Enhance Security with Simple Two-Factor Authentication

Stronger Security and Lower Costs Are Closer Than You Think

Are You Prepared for 21st-Century Threats?

Your users are increasingly mobile and increasingly connected—accessing sensitive data and corporate networks from almost anywhere on a variety of devices. It is therefore no surprise that attacks are on the rise as well. They are not only more frequent, but also more sophisticated and purpose-driven. Malware and hackers are determined to steal your company’s and your customers’ confidential data, and are successful far too often, costing companies an average of $7.2 million per breach. It is a trivial matter these days for data thieves to gain access to network credentials and customers’ online accounts because the traditional username and password approach to security is broken. One weak password can have extremely costly consequences, including brand damage, compliance violations and fines, and even litigation.

When faced with the need to create multiple logins for multiple systems, employees often take shortcuts. They might use the same password, which is often a standard dictionary word or common phrase. These passwords can be simple to crack in brute force attacks. Employees might also fall victim to phishing schemes, social engineering, and man-in-the-browser attacks, which can put even strong user names and passwords at risk.

Fortunately, you can protect data, networks, and user accounts by deploying solutions from Intel and Symantec.
Increase Security, Not Complexity

Symantec and Intel can help you protect your networks and user accounts from unauthorized access with two joint solutions:

• Identity Protection—One-Time Password. This solution enables simple two-factor authentication for customer web portals and internal assets such as VPNs and software-as-a-service (SaaS) portals. Authentication tokens embedded into PCs and laptops equipped with the latest Intel® Core™ vPro™ processors generate a one-time password, which is validated by Symantec® Validation and ID Protection (VIP) Service.

• Identity Protection—PKI. This solution makes it easier to protect critical information and applications through public key infrastructure (PKI)-based authentication. Authentication keys and certificates are securely stored in the PC or laptop’s hardware while backend management of the PKI environment is handled by Symantec® Managed PKI Service. Like Identity Protection—One-Time Password, this solution protects web sites and internal assets. It also enables advanced functions such as digital signing, document verification, and e-mail encryption.

These identity-protection solutions provide hardware-enhanced defense against unauthorized account and network access while eliminating the need for discrete hardware tokens that can be costly to configure and manage, and easy for users to lose.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Protect networks from unauthorized user access. Protect web-based customer accounts from compromise.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Intel Components</td>
</tr>
<tr>
<td>Identity Protection—OTP</td>
<td>Intel® Identity Protection Technology (Intel® IPT) with OTP: Enables hardware-based two-factor authentication that is simpler and more secure than software-only solutions.</td>
</tr>
<tr>
<td>Symantec Components</td>
<td>Symantec® Validation and ID Protection Service (VIP): Cloud-based service that verifies the validity of one-time passwords generated by Intel IPT.</td>
</tr>
<tr>
<td>Identity Protection—PKI</td>
<td>Intel® IPT with PKI + Protected Transaction Display (PTD): Secures private encryption keys for PKI environments; encrypted display for protection against malware scraping of PINs and other credentials.</td>
</tr>
<tr>
<td>Symantec Components</td>
<td>Symantec® Managed PKI Service: Provides enterprise-scale PKI without the cost and overhead associated with a self-deployed and self-managed infrastructure.</td>
</tr>
</tbody>
</table>

Protect Account Security with Identity Protection—One-Time Password

You can counteract weak passwords and poor password practices more easily than you might think with Identity Protection—One-Time Password (OTP). It provides two-factor authentication using Intel IPT with OTP and Symantec VIP, a cloud-based authentication service that validates OTPs generated by Intel IPT. This joint solution strengthens account and VPN security—especially for networks that are accessed by mobile employees—by adding a second factor to the traditional username and password approach. Cloud-based authentication helps organizations protect their data, comply with industry regulations, and enable a mobile workforce.

With Identity Protection—One-Time Password, you can deploy:

• Simple, hardware-based two-factor authentication
• Secure remote access through the Web or VPN
• Web and VPN authentication
• Protection when digital certificates are not supported
• Protection for legacy applications
• RSA token replacement
In a typical two-factor authentication infrastructure, IT assigns users a physical fob that changes tokens on a regular basis. The fob generates the tokens using the same algorithm as the remote authentication service. When a user authenticates, they must provide a username and password combination, in addition to the fob token.

Systems equipped with Intel IPT contain an embedded token that uses Symantec algorithms to generate OTPs. When used in conjunction with Symantec VIP authentication on services such as a web site, VPN, or other enterprise applications, users provide their user name, password, and the OTP generated by Intel IPT to log on. Because users can use an OTP only once, this two-factor authentication method is stronger than a simple username and password. With Symantec VIP and Intel IPT, authentication is associated with both the user and the laptop or PC they use, protecting corporate networks from unauthorized access even if the user’s login credentials are compromised.

Symantec VIP and Intel IPT can also protect website customers from identity theft. When a customer visits an OTP-enabled web site and opts in for the additional security, Intel IPT generates a secure OTP, which Symantec VIP validates, and the customer enters it along with his or her user name and password. The solution ensures that identity thieves can’t access customer accounts, even if the thieves have stolen or otherwise cracked a user name and password.

Identity Protection—PKI can power:

- Hardware-based two-factor authentication using digital certificates
- Secure remote access through the Web or VPN
- Certificate-based Web authentication
- E-mail encryption and decryption
- Application-level encryption
- Digital-signature support
- Offline authentication
- Auditing for strict compliance requirements
- VPN authentication

An on-premises PKI solution can be complex and costly. Such deployments often require dedicated, trained personnel to create and manage the infrastructure. Because of the need for highly secure facilities, policies and procedures for protecting the private keys used for certificates, and highly available hardware and software, costs and complexity can rise rapidly. Symantec Managed PKI Service helps overcome the cost and complexity of a PKI infrastructure. It provides scalability and availability, while shielding organizations from complex operational processes and certificate management.

Trust is also a key aspect of any PKI solution. An organization might be able to act as its own certificate authority and issue its own certificates, but those certificates will most likely not be trusted outside of the organization. The organization might need to build a separate, additional PKI infrastructure using a trusted, third-party certificate authority for business-to-business communications. By contrast, Symantec Managed PKI Service offers the most recognized and trusted digital certificates in the world, enabling gold-standard PKI solutions.

A managed PKI solution from Symantec can also scale more easily to the growing needs of an organization. Many organizations start with simple solutions to authenticate devices or users on a network, but later move into more complex solutions that require public trust, such as secure e-mail or document signing. With traditional PKI solutions, organizations need to understand in advance which particular capabilities they will need, and then overbuild the infrastructure to accommodate future growth. With Symantec Managed PKI Service, the infrastructure is already in place to enable any PKI-related capability on-demand.

Figure 1. Strengthen protection for customers’ data in online accounts with Symantec® VIP and Intel® IPT

Simplify Your PKI-Based Solutions with Identity Protection—PKI

Your organization can deploy strong authentication and advanced public key infrastructure (PKI)-based security capabilities, such as e-mail encryption and digital signing, simply and cost effectively with Identity Protection—PKI. The solution is based on Symantec Managed PKI Service. This cloud-based service makes it easier for organizations to issue, renew, and revoke certificates without the hassles and costs associated with maintaining an on-premises PKI infrastructure.
When organizations use the Symantec service with Intel IPT, they can further strengthen security and protect sensitive information. Using a protected space on PC hardware, Intel IPT secures the private encryption keys for use with public Symantec certificates. Symantec Managed PKI Service works seamlessly with Intel IPT to provide a PKI solution that is faster, simpler, and more cost-effective than an on-premise solution. Organizations can strengthen the solution further through Intel IPT with protected transaction display (PTD). This hardware-embedded I/O encryption technology hides user input, such as PINs, from malware scrapers designed to capture keystrokes.

Figure 2. Intel PTD protects the display from malware scraping and proves human presence at the PC to help protect against man-in-the-middle and man-in-the-browser attacks

With Symantec Managed PKI Service and Intel IPT, organizations can deploy enterprise-scale PKI infrastructure without the costs and overhead of a self-deployed and self-managed infrastructure.

Secure Your Networks and Simplify Your Infrastructure

Want to secure your networks and user accounts while simplifying your infrastructure? Symantec VIP, Symantec Managed PKI Service, and Intel IPT provide powerful, cloud-based and hardware-based tools for securing your data. You can combat the ever-increasing sophistication of attacks while giving your employees the mobility they demand, all without the complexity, redundancy, and scalability problems associated with on-premise PKI and OTP solutions.

For more information, please visit: www.intel.symantec.com/security, or contact your Symantec or Intel sales representative to arrange for a proof-of-concept today.

2 No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Core™ processors may require additional software, hardware, services and/or an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details.
3 No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd or 3rd generation Intel® Core™ processor, enabled chipset, firmware, and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://ipt.intel.com.

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Copyright © 2012 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, and Intel vPro are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.