

Papa Gino's Holdings Corporation

CHALLENGE

Find a cost-effective, scalable way to eliminate ad hoc security methods and protect mission-critical data and daily business transactions

SOLUTION

Unify security operations using the open standards of Trusted Platform Module (TPM) security technology and Wave Systems' suite of platform technologies including: Wave Systems EMBASSY Trust Suite software on Dell™ Latitude™ notebooks and Dell OptiPlex™ desktop computers and both Wave Systems Key Transfer Manager Server and Wave Systems Enterprise Authentication Server provided by Dell

BENEFIT

A standardized approach to enterprise security can reduce the risks and costs of network security, bolstering workplace efficiency

Recipe for Success

Open standards technologies provide the ingredients for delivering security across the Papa Gino's enterprise

Every success story begins with a great idea. For Papa Gino's Holdings Corporation, the big idea was hatched at a Boston pizza shop nearly half a century ago when a young man with a dream and a pizza recipe decided to use his belief in high-quality ingredients and service to build a New England pizza business. Today, the company founded by the entrepreneur operates one of New England's leading Italian quick-service restaurant chains, including 170 Papa Gino's establishments and 200 D'Angelo Sandwich Shop locations. Serving more than 50 million guests annually, Papa Gino's eateries dish up premium value for the company's patrons.

Technology has also been baked into the company's focus on high quality. Information technology systems at Papa Gino's support daily operations at company stores and in the corporate office. Thanks to its smart use of IT, employees are able to compile and share information—everything from point-of-sale and franchise transactions to payroll and employee data—throughout the enterprise's locations via the company network. "We realized early on that in a geographically dispersed environment, it is essential that employees are operationally connected and data is securely transmitted," says Chris Cahalin, network manager at Papa Gino's.

Tossing up security issues

When the company began looking to upgrade its point-of-sale equipment, Cahalin was also tasked with evaluating options for consolidating equipment and improving security. At the time, Papa Gino's did not have a unified approach to securing sensitive data at the store level or in the corporate office. As a result, employees



in departments like human resources and finance were hindered in their ability to implement stronger authentication and prevent unauthorized access to confidential e-mails, payroll records, and customer information.

Due to the lack of standardized TPM-enabled systems, employees were left to implement their own brand of security by building password managers or downloading third-party encryption software. Unfortunately, the ad hoc solutions resulted in wasted time and money spent retrieving information lost due to forgotten passwords, lost encryption keys, and missing laptops. "We were spending tens of thousands of dollars to recover or recreate lost work," says Cahalin. "It was clear that we needed a better way to secure information across the network and improve productivity for employees."

Changes to the menu

Prior to choosing Dell, Papa Gino's had a mixed IT environment with multiple vendors and different proprietary systems. The company needed a way to simplify and secure network operations for the enterprise. To strengthen the security of business data and help protect the sensitive information of its employees and customers, Papa Gino's chose Dell. The key ingredient? The focus at Dell on delivering open standards-based security technologies.

As Cahalin began to research Dell systems, he quickly became interested in TPM security technology to gain greater manageability, continuity, and efficiency while helping to secure corporate systems. The TPM device is a chip on the motherboard that hides encrypted information from the operating system, and therefore from harmful Trojan viruses and hackers. Operating like a bank vault, TPMs hold computer-generated encryption keys that are initialized and owned at the user level and can be securely copied—in an encrypted format—to backup servers to avoid data loss due to forgotten passwords or keys.

While other vendors were considered by Cahalin for the IT consolidation, Dell offered both open standards and TPM security on desktops and notebooks, which swayed the decision toward Dell. "Our research showed the open standards-based TPM solution integrated into Dell desktops and notebooks was excellent when compared to proprietary options. With the Dell approach, I realized that I had a cost-effective way to implement security literally overnight," says Cahalin.

The secret sauce

In order to implement the Dell-based security solution, employees at the Papa Gino's corporate office and store locations were provisioned with Dell OptiPlex GX280 and OptiPlex GX620 desktops as well as Dell Latitude D610 and Latitude D810 notebooks.

To facilitate the out-of-the-box implementation, the Dell equipment arrived at Papa Gino's locations with TPM devices pre-installed. Cahalin then installed Wave Systems EMBASSY Trust Suite software to provide end-user applications that work with the TPM technology to help solve and simplify security challenges.

Unlike other TPM offerings—which place limitations on the space and location of encrypted files—the TPM technology integrated into Dell desktops and notebooks allows for unrestricted locations and sizes of encrypted file storage. The combination of TPM technology and Wave EMBASSY Trust Suite software provides one of the first system-level authentication capabilities available on the market. While the powerful Wave Systems EMBASSY Security Center application, installed on OptiPlex desktops and Latitude notebooks, can actively manage the TPM device and user credentials, Papa Gino's chose to centrally manage all TPM-enabled devices using two Wave Systems server products: Key Transfer Manager Server and Enterprise Authentication Server.

"Right from the box, Dell security is as hot as our pizza. The TPM technology integrated into our Dell desktops and notebooks helped simplify network operations, lower costs and risks, and boost company productivity."

— Chris Cahalin
Network Manager
Papa Gino's Holding Corporation

Users have unprecedented flexibility with the integrated TPM technology to choose a strong combination of authentication factors that go beyond static, reusable passwords. High trust factors, such as TPM-protected certificates and passwords—and even biometric identification protocols—enable Papa Gino's employees to achieve a great level of authenticity when accessing information.

Additionally, securing e-mail is easy and fast with the integrated TPM system in place. Users simply click on an icon—supplied by EMBASSY Trust Suite and tightly integrated into Microsoft® Office software—to save and encrypt files or create digital certificates. EMBASSY Trust Suite software works in conjunction with integrated TPM technology on Dell computers to provide

the ability to quickly and securely launch digital certificates, which are used to safely verify, encode, and decode e-mail messages between senders and recipients. Using industry standards, Dell desktops and notebooks with integrated TPM technology and EMBASSY Trust Suite software interoperate with a certificate authority provider, increasing the ease of creating encrypted e-mail transmissions while helping to reduce the risks often associated with the process.

“What did we gain from all this? In a word, control. Dell has enabled the Papa Gino's corporation to control access to backup, recovery, and security for all of its data assets.”

— **Chris Cahalin**
Network Manager
Papa Gino's Holding Corporation

With identity theft a prevalent concern for anyone conducting business transactions across the Internet, IT departments are focusing on the protection of company and employee information. Private Information Manager (PIM) software included in Wave Systems EMBASSY Trust Suite loaded on Dell desktops and notebooks delivers instant identity management for Papa Gino's employees. By keeping personal data—such as contact information, passwords, bank access codes, and credit card numbers—securely protected in TPM-housed PIM software, users can avoid malicious phishing and pharming by predatory scammers. When a user is asked to complete or generate online forms, the PIM application safely populates them with the requested information.

The Dell security infrastructure also includes the Wave Systems Key Transfer Manager Enterprise Server and Enterprise Authentication Server applications. Using the Microsoft® Active Directory® service for user authentication and policy management and collaborating with EMBASSY Trust Suite's Key Transfer Manager client, Key Transfer Manager Enterprise Server works in the background to reliably detect, archive, and restore protected encryption keys from one TPM-enabled system to another. In the Papa Gino's enterprise, TPM-secured keys vaulted on each desktop and notebook are formatted into individual packages and then securely transmitted to the server for storage and subsequent

recovery. The strongest multi-factor user logons are easily managed and set for biometric, smart card, password, and machine authentication of a user's personal computer to a server. Using the EMBASSY Trust Suite platform, IT managers can easily implement different departmental security policies as required. For example, accounting employees could be required to log on to trusted computers using biometric and password authentication while employees in other departments, such as shipping, could continue using passwords, smart cards, or the TPM itself using public key infrastructure certificate authentication.

When asked to assess his new security capabilities, Cahalin offers a blunt assessment of the benefits. “What did we gain from all this? In a word, control,” says Cahalin. “Dell has enabled the Papa Gino's corporation to control access to backup, recovery, and security for all of its data assets.”

A feast of benefits

Papa Gino's is enjoying a heaping serving of advantages from the Dell infrastructure. Dell computers help protect personal information and intellectual property from being stolen or accessed by anyone other than intended users. Human resources employees can now securely transmit confidential records such as pay raise amounts and annual review records only to authenticated recipients. And IT administrators can focus on issues of strategic importance instead of putting out fires.

With automatic encryption at the user level, the company's network administrators are saving time and money. Prior to the use of Dell desktops and notebooks with TPM capabilities, Cahalin engaged third-party vendors to help encrypt content on the network before conducting system backups. Now while encryption keys reside locally in the TPMs, copies of the keys are automatically deposited to Key Transfer Manager Server so that all Papa Gino's information is protected and retrievable.

Securing digital certification used to be a time-consuming and expensive effort for IT administrators—and without digital certificates, sending vital content was risky. Now the dilemma is solved with integrated TPM and EMBASSY Trust Suite technology on Dell desktops and notebooks, as certification functions are built-in and managed by the system. Employees in the finance department, for example, can quickly and securely correspond with Papa Gino's banking partners by launching digital certificates right from their computer desktops.

“Prior to the Dell solution, unauthorized access to anything on the network was possible despite following today's best practices. With integrated TPM and EMBASSY Trust Suite technology on Dell desktops and notebooks, Papa Gino's has achieved easy encryption and low risk for every user on our system,” says Cahalin.

“Thanks to Dell and Wave Systems, data protection is at a whole new level.”

With the unified flexibility of the integrated Dell security package—rather than ad hoc passwords and methods for security at the user level—Cahalin no longer has to dedicate staff to long hours of recovering or recreating lost, stolen, or inaccessible data. Even business partners and franchisees can be folded into the enterprise-wide security implementation at Papa Gino's—because open standards provide the opportunity to manage any TPM, regardless of brand. And with

HOW IT WORKS

HARDWARE

- TPM-enabled Dell OptiPlex GX280, OptiPlex GX620 desktops; TPM-enabled Dell Latitude D610 and Latitude D810 notebooks

SOFTWARE

- Wave Systems EMBASSY Trust Suite
- Wave Systems Key Transfer Manager Server
- Wave Systems Key Transfer Manager Enterprise Server
- Wave Systems Enterprise Authentication Server

seemingly unlimited storage for encrypted files both on hard drives and the network, Papa Gino's benefits from the unwavering Dell focus on creating scalable enterprises.

“Right from the box, Dell security is as hot as our pizza. The TPM technology integrated into our Dell desktops and notebooks helped simplify network operations, lower costs and risks, and boost company productivity,” says Cahalin. “The net results are phenomenal.”

**GET MORE OUT OF YOUR
SCALABLE ENTERPRISE.**



Visit www.dell.com for more information.

February 2006
Printed in the U.S.A.
Dell cannot be responsible for errors in typography or photography. Dell, the DELL logo, Latitude, and OptiPlex are trademarks of Dell Inc. Microsoft and Active Directory are registered trademarks of Microsoft Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others. © 2006 Dell Inc. All rights reserved. Reproduction in any manner whatsoever without the written permission of Dell is strictly forbidden.