiar to any enterprise information security and IT operations department personnel. The Standard applies these best practices specifically to the protection and handling of sensitive card verification and cardholder data, with the ultimate goal of preventing both accidental and fraudulent misuse of payment cards.

PCI has six main directives, each with its own requirements:

- Build and maintain a secure network
  - Install and maintain a firewall configuration to protect cardholder data
  - Do not use vendor-supplied defaults for system passwords and other security parameters

- Protect cardholder data
  - Protect stored cardholder data
  - Encrypt transmission of cardholder data across open, public networks
- Maintain a vulnerability management program
  - Use and regularly update antivirus software
  - Develop and maintain secure systems and applications
- Implement strong access control measures
  - Restrict access to cardholder data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data
- Regularly monitor and test networks
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes
- Maintain an information security policy
  - Maintain a policy that addresses information security

The PCI Security Standards Council set a staggered rollout for compliance based on perceived merchant risk levels, a measure that takes into account transaction volume and security history. Here's how it breaks down:

- Online merchants, large-volume merchants (major national retailers who process more than 6 million transactions per year) or merchants that have been previously hacked are considered high risk (Level 1) and were required to be compliant in September 2006. New Level 1 merchants have one year to become compliant.
- Level 2 merchants (retailers who process 1 million to 6 million transactions per year) were required to be compliant in March 2007. New Level 2 merchants must be compliant by September 2007.
- Level 3 merchants (20,000 to 1 million transactions per year) must have demonstrated compliance by June 2007.

PCI compliance is encouraged through a combination of incentives and fines. Each card association sets its own schedule, but typically the incentive is the ability to retain preferential processing fees and avoid fines assessed for data breach incidents or non-compliance. For instance, Visa assesses fines of up to $50,000 for the first violation in a 12-month period, and $100,000 for subsequent violations in that same period. MasterCard levies fines of up to $25,000 against non-compliant major national retailers and fines of up to $5,000 on medium and large retailers. American Express may fine merchants up to $15,000 per day of sensitive data exposure. In 2006, Visa levied a total of $4.6 million in fines, up from $3.4 million in 2005.

The payment card industry is becoming increasingly adamant about compliance. In late 2006 as part of an overall program to raise compliance, Visa began offering acquirer banks financial incentives if their members were fully compliant by August 2007. Starting in September 2007, Visa will begin to fine acquirer banks $5,000 per month for each non-compliant merchant. The fines increase to $25,000 per month for each non-compliant merchant after December 2007.

Failure to comply with PCI has consequences beyond fines. Point-of-sale equipment may be withdrawn and the card association membership may be revoked, leading to reduced sales. If data is compromised, merchants face lost revenue and legal costs. Yet the soft costs may ultimately outweigh hard dollar losses: A high profile data compromise can result in significant negative publicity and a loss of customer confidence. Fallout from a security breach can make cardholder association penalties look like a slap on the wrist.

Despite the carrots and sticks and despite the enormous potential damage to a company from publicized security breaches, the reality is that most merchants are lagging in compliance. As of July 2007, Visa announced that 40 percent of Level 1 merchants validated compliance with PCI and another 50 percent had submitted their initial validation and were working to address the remaining security deficiencies. The remaining 10 percent were working on their initial investment. Among Level 2 merchants, 33 percent validated compliance while another 42 percent were in process. The remaining 25 percent are beginning the process. Among Level 3 merchants, 52 percent are compliant and another 22 percent are in process. The remaining 24 percent have not yet validated compliance. Clearly, a secure and cost-effective solution to PCI-compliance headaches couldn't be more necessary.

Checklist Compliance or Real Risk Reduction?

Despite the pressure to – and importance of – complying with payment card data security mandates, compliance remains challenging for many organizations. Operating in a highly competitive, low-margin industry, retailers have typically lagged in IT spending. Retailers earmarked 1.5% of their sales revenue for their IT budget, according to InformationWeek's 2006 research of the 500 leading users of technology. When looking across industries the average company allocated 3.1% of its sales revenue to IT.

With PCI mandates looming, retailers have had to quickly adjust to implement security technologies and achieve compliance. Compliance is a journey, and the first step is to evaluate the bare minimum necessary to pass an audit. Many companies hit this low bar in order to pass the audit, but don't fundamentally change their practices. They make an unspoken decision to simply "take their chances," paying fines if they are caught, and hoping they don't suffer a data breach worthy of the evening news.

PCI compliance also lags because some companies are simply confused about how to adequately comply. PCI is a set of best practices that significantly impacts both security infrastructure *and* IT processes. There is no single PCI solution and no true litmus test to pre-certify PCI compliance prior to an audit. Adding to the confusion is the reality that PCI is just one of many industry and government regulations that companies must field, and they may find it difficult to translate the overlapping requirements of state, federal, industry, and international regulations to a single plan of action.

But as companies realize the full extent of the dangers of data loss from both internal and external threats, they become more serious about compliance, systematically addressing holes in their security policies and technologies, and bringing their processes in line with industry best practices. And finally, companies begin to approach compliance from the perspective of risk reduction and competitive differentiation.

Industry-leading companies realize that PCI compliance represents a real opportunity to reduce risk. The bottom line is that protecting customer data from the outset is far less costly than dealing with a highly publicized security breach. For instance, Choice Point paid out $43 million in direct charges after its high-profile data breach. Retailer T.J. Maxx reported $20 million in costs associated with its breach in data security, not to mention the numerous class-action lawsuits still in the offing.

Smart spending on compliance initiatives can mitigate these risks and ultimately create confidence among customers and suppliers that can lead to new revenues. The companies that are the most successful in meeting compliance requirements spend $1 on IT security for every $29,330, or about 10% of the IT budget, according to the IT Policy Compliance Group. Gartner Research estimates the cost of PCI compliance at $16 per customer.

Securing the Lines of Communication

A key part of achieving real risk reduction with PCI means securing the relevant lines of communication across internal employees, partners and customers. A credit or debit card transaction may involve anywhere from a few to a dozen companies responsible for card validation, payment processing, merchant statements, and other intermediate payment card services.

Tumbleweed provides solutions that identify and protect sensitive cardholder data in transit, helping companies avoid data breaches and demonstrate compliance with PCI DSS requirements. Tumbleweed solutions incorporate the proven security technologies that PCI compliance demands – comprehensive email security, secure file transfer, content filtering, strong encryption, access controls, auditing and reporting capabilities, and more.

Tumbleweed Protects PCI Data Sent via Email

Sending payment card numbers in email over unsecured lines of communication is extremely risky, but it happens all the time. Sometimes this kind of risky communication happens in the course of doing business: A customer support rep at a credit card company is researching a chargeback, and emails the retailer with the customer name, credit card number, item purchased, and purchase amount. Or a clerk in a retailer's accounts receivables department creates a password-protected zip file listing the card numbers of late payers, then emails it to her manager.

When such emails are sent "in the clear" – that is, un-encrypted – they violate corporate security policies and PCI requirements, and put the business at risk. Emails sent in the clear can be compromised by malware on either end, captured in transit by malicious attackers, or simply be forwarded to an unauthorized person. And passwords protecting data attached to these emails can be cracked with relative ease.

There are other threat scenarios to consider. An employee with the best of intentions may accidentally disclose sensitive information by addressing an email to the wrong person. Or an employee may knowingly email a file of credit card numbers to a personal email account with the intention of selling them in the underground. It's a fact that many security breaches can be traced to intentional acts by insiders. Criminals external to a company may penetrate the company's IT infrastructure and steal emails containing payment card information. Systems can be compromised by worms, viruses and other malware that infiltrate via email and expose systems to intrusion. Vulnerabilities like missing software patches can be exploited by attackers, allowing them to access systems and unprotected data.

A best practice followed by one prominent national grocery chain is to protect cardholder information in email by filtering all emails for primary account numbers and card stripe data. All emails containing primary account numbers are encrypted before they are sent, and any email that contains card stripe data is automatically blocked, and immediate warnings are sent to the employee and to the human resources department at company headquarters. This grocery chain uses Tumbleweed MailGate to secure their lines of communication, and to keep them PCI-compliant.

Tumbleweed's MailGate suite of email security products enables companies to protect sensitive data against unintended or unprotected transmission through email. MailGate filters content and identifies sensitive information in email and attachments – such as primary account numbers and magnetic stripe data – and allows a company to specify and enforce protection policies by blocking, quarantining, or encrypting messages in accordance with compliance mandates. Comprehensive inbound and outbound antivirus and antispam protection eliminates viruses, spyware, and other malicious email attacks whose aim could be to hijack sensitive data.

MailGate provides flexible, granular controls to enforce security policies and to notify managers of policy violations, which is critical to changing employee behavior by raising awareness of potential compliance violations or data breaches. Compliance and security teams will appreciate MailGate's easy-to-use templates for identifying primary account numbers, magnetic stripe data, and other sensitive cardholder information in email messages. MailGate is easy to deploy and manage, and supports the compliance audit process with robust reporting and monitoring tools.

Deployed together, Tumbleweed email security products map to six of the 12 PCI requirements.

- **Requirement 2: Build and Maintain a Secure Network**
  PCI Challenge: Do not use vendor-supplied defaults for system passwords and other security parameters.

  Tumbleweed Solution: Administrators can require that all default passwords for MailGate and Secure Messenger are changed upon initial deployment and at regular intervals.

- **Requirement 3: Protect Cardholder Data**
  PCI Challenge: Protect stored data.

  Tumbleweed Solution: MailGate enables a company to protect stored data and prevent accidental data leaks. Through a simple checkbox interface, MailGate can be configured to identify primary account numbers and other cardholder data in email messages, and to take a specific action regarding such emails, including quarantine, return, drop, annotate,

add disclaimers, modify headers, or tag messages for future analysis. Administrators can build custom roles and specify rules around senders, recipients, content, attachments, message headers, and file size.

MailGate delivers automatic gateway-to-gateway strong encryption for any remote domain through policy-based TLS encryption, and provides a wide range of encryption methods and secure email delivery options, including remote certificate error checking and validation, S/MIME and PGP protocols, and secure Web-based delivery.

MailGate's Secure Messenger protects organizations at the perimeter, guaranteeing that all users comply with corporate security and PCI policies. Secure Messenger works with MailGate Email Firewall to inspect outbound mail at the network gateway and automatically redirect messages containing sensitive content to a secure, encrypted channel. It then applies the most appropriate delivery method for each recipient, either offline push with Secure Envelope, or online pull with Secure Webmail.

≫ Requirement 4: Protect Cardholder Data

PCI Challenge: Encrypt transmission of cardholder data and sensitive information across open, public networks.

Tumbleweed Solution: With Secure Messenger, merchants can choose between Secure Envelope (offline push) or Secure Webmail (online pull) delivery methods to ensure ease of use and PCI compliance. Secure Envelope delivers an encrypted message directly to a recipient's inbox without requiring any special email client software or digital certificates to decrypt. Secure Webmail is based on Tumbleweed's patented staging server technology, which notifies a recipient of messages awaiting retrieval with an authenticated, encrypted Web link to a secure server. Secure Messenger supports S/MIME encryption and digital signature technology.

≫ Requirement 5: Maintain a Vulnerability Management Program

PCI Challenge: Use and regularly update antivirus software.

Tumbleweed Solution: MailGate protects the Internet gateway against viruses, worms, Trojans, spyware, and other malware, eliminating threats before they reach endpoints. MailGate inspects incoming and outgoing messages to detect and disinfect potentially damaging messages before they enter or leave your network. MailGate's zero-hour virus outbreak protection quarantines suspicious messages and attachments in the earliest hours of an outbreak, before malware can spread widely and compromise data integrity or system availability.

MailGate prevents accidental data leaks through deep content filtering capabilities, which scan messages and more than 300 attachment types. Flexible policy controls allow a company to block, quarantine, modify, reroute, or encrypt messages to prevent the loss of cardholder data or other sensitive information. Intelligent Edge Defense controls SMTP connections and defends against directory harvest and denial-of-service attacks, further protecting your business from cyber-criminals. MailGate is an appliance solution that can be installed in minutes, to begin securing your organization's email infrastructure immediately.

≫ **Requirement 6: Maintain a Vulnerability Management Program**
PCI Challenge: Develop and maintain secure systems and applications.

Tumbleweed Solution: Tumbleweed develops all of its applications – including MailGate and Secure Messenger – based on secure coding guidelines under the close supervision of Tumbleweed's Chief Architect. Tumbleweed developers use automated tools such as Fortify source code analyzers to identify unsafe practices. In addition to stringent internal coding practices and reviews, Tumbleweed periodically submits its Web interfaces for third-party vulnerability assessments.

≫ **Requirement 10: Regularly Monitor and Test Networks**
PCI Challenge: Track and monitor all access to network resources and cardholder data.

Tumbleweed Solution: MailGate logs all access to systems, so businesses can track and monitor access to MailGate.

Tumbleweed Protects PCI Data Sent via File Transfers

After a day's sales, a retailer settles up its transactions by sending primary account numbers, card validation numbers, and other sensitive data to the payment processor. Once the settlement process is initiated, the funds are transferred from the card issuing bank into the merchant's checking account. This transfer of sensitive data must be done with care, or the company runs the risk of losing data, violating corporate security policies, and failing to meet PCI requirements. Bulk transfers of credit card data may require greater security in several instances.

The settlement process requires moving massive amounts of sensitive data, which can be compromised either accidentally or intentionally. For many retailers, these processes still involve using either expensive but secure leased lines (legacy technology), or a homegrown FTP solution that lacks sufficient security or management controls. Criminals can infiltrate systems at the retailers, payment processor or other points along the way. Even if data-in-transit is sufficiently secured, it may be parked on an an FTP server that is accessible to multiple merchant customers. By exploiting inherent vulnerabilities in the FTP site or taking advantage of an unprotected Internet connection, attackers can break into an unprotected FTP server and hijack sensitive data.

Tumbleweed SecureTransport avoids the potential loss of large volumes of cardholder information by establishing a secure file-transfer process that meets PCI requirements from the get-go. SecureTransport ensures end-to-end protection for file transfers with strong encryption and access controls, and a proven two-tiered security architecture that prevents storage of sensitive data in the DMZ.

Using SecureTransport, companies can protect the entire file transfer process so that bulk or ad hoc cardholder data is transmitted securely and in compliance with PCI, even from legacy or third-party applications. Highlights for ensuring PCI compliance include:

- Role-based access controls that limit access to sensitive information and generate a log of access history

- Flexible authentication controls and data routing facilities that eliminate the need for shared accounts and strengthen authentication
- Secure web-based administration support built to meet or exceed web application best practices for managed file transfer

SecureTransport demonstrates comprehensive file transfer protection mapping to seven of the 12 PCI requirements.

≫ **Requirement 1: Build and Maintain a Secure Network**
PCI Challenge: Install and maintain a firewall configuration to protect data.

Tumbleweed Solution: Using SecureTransport's multi-tier security architecture and the SecureTransport Edge™ multi-protocol file transfer gateway, retailers can stream file-transfer data to prevent storage of sensitive information in the DMZ. Additionally, SecureTransport server supports network address translation (NAT) for secure FTP data connection negotiations, preventing internal IP addresses from being revealed on the public Internet.

≫ **Requirement 2: Build and Maintain a Secure Network**
PCI Challenge: Do not use vendor-supplied defaults for system passwords and other security parameters.

Tumbleweed Solution: SecureTransport separates client protocol handling from the storage of data on the SecureTransport server, which meets the PCI requirement to implement only one primary function per server.

SecureTransport handles all of its own file protocols and does not rely on the underlying operating system for support, which meets the PCI requirement to disable all unnecessary and insecure services and protocols.

Administrators can define administrative and delegated roles to prevent misuse of access. All non-console administrative access is encrypted, and the SecureTransport administration service runs as an HTTPS process. Administrators can choose the automatic start option during installation, so that the administration service will start automatically each time the server is started or rebooted. Access to the administrator console is not required for help desk support. Administrators can use SSH for secure access to the UNIX console, or Windows Desktop Remote for the Microsoft Windows console.

≫ **Requirement 3: Protect Cardholder Data**
PCI Challenge: Protect stored cardholder data.

Tumbleweed Solution: SecureTransport offers powerful configuration controls that keep cardholder data storage to a minimum. SecureTransport can perform event-driven data removal once files are delivered, so that file deletion is not delayed pending scheduled clean-ups.

SecureTransport is independent of the content it transfers – the application architecture does not store or log any content information. Merchants can be confident that no primary account numbers or magnetic stripe data is being stored. In addition, SecureTransport's non-repudiation transfer receipts contain a one-way hash of the file, so the transfer cannot be compromised.

SecureTransport can protect data in its repository with 3DES encryption. Repository encryption is tied to application-level authentication and access controls, rather than to the underlying operating system. Decryption keys are stored in a protected key store and access credentials are encrypted and embedded in the application.

SecureTransport securely generates and stores keys. Symmetric enciphering keys are generated a random source. Key-encrypting RSA and PGP keys are stored in a protected key store with encrypted access credentials.

SecureTransport supports the PCI requirements for periodic key changes and revocation of old keys. All keys generated and stored in SecureTransport are subject to key expiration. The default is 365 days, but the expiration can be configured. The attempted use of an expired key is also flagged.

≫ **Requirement 4: Protect Cardholder Data**
PCI Challenge: Encrypt transmission of cardholder data and sensitive information across open, public networks.

Tumbleweed Solution: SecureTransport supports strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks. SecureTransport can be configured to limit the algorithms SSL can use to negotiate the session. SecureTransport supports AES 256 and DES-CBC3 encryption. For SafeTP Daemon (SFTPD) algorithms, SecureTransport supports 3DES with a key length of 192 and Blowfish with a key length of 128.

≫ **Requirement 6: Maintain a Vulnerability Management Program**
PCI Challenge: Develop and maintain secure systems and applications.

Tumbleweed Solution: Tumbleweed implements secure coding practices for SecureTransport and publishes internal coding guidelines under the close supervision of Tumbleweed's Chief Architect. Tumbleweed developers use automated tools such as Fortify to identify unsafe practices. In addition, Tumbleweed periodically submits its Web interfaces for third-party vulnerability assessments.

≫ **Requirement 7: Implement Strong Access Control Measures**
PCI Challenge: Restrict access to cardholder data by business need-to-know.

Tumbleweed Solution: SecureTransport provides custom definition of administrative roles and delegated roles, limiting access to only those who need it.

≫ Requirement 8: Implement Strong Access Control Measures

PCI Challenge: Assign a unique ID to each person with computer access.

Tumbleweed Solution: SecureTransport supports strong access control measures to meet PCI requirements for username-plus-password or token access control. For authentication, SecureTransport can require the SSL user to present a username and password as well as a client certificate. SecureTransport can also require both username and password and a public key to authenticate SSH, SSH File Transfer Protocol (SFTP) and Secure Copy (SCP) users. For remote users, SecureTransport supports two-factor authentication using a combination of username/password and RSA key (X.509 or SSH2) credentials. All stored passwords are encrypted using a one-way hash function.

SecureTransport supports PCI password-related requirements:

- SecureTransport requires that users confirm the old password before resetting their password, to verify user identity. An add-on security module is available to preclude users from choosing a new password that is the same as any of the last four passwords he or she has used.
- New users can be required to change passwords immediately after the first use.
- Administrators can disable accounts to revoke access for terminated users.
- Administrators can specify how frequently passwords are to be changed, meeting the PCI requirement to change passwords every 90 days.
- Administrators can specify the minimum number of alphabetic, numeric, and special characters required in a password, meeting the PCI requirement for a minimum of seven characters for passwords.
- Administrators can configure the number of failed login attempts before an account is locked, which meets the PCI requirement to lock out a user after no more than six failed attempts.
- Administrator and user sessions have separate configurable timeouts. The default setting is 15 minutes, after which a user will have to re-enter a password to reactive the session.

≫ Requirement 10: Regularly Monitor and Test Networks

PCI Challenge: Track and monitor all access to network resources and cardholder data.

Tumbleweed Solution: SecureTransport supports the PCI requirement to establish processes for linking all access to system components to an individual user. SecureTransport maintains detailed administrative logs that record user, timestamp, and substance of the change. All end-user access to files is audited and can optionally include a signed hash of the file content in an MDN receipt.

SecureTransport audit trails can be secured so that they cannot be altered. SecureTransport offers a tamper-evident record of transmission, and can optionally require that a user sign history audit records in MDN receipts. Access to tracking and audit reports is restricted to administrators whose roles explicitly include this permission. All audit logs are stored in a subdirectory specifically for this purpose.

SecureTransport provides a facility for periodic log rollover and maintenance. Log retention is highly configurable and is subject only to storage constraints, so a company can meet the PCI requirement to retain audit trail history for at least one year, including at least three months online. Logs can be exported for external archiving.

Conclusion

Tumbleweed protects lines of communication with employees and business partners, including bulk file transfers and email. For more than 15 years, Tumbleweed solutions have secured data, access, applications, and processes for the most demanding security environments, including 7 out of the top 10 worldwide banks, 8 out of the top 10 U.S. banks and 50 percent of the Fortune 100. Retailers facing PCI compliance mandates can leverage Tumbleweed's expertise and robust solutions to protect bulk file transfers and email from malicious hacker attacks and accidental data loss. Tumbleweed provides solutions that identify and protect sensitive cardholder data in transit, helping companies avoid painful data breaches and achieve compliance with PCI DSS requirements. Tumbleweed solutions incorporate proven security technologies vital to PCI compliance – comprehensive email security, secure file transfer, content filtering, strong encryption, access controls, monitoring and reporting, and more.

Tumbleweed Secures the Lines of Communication for PCI Compliance

Category	Requirement	Tumbleweed	MailGate	Secure Messenger	Secure Transport
Build and Maintain a Secure Network	Requirement 1: Install and maintain a firewall configuration to protect cardholder data	√			√
Build and Maintain a Secure Network	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security	√	√		√
Protect Cardholder Data	Requirement 3: Protect stored cardholder data	√	√	√	√
Protect Cardholder Data	Requirement 4: Encrypt transmission of cardholder data across open, public networks	√		√	√
Maintain a Vulnerability Management Program	Requirement 5: Use and regularly update anti-virus software	√	√		
Maintain a Vulnerability Management Program	Requirement 6: Develop and maintain secure systems and applications	√	√		√
Implement Strong Access Control Measures	Requirement 7: Restrict access to cardholder data by business need-to-know	√			√
Implement Strong Access Control Measures	Requirement 8: Assign a unique ID to each person with computer access	√			√
Implement Strong Access Control Measures	Requirement 9: Restrict physical access to Cardholder data	N/A	N/A	N/A	N/A
Regularly Monitor and Test Networks	Requirement 10: Track and monitor all access to network resources and cardholder data	√	√		√
Regularly Monitor and Test Networks	Requirement 11: Regularly test security systems and processes	N/A	N/A	N/A	N/A
Maintain an Information Security Policy	Requirement 12: Maintain a policy that addresses information security	N/A	N/A	N/A	N/A

Note: Grayed-out requirements fall outside the scope of email and FTP security hardware/software solutions.

ABOUT TUMBLEWEED

Tumbleweed provides security solutions for email protection, file transfers, and identity validation that allow organizations to safely conduct business over the Internet.

Tumbleweed offers these security solutions in three comprehensive product suites: MailGate, SecureTransport and Validation Authority. MailGate provides protection against spam, viruses and attacks, and enables policy-based message filtering, encryption and routing. SecureTransport enables business to safely exchange large files and transactions without proprietary software. Validation Authority is the world-leading solution for determining the validity of digital certificates.

The result: organizations using Tumbleweed security solutions can safely and securely use the Internet for business, significantly reducing their costs.

Tumbleweed®

California, USA
Corporate Headquarters
Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063

Phone: 650-216-2000/800-696-1978
www.tumbleweed.com

New York, USA
Tumbleweed Communications Corp.
245 Park Ave, 24th Floor
New York, NY 10167

Phone: 212-209-7363/800-696-1978
www.tumbleweed.com

United Kingdom
Tumbleweed Communications Ltd.
Hurst Grove, Sanford Lane
Hurst, Berkshire RG10 OSQ
UK

Phone: +44 (0)118 934 7100
www.tumbleweed.com

APAC
Tumbleweed Communications
Centennial Tower, Level 21
3 Temasek Avenue
Singapore 039190

Phone: 65-65497143
www.tumbleweed.com