This page intentionally left blank
Contents
Section I. Overview ................................................................. 5
What is Trend Micro Smart Protection Complete ........................................ 5
Section II. Trend Micro Smart Protection Complete ...................................... 7
  Section II.2 Trend Micro Smart Protection for Endpoints ................................ 8
    Section II.2.1 Trend Micro Control Manager ............................................. 8
    Section II.2.2 Trend Micro OfficeScan (Endpoint Protection) ........................ 8
    Section II.2.2.a Trend Micro Integrated Data Loss Prevention ......................... 9
    Section II.2.2.b Trend Micro Mac Security ............................................. 10
    Section II.2.2.c Trend Micro Virtual Desktop Infrastructure .......................... 10
  Section II.2.3 Trend Micro Endpoint Application Control ................................ 10
  Section II.2.4 Trend Micro Mobile Security ............................................. 11
  Section II.2.5 Trend Micro Endpoint Encryption ........................................ 11
  Section II.2.6 Trend Micro ServerProtect for Windows .................................. 11
  Section II.2.7 Trend Micro ServerProtect for Linux ...................................... 12
  Section II. 2.8 Trend Micro Vulnerability Protection .................................... 12
  Section II.2.9 Trend Micro Instant Messaging Security ................................... 13
  Section II.2.10 Trend Micro ScanMail for Microsoft Exchange ......................... 13
  Section II.2.11 Trend Micro ScanMail for IBM Lotus Domino .......................... 13
  Section II.2.12 Trend Micro PortalProtect™ Suite for Microsoft® Sharepoint® .. 14
  Section II.2.13 Trend Micro InterScan Messaging Security Virtual Appliance ...... 14
  Section II.2.14 Trend Micro InterScan Web Security Virtual Appliance .............. 15
  Section II.2.15 Trend Micro InterScan Web Security as a Service ..................... 15
  Section II.2.16 Trend Micro Hosted Email Security ..................................... 16
  Section II.2.17 Worry-Free Business Security Services ................................ 16
    Section II.2.18 Support ........................................................................ 17
Section III. Architecture ........................................................................ 17
Section IV. Planning Your Deployment .................................................... 18
Section V. Best Practices Considerations ............................................... 23
  Section V.1 Deploying Multiple Applications ........................................... 26
Section VI. Licensing ............................................................................. 27
Appendix I. Smart Protection Complete Acronyms ...................................... 29
Section I. Overview

What is Trend Micro Smart Protection Complete

Your users are accessing corporate resources in the office, at home, on the road, or anywhere in between. And they are not always working on a corporate network, device, or application. So it’s difficult to protect them anytime, anywhere. To further complicate matters, you’re moving to the cloud. But you’re not all there. And you don’t want to be locked into a single approach. At the same time, you need to have visibility across all layers of security.

While traditional security isn’t keeping up with your users, threats ARE. You need constant vigilance to hit threats head on with a dragnet of interconnected security solutions that consolidates your view across all threat vectors. And you need a forward-thinking security vendor that can predict developments before they strike. It’s time to think seriously about complete user protection.

Trend Micro™ Complete User Protection is an interconnected suite of security functions that protects your users no matter where they are going or what they are doing. Trend Micro’s modern security solutions deliver the best protection at multiple layers: endpoint, application, and network using the broadest range of anti-malware techniques available. Plus, you can evolve your protection along with your business using flexible, on-premise, cloud and hybrid deployment models that fit your IT environment today and tomorrow. And most importantly, you can manage users across multiple threat vectors from a single management console, giving you complete oversight of your security all across your environment.

Trend Micro Complete User Protection protects all user activities, reducing the risk of sensitive information loss. You get advanced protection with endpoint security, email and collaboration security, web security, and mobile security. The result is a protective shield that is extremely difficult for cyber criminals to penetrate. Plus, you can analyze suspicious behavior better with access to optional sandboxing capabilities across multiple layers of protection, from endpoint and mobile to mail server and web gateway.

You can trust Trend Micro to deliver the best protection for all of your users.

- **Broadest threat protection.** You get a full range of integrated protection across gateways, endpoints, mobiles, servers, and applications. All across the network, you get multiple layers of anti-threat techniques that prevent even the most sophisticated threats.

- **Advanced threat protection.** In addition to world-class security fueled by global threat intelligence, you’re protected by integrated threat sandboxing, Command & Control detection, application control, behavior monitoring, and host intrusion protection.

- **Better protection of your information.** Integrated data loss prevention protects your information through instant messaging to the endpoint and web and email gateways. Endpoint and email encryption ensures only authorized eyes can see your information. And application and port control prevents users from sending information where it doesn’t belong.
- **Comprehensive view of user security.** Now you can manage all layers of security from a single management console for comprehensive analysis of data and threats across your user protection.

- **Real-time interconnected threat intelligence.** Take your protection beyond the traditional signature approach to benefit from threat insights from Trend Micro’s threat defense experts and real-time updates from our global threat intelligence network.

Trend Micro Complete User Protection ensures maximum flexibility by providing multiple deployment models that best fit your IT strategy. With Trend Micro, you have the flexibility to choose the deployment model that fits you best, including a mix of on-premise and cloud. And, instead of managing discrete solutions for on-premise and cloud-based security, Trend Micro gives you the flexibility to manage cloud and on-premise deployments from a single management console.

You not only get a single view of all threat in a timely and efficient manner. Plus, you’re able to dive deeper to easily understand how threats are spreading for a particular user across multiple systems. With visibility across the entire threat lifecycle, threat investigations are much simpler.

Trend Micro Complete User Protection gives you stronger security that’s also lightweight so it won’t impact the user experience, and it supports all of the devices and applications that your users typically want. Finally, global threat intelligence from Trend Micro™ Smart Protection Network™ rapidly and accurately identifies new threats across all layers of security with real-time threat updates, providing complete user protection from an industry leader you can trust.

Trend Micro makes Complete User Protection simple, with a series of pre-packaged suites that address the concerns that are most important to you. The pre-package suites are: Smart Protection for Endpoints, eight additional Security Solutions, and a Support Services offering. These suites along with the business problem and solutions provided are discussed in Section II.
Section II. Trend Micro Smart Protection Complete

Trend Micro Smart Protection Complete integrates security across all layers.

Figure 1. Example Network Diagram: On Premise

Figure 2. Example Network Diagram: Cloud
### Trend Micro Smart Protection Complete Product Matrix

<table>
<thead>
<tr>
<th>Centralized Management</th>
<th>Control Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Protection</td>
<td>OfficeScan</td>
</tr>
<tr>
<td></td>
<td>- Integrated Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>- Mac Security</td>
</tr>
<tr>
<td></td>
<td>- Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>Application Control</td>
<td>Application Control</td>
</tr>
<tr>
<td>Data Security and Confidentiality</td>
<td>Endpoint Encryption</td>
</tr>
<tr>
<td>Mobile Security</td>
<td>Mobile Security</td>
</tr>
<tr>
<td>Protection for Business Applications</td>
<td>ServerProtect for Windows</td>
</tr>
<tr>
<td></td>
<td>ServerProtect for Linux</td>
</tr>
<tr>
<td>Host Intrusion Protection</td>
<td>Vulnerability Protection (formally named as IDF)</td>
</tr>
<tr>
<td>Cloud Solution for Endpoint and Mobile</td>
<td>Worry-Free Business Security Services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend Micro Smart Protection Complete – Additional Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging</td>
</tr>
<tr>
<td>E-Mail</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Sharepoint</td>
</tr>
<tr>
<td>Gateway Security</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cloud Solutions for Email and Web</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Table 1: Smart Protection Complete Product Matrix**

### Section II.2 Trend Micro Smart Protection for Endpoints

#### Section II.2.1 Trend Micro Control Manager

As enterprises deploy security solutions across multiple layers of their IT infrastructure to protect against a wide range of threats, it is becoming increasingly difficult to centrally manage security and data protection policies across the enterprise. To address the resulting complexity, operational inefficiency, and loss of visibility, organizations require consistent security management that bridges IT silos that often separate threat and data loss prevention. A centralized approach will improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administration.

Trend Micro Control Manager™ provides central threat and data loss prevention (DLP) policy management across layers of the IT infrastructure. Customizable data displays provide the visibility and situational awareness that equip organizations to rapidly assess security status, identify threats, and respond to incidents. Control Manager enables you to streamline administration and achieve more consistent policy enforcement with single-click deployment of data protection policies across endpoint, messaging, and gateway solutions.

#### Section II.2.2 Trend Micro OfficeScan (Endpoint Protection)

In the “bring-your-own-device” (BYOD) environment, protecting your endpoints against ever-evolving threats has become a costly juggling act for IT managers. With mobile devices and cloud computing
thrown into the picture, protecting your data from loss or theft is top of mind. Add to that the performance issues associated with trying to apply traditional security to virtual desktop infrastructures and it's clear, IT needs a flexible endpoint security platform that will adapt to changing needs with a light and lean architecture geared for performance.

Trend Micro™ OfficeScan™ endpoint security delivers real-time protection against the latest threats, using a light and lean client optimized for physical and virtual endpoint deployments. OfficeScan enhances your endpoint protection with cloud-based global threat intelligence, integrated data loss prevention (DLP), and a virtualization-aware client that reduces the endpoint footprint, protects sensitive data, and improves endpoint performance across the enterprise.

Section II.2.2.a Trend Micro Integrated Data Loss Prevention

Now more than ever, your data is on the move—whether it’s on a laptop, flash drive, or moving across physical, virtual, and cloud infrastructures. At any point along the way, your financial data, customer information, intellectual property, or trade secrets could be lost or stolen. Securing this data is further complicated by several growing risk factors:

- Rapidly evolving compliance regulations and mandates
- Continued growth of workforce mobility
- Employees using their own mobile devices and consumer apps for work
- Rising frequency of advanced persistent threats (APTs) and data breach incidents

To avoid embarrassment, reputation damage, regulatory fines, and revenue loss, today’s enterprise must be able to identify, track, and secure all confidential data from multiple points within the organization without impacting employee productivity and performance. In the past, many organizations tried traditional data loss prevention (DLP) solutions but found they were too intrusive, too complex to manage, and too costly to acquire, deploy, and maintain.

Trend Micro™ Integrated DLP minimizes the complexity and cost of data security by integrating DLP functionality directly into your existing Trend Micro solutions and management consoles. With a lightweight plug-in, you can quickly and easily gain visibility and control of your sensitive data and prevent data loss via USB, email and web. The DLP plug-in requires no extra hardware or software, and it leverages built-in regional and industry-specific templates to simplify deployment. Integrated DLP allows you to deploy data security for a fraction of the cost and time of traditional enterprise DLP solutions.

The Trend Micro Data Loss Prevention Module, a part of the OfficeScan product, protects your sensitive data for maximum visibility and control. Additional features include:

1. Protection of private data—on or off network
2. Coverage of the broadest range of devices, applications, and file types
3. Identification of sensitive data throughout your network
4. Detection of data-stealing malware and mitigates risky behavior
5. Improved compliance with greater visibility and enforcement
Section II.2.2.b Trend Micro Mac Security
The Trend Micro Security for Mac Module is a part of the OfficeScan product. The administrative console gives you complete control and visibility for the Apple Macintosh clients. Trend Micro Mobile Security for Mac protects Apple Macintosh clients on your network by preventing them from accessing malicious sites and distributing malware—even if the malware is not targeted at Mac OS X. Trend Micro Mac Security also:

1. Reduces exposure to web-based threats, including new Mac-targeting malware
2. Blocks malware for all systems, including both Mac OS X and Windows
3. Adheres to Mac OS X look and feel for positive user experience
4. Saves time and effort with centralized management

Section II.2.2.c Trend Micro Virtual Desktop Infrastructure

You’re looking to extend virtualization benefits to the desktop. Virtualization can isolate control of desktop environments, streamline management, and lets you consolidate hardware. But using endpoint security products designed for physical endpoints to protect virtual desktops can cause serious resource bottlenecks and generate “security storms” that impact performance. This type of contention and consumption of server resources can lead to sub-optimal consolidation ratios and undercut the ROI of your Virtual Desktop Infrastructure (VDI) initiatives. But securing your VDI environments doesn’t have to mean sacrificing performance and resources.

Trend Micro’s comprehensive, VDI-centric security for virtual desktops will help you improve protection and performance. And in the process, you’ll maximize consolidation ratios with security solutions designed specifically to handle the rigors of desktop virtualization. It’s results like these that have helped make Trend Micro the #1 leading provider of virtualization security.

Whether you are extending your virtualization successes from servers to desktops or looking for a unified approach for all your physical and virtual desktops, Trend Micro has a solution that will help you maximize protection and performance.

Section II.2.3 Trend Micro Endpoint Application Control

With hundreds of thousands of new malicious software applications being rolled out daily, it has become extremely difficult to protect all potential threat vectors. Without application control, you risk losing private company data from the machines of users who may be doing things they shouldn’t be doing with applications they shouldn’t be using. You need to safeguard data and machines against both inadvertent end user behavior and unauthorized infiltration via unauthorized applications. Unfortunately, traditional antivirus doesn’t offer the capabilities to do this. You need a layered approach to security that proactively blocks malware before it executes on the endpoint via bad applications. Plus you need to be able to quickly react to malware when it does reach the endpoint.

Trend Micro Endpoint Application Control allows you to enhance your defenses against malware and targeted attacks by preventing unwanted and unknown applications from executing on your corporate endpoints. With a combination of flexible, easily managed policies, whitelisting and blacklisting capabilities, as well as a global, cloud-powered application database, this easy-to-manage solution significantly reduces your endpoint attack exposure. To support a layered approach to security,
Endpoint Application Control integrates with Trend Micro Complete User Protection solutions to deliver multiple layers of interconnected threat and information protection.

Section II.2.4 Trend Micro Mobile Security
Companies that allow BYOD can boost productivity and reduce overall IT and support costs—but there are risks involved. To reap the advantages, you need mobile security that can protect the wide range of mobile devices and applications, in addition to protecting against threats and corporate data loss.

Trend Micro™ Mobile Security is a 4-in-1 solution that integrates mobile device security, mobile application management, mobile device management, and data protection, giving you full visibility and control of mobile devices, apps, and data through a single built-in console. Mobile Security also integrates with Trend Micro Control Manager™, which can automate the management of one or multiple servers along with other Trend Micro security solutions. By enabling centralized policy deployment and visibility across Trend Micro endpoint, messaging, web, and gateway security, it greatly reduces complexity and costs compared to standalone mobile security and MDM solutions that require new management infrastructures.

Unlike other solutions, Trend Micro Mobile Security integrates layers of data protection to secure your corporate data—no matter where it goes. Encryption, DLP, remote lock and wipe, password enforcement, and other tools work together with device security and app management to keep your data safe.

Section II.2.5 Trend Micro Endpoint Encryption
The proliferation of data and bring-your-own devices in today’s enterprises has increased the complexity of protecting confidential data, meeting compliance mandates, and preventing costly data breaches. Ensuring that sensitive data is secured in the case of device loss has never been more difficult.

Trend Micro™ Endpoint Encryption encrypts data on a wide range of devices—Windows and Macintosh laptops, desktops, CDs, DVDs, USB drives and any other removable media. This solution combines enterprise-wide full disk, file/folder, and removable media encryption with granular port and device control to prevent unauthorized access and use of private information. A single, well-integrated management console allows you to manage your users holistically—using the same interface for endpoint protection and other Trend security products. Deploying Trend Micro Endpoint Encryption helps ensure that your data will continue to be protected as your mobile computing devices and organizational needs change.

Section II.2.6 Trend Micro ServerProtect for Windows
Enterprise servers can be a vulnerable, centralized point of information exchange. Even from inside the network, users or applications without adequate protection can unintentionally upload infected files to the server, which can spread to other systems that access these files. Additionally, large organizations may have hundreds or thousands of individual server machines that require monitoring, configuration, and maintenance. More importantly, today’s sophisticated attacks can target multiple points on the network and leave unseen trails of damage and the potential for re-infection.
Trend Micro™ ServerProtect™ delivers the industry’s most reliable virus, spyware and rootkit protection while simplifying and automating security operations on servers. ServerProtect scans and detects malware in real time and incorporates cleanup capabilities to help remove malicious code and repair system damage. Administrators can use one management console to centrally enforce, administer, and update malware protection on every server throughout an organization. This robust solution enables enterprises to secure the entire server file system including compressed archives, distribute virus patterns to remove any viruses that get through, and help automate the damage cleanup process to resolve problems left by virus infections. As a result, the cost and efforts associated with a virus infection can be significantly reduced.

Section II.2.7 Trend Micro ServerProtect for Linux

Linux-based servers frequently interact with clients running other operating systems, such as Microsoft™ Windows™. They store and serve files created on and for those platforms. At the same time, the increasing popularity of the Linux platform has resulted in the growth of viruses and other malware specifically targeting Linux servers. With Linux now representing 15-20% of the worldwide server market and growing, these attacks are becoming more frequent and more severe. Thus, securing Linux-based servers from hosting infected files is imperative for any enterprise.

Trend Micro ServerProtect for Linux 3.0 offers comprehensive real-time protection for enterprise web-servers and file-servers, preventing them from spreading viruses, spyware, and other Web threats to internal or external endpoints. Managed through an intuitive portable Web-based console, ServerProtect provides centralized virus/malware scanning, pattern updates, event reporting, and configuration. The solution’s stability and reliability is evidenced by certifications from all major Linux vendors as well as independent third parties such as Virus Bulletin. ServerProtect for Linux is a key component in the comprehensive threat prevention offered by Trend Micro™ Enterprise Protection Strategy.

Section II. 2.8 Trend Micro Vulnerability Protection

Today’s enterprise endpoints face more sophisticated attacks than ever, especially when they are outside the corporate network and no longer protected by multiple layers of security. In addition, point of sales devices and networked devices with embedded operating systems are difficult to update and patch. To keep your business fully protected from breach or targeted attack, all types of endpoints require a blended approach to protection that secures data and applications from hacking attempts, Web threats, and the increasing threat of vulnerabilities being exploited.

Trend Micro Vulnerability Protection provides earlier, stronger endpoint protection by supplementing client-level antivirus and anti-malware security with pro-active virtual patching. A high-performance, deep-packet inspection engine monitors incoming and outgoing traffic for network protocol deviations, suspicious content that signals an attack, or security policy violations. Vulnerability Protection prevents vulnerabilities from being exploited with easy and fast to deploy filters, providing full protection before patches can be deployed. When used in conjunction with additional Trend Micro endpoint products, Vulnerability Protection provides the industry’s most secure protection for endpoints, whether they are on the network, mobile, or remote.
Formerly, the Trend Micro Intrusion Defense Firewall (IDF) Module was an add-on within the OfficeScan product, and is now available as a standalone application. Its network-level Host Intrusion Prevention System (HIPS) stop zero-day threats immediately with and enables virtual patching. Additional capabilities are:

1. Shield vulnerabilities in operating systems and client applications before patches are available.
2. Deploy true zero-day protection from known and unknown threats.
3. Protect your critical platforms, including Windows 8.

Section II.2.9 Trend Micro Instant Messaging Security
A growing number of companies use instant messaging to connect employees, partners, and customers in real time. While live communication improves productivity, it also presents a new opportunity for cybercriminals to work more quickly, spreading malware, luring victims to malicious sites, and stealing data in a flash. Given the instant exposure to fast-moving threats, instant messaging protection is critical.

Trend Micro™ IM Security for Microsoft™ Lync and Office Communications Server (OCS) secures your enterprise IM communications by stopping threats instantly. With its Web Reputation capability, powered by Trend Micro’s Smart Protection Network, IM Security takes advantage of a unique cloud-client architecture and correlated threat intelligence to block links to malicious sites—before the links can be delivered. Combined with our leading antivirus, new antispyware, and zero-day protections, IM Security works to thwart attacks sooner, before any damage can occur. With flexible content filtering, IM Security also prevents inappropriate IM use and data theft.

Section II.2.10 Trend Micro ScanMail for Microsoft Exchange
More than 90% of targeted attacks begin with a spear phising email, which means your mail server security is more important than ever. Unfortunately, most mail server security solutions, including the limited set of built-in protections in Exchange 2013, rely on pattern file updates, which only detect traditional malware. They don’t include specific protections to detect malicious URLs or document exploits commonly used in targeted attacks or advanced persistent threats (APTs).

Trend Micro ScanMail™ Suite for Microsoft® Exchange™ stops highly targeted email attacks and spear phising by using document exploit detection, enhanced web reputation, and sandboxing as part of a custom APT defense—protection you don’t get with other solutions. In addition, only ScanMail blocks traditional malware with email, file, and web reputation technology and correlated global threat intelligence from Trend Micro™ Smart Protection Network™ cloud-based security.

Time-saving features like central management, template-based data loss prevention (DLP), and role-based access have earned ScanMail the lowest administration overhead and TCO of the five leading security vendors, based on a comparison study by Osterman Research. ScanMail also delivers high performance with native 64-bit support—for the fastest mail throughput speeds.

Section II.2.11 Trend Micro ScanMail for IBM Lotus Domino
Most mail server security solutions rely on periodic updates and threat databases—they don’t detect malicious URLs or targeted attacks such as advanced persistent threats (APTs). These hidden threats
usually enter the network through highly targeted emails, making the messaging gateway and mail server the right place to stop them.

Like its Exchange sibling, ScanMail™ Suite for IBM® Lotus® Domino™ stops highly targeted email attacks, such as spear phishing, by using document exploit detection, enhanced web reputation, and sandboxing as part of a custom APT defense. ScanMail also blocks traditional threats with reputation technology and correlated global threat intelligence from Trend Micro™ Smart Protection Network™ cloud-based security.

Time saving features like central management, template-based data loss prevention (DLP), role-based access and Domino optimizations enable ScanMail to lower TCO by 35% according to analyst research.

Section II.2.12 Trend Micro PortalProtect™ Suite for Microsoft® Sharepoint®
Many companies are now using Microsoft® SharePoint® to connect with employees, partners, and customers for real-time collaboration. Businesses are also using more SharePoint capabilities than ever before—moving beyond simple content repositories to build team sites, create intranet and extranet portals, utilize wikis and blogs, and create social communities.

These dynamic collaboration environments help improve your productivity, but they also increase your security risks, especially when opened to external parties.

Trend Micro™ PortalProtect™ secures your collaborations with a dedicated layer of protection that guards against malware, malicious links, and other threats that SharePoint administrators are often unaware of. Its web reputation technology blocks malicious links from entering your web portals, while its powerful content filtering scans both files and web components of SharePoint.

PortalProtect goes above and beyond standard antivirus protection by delivering scalable strong web threat protection and data loss prevention.

Section II.2.13 Trend Micro InterScan Messaging Security Virtual Appliance
Most of the day-to-day activities for employees are creating and responding to email. More than 90 percent of all email is spam. With the rise of targeted spear phishing, even your savviest employees can mistakenly click on a malicious link and expose your enterprise to cybercrime.

Trend Micro™ InterScan™ Messaging Security provides the most comprehensive protection against both traditional and targeted attacks. Using the correlated intelligence from Trend Micro™ Smart Protection Network™ and optional sandbox execution analysis, it blocks spam, phishing and advanced persistent threats (APTs). The included hybrid SaaS deployment option combines a powerful gateway virtual appliance with a SaaS pre-filter that stops majority of threats and spam in the cloud—closer to their source. This hybrid solution delivers the best of both worlds: the privacy and control of an on-premise appliance with an in-the-cloud pre-filter for resource efficiency and proactive protection.
The Data Privacy and Encryption Module solves the toughest regulatory compliance and data protection challenges by securing outbound data. This optional module offers easy-to-use identity-based encryption and customizable data loss prevention (DLP) templates for quick deployment.

Section II.2.14 Trend Micro InterScan Web Security Virtual Appliance

Traditional secure web gateway solutions that rely on periodic updates to cyber threats cannot keep pace with today’s rapidly evolving web threats. In addition to blocking malicious code, inappropriate websites, and targeted attacks, security managers also need to secure the expanding use of Web 2.0 and cloud-based applications while reducing overhead and bandwidth costs.

Trend Micro™ InterScan™ Web Security dynamically protects against cyber threats at the Internet gateway. With the growing use of cloud-based consumer applications in the workplace, application visibility is essential to understand network risks. By integrating application control, zero-day exploit scanning, anti-malware scanning, Advanced Persistent Threat (APT) detection, real-time web reputation, URL filtering, and anti-botnet detection, InterScan Web Security delivers superior protection from advanced threats.

You can prevent sensitive data from leaving your organization with integrated data loss prevention (DLP) for InterScan Web Security. With customizable templates, the optional Data Loss Prevention Module filters information to help you with regulatory compliance and data privacy. With integrated DLP at the Web gateway, you can:

1. Scan outbound traffic for content that includes sensitive data
2. Create policies using predefined templates to better meet regulatory privacy requirements by filtering personally identifiable information
3. Generate DLP policy violation reports tied to specific users
4. Provide auditing functions to measure DLP policy effectiveness

Section II.2.15 Trend Micro InterScan Web Security as a Service

Trend Micro™ InterScan™ Web Security as a Service dynamically protects against cyber threats in the cloud, before they reach your users or network. Because it is located in the cloud it protects any user, in any location, on any device, all based on a single policy that moves with the user. Using the cloud ensures that the solution will grow flexibly with your business without the need to purchase, manage, or maintain software or hardware. Even if you already have a secure web gateway on premises, you can use InterScan service as an additional layer of security to more simply and cost-effectively secure remote offices and mobile employees. Better yet, you’ll avoid the high costs of backhauling traffic to your corporate network or managing multiple secure gateways at multiple offices.

InterScan Web Security as a Service gives you visibility and control of how safely your users interact with today’s most common applications and protocols. The service delivers superior protection from advanced threats by integrating application control, zero-day exploit and anti-malware scanning, Advanced Persistent Threat (APT) detection, real-time web reputation, URL filtering, and anti-botnet detection in a single solution. Because cyber criminals never stand still, the InterScan service leverages
real-time threat intelligence from the Trend Micro Smart Protection Network™, which applies real-time intelligence from 10 billion URL inquiries a day.

The Data Privacy and Encryption Module solves the toughest regulatory compliance and data protection challenges by securing outbound data. This optional module offers easy-to-use identity-based encryption and customizable data loss prevention (DLP) templates for quick deployment.

Section II.2.16 Trend Micro Hosted Email Security
Email is mission critical, but spam and email-based malware volume is growing exponentially; it’s difficult to keep up. At the same time, while other critical projects are pending—like Voice over IP, adding infrastructure capacity and securing your mobile workforce—that doesn’t mean you can afford to neglect email security maintenance. Doing so will lead to a decline in your email security and spam-blocking effectiveness, which will inevitably lead to email delivery latency, mail server downtime, and even a major network outage.

Trend Micro Hosted Email Security—protecting Microsoft Exchange, Microsoft Office 365, and other hosted email systems—is a no-maintenance-required solution that delivers continuously updated protection to stop spam and email-based malware before they reach your network. Moreover, Hosted Email Security customers are covered by a contractually binding Service Level Agreement (SLA). If Trend Micro doesn’t deliver, you’re eligible for your money back.

Section II.2.17 Worry-Free Business Security Services
Cloud-based security is a great choice to support your business with fast delivery, low maintenance, and—most importantly—immediate, effective protection. With security delivered from the cloud, you eliminate the cost and hassle of provisioning, managing, and scaling security hardware and software. And you ensure fast, consistent delivery of the newest security technologies and updates, helping you stay compliant and reduce risk.

Worry-Free™ Business Security Services is a hosted service that is a snap to install and easy to manage. It provides your business with industry-leading protection for your Windows, Mac, and Android devices. Now, you can manage your business devices from anywhere and always feel confident that your data is safe.

Worry-Free Business Security Services is powered by the Trend Micro Smart Protection Network™ — a worldwide early warning system that blocks threats before they can reach your business machines. Your devices will have constant access to the latest threat information.

Even security for remote workers or branch offices can be managed via the Internet with the Worry-Free Business Security Services’ web-based console. Security policy or settings can be pushed to everyone on staff, no matter where they are located. There’s no need for remote workers to be under LAN or VPN to get the latest protection policy. It also updates automatically, so there’s no need to spend time and resources on patching or updates.
Section II.2.18 Support

At Trend Micro, we live and breathe security—only security—and are 100% dedicated to making the world safe for exchanging digital information. So as the security landscape becomes more complex, our support teams become more knowledgeable and sophisticated in handling customer issues.

With Trend Micro Support, you can maximize your security stance, minimize threats, and free up your valuable IT resources for other critical functions.

Support engineers include former system administrators, network and data center engineers, and service consultants with several years of experience dealing with daily security challenges. They have deep insight and security expertise as well as access to the Trend Micro global technical ecosystem and tools that help address the range of security concerns including content, data center, and risk management.

For more information about the technical support that is available to you and to contact the Support team, refer to your Trend Micro Support welcome letter received at the time of purchase.

Section III. Architecture

Industry experts estimate that Internet access was consumerized about mid-1994. It was about this time that the proliferation of less complex, low-cost firewalls allowed companies and individuals to attach to the Internet with safety using a single-box security device based on the Windows Operating Systems. These easier-to-use, application-level firewalls didn’t require specialized IT or knowledgeable technical staff to connect, operate, and to protect their Users and Company assets from the early hazards of the Internet. It was perfectly acceptable to provide a single layer of defense for Corporate Users and Assets from the Internet.

In 1999 and 2001, application-aware malware passed the application-layer firewalls via Port 25 (SMTP/Email). In March 26, 1999, the Melissa mass mailer virus was released and was discussed in Newsgroups. On February 11, 2001, another application-aware malicious program, a worm, was propagated through SMTP.

Issues like these and other Internet activities, DDoS attacks, etc., re-enforced the concept of layered levels of defense for Corporate Users and Assets. Firewalls alone were no longer sufficient and more advanced protection for Corporate Servers, Users PCs, and other assets were required.

At this time, Trend Micro was already providing layered defense solutions having introduced LAN Server Virus Protection in 1995 and InterScan™ VirusWall (Internet Gateway Virus Protection) in 1996. Initial thoughts were to protect the desktop with Anti-Virus software, however, if 80-90% could be stopped at the gateway this would provide higher level of confidence in protecting Users and Corporate Assets.

The InterScan™ VirusWall provided protection for the four major protocols used at that time, and Mail (SMTP), Web (HTTP), POP3 (ISP Mail), and FTP (data transfer) still are the primary protocols in use today. Stopping information at the perimeter put less stress on Corporate resources, and virus and spam...
transmitted via SMTP wouldn’t be need to be backed up unnecessarily. (Remember, backup storage was costly and lower density-tape solutions were the norm— not the low-cost, high-capacity, disk storage or USB devices we use today.)

All seemed protected until the first infection occurred via the back door: an employee brought something in from home, attached to the Company network and infected the Company’s e-mail system, thus the need for another layer of protection. Trend Micro responded by introducing another layer of defense with its ScanMail™ for Microsoft Exchange Servers in 1997.

As we have seen protection was first introduced at the first point of infection, broadened out to the perimeter and then moved back into the Corporation. With this recognition, layered lines of defense became not only an option for some but also a corporate edict for all. Today, Trend Micro continues this philosophy of providing layered lines of defense, but also adds additional features with real-time updates and proactive protection with its Smart Protection Network.

The Trend Micro Smart Protection Complete products provide layered lines of defense, interconnecting with all the components of the corporate security infrastructure. Working together, they provide intelligent protection in real-time, supported by security updates provided via a cloud-based solution instead of traditional desktop pattern updates— a solution transparent to both administrators and end-users.

**Section IV. Planning Your Deployment**

This section discusses the deployment capabilities for the Trend Micro Smart Protection Complete products.

(It is beyond the scope of this document to adequately discuss actual deployment scenarios for each of the 20 products contained in Smart Protection Complete. For in-depth Deployment and Best Practices Guides please refer to the Trend Micro Smart Protection Complete Deployment Kit Getting Started Guide, Deployment Guides and Best Practices Guides in listed in Appendix III and IV respectively.)

The threat landscape has been evolving of the past few years. Where we once had a ubiquitous user operating system, Windows, mobile devices now outsell PCs and are accelerating Internet traffic. Over half of the 1 billion-plus Facebook users access and update their social networking information from their mobile devices. At the same time, new and emerging technologies like the cloud and virtualization in your data center have effectively punched a hole in your protected boundary as well, also putting sensitive information at risk.

Cyber threats are becoming increasingly more targeted and sophisticated – and are using this broader attack surface to enter your organization, further putting sensitive information at risk. Trend Micro estimates that there is one new threat created every second. The average data breach costs $3.7 million according to Netdiligence. We have found that 90% of organizations have active malware, and more than half are not aware of intrusions.
To protect from this increasingly complex threat landscape, Trend Micro’s Smart Protection Complete provides 20 solutions for multiple lines of defense. Deploying 20 products, each with its own console to administer, configure, and monitor would be daunting, but larger enterprises deploying multiple instances of the Smart Protection Complete product portfolio could be using 50 or more products; enterprises managing individual consoles is simply impractical.

This is why Trend Micro provides Control Manager, a flexible, robust, web-based enterprise management console that is an integral part of the Smart Protection Complete solution. Trend Micro Control Manager enables central threat and data loss protection policy management across Trend Micro’s Smart Protection Complete products and services at the corporate desktop, mail servers, file servers, business line of application servers, and gateway layers. Control Manager’s centralized, single monitoring focal point enables the aggregation of security content information, logs, and events from throughout the Enterprise network. Trend Micro Control Manager enables IT administrators to manage both high-level monitoring and reporting activities and low-level tasks such as managing data loss prevention templates and policies to deploying updates to the individual security products.

If even greater level of granularity and control is required, Trend Micro Control Manager allows the IT administrator to easily access to the individual product consoles. The easy access is supported by a single sign-on capability: The IT administrator only needs to sign-in once, at the Control Manager console, and the credentials will be passed to the actual product console if access to those consoles are required.

The Trend Micro Control Manager is available in two versions: Standard and Advanced. The Trend Micro Control Manager Advanced version provides for a two-tier cascading model, where multiple instances of
Control Manager are used. You would use the Advanced edition for Enterprise environments where requirements exceed the capacity of a single console, or large distributed environments that have deployed multiple Trend Micro Control Manager and have the requirement to monitor security posture in a multi-tiered environment. The upper-tiered console, referred to as the Parent, can monitor and manage downstream consoles, referred to the Child.

![Control Manager Diagram](image)

**Figure 4: Trend Micro Control Manager Parent with 2 Child Servers**

The Parent-Child relationship of Trend Micro Control Manager provides for limitless possibilities of when and how to use Trend Micro Control Manager. The following table provides guidance to consider in the design of your deployment architecture.

<table>
<thead>
<tr>
<th>Considerations</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company network and security policies</td>
<td>If company network and security policies require different access and sharing rights for grouping managed products, endpoint products, and Child servers.</td>
</tr>
<tr>
<td>Organization and function</td>
<td>Based on company’s organization and functional divisions to group managed products, endpoints, and child servers. For example, you might use separate Trend Micro Control Managers for production and for a factory floor.</td>
</tr>
<tr>
<td>Geographical location</td>
<td>Using geographical locations as criteria for grouping managed products, endpoint products, and child servers. For example, have separate Trend Micro Control Manager installations managing products local to its geography instead of having products communicate over large distances like oceans or mountainous regions that would affect communications or incur increased telecommunication over communication lines such as ISDN, etc.</td>
</tr>
<tr>
<td>Administrative responsibility</td>
<td>Based on system, IT administrator, or security personnel responsibilities. Group managed products, endpoint products, and child servers.</td>
</tr>
</tbody>
</table>

*Table 2: Considerations for Grouping Trend Micro Control Manager, Child Servers and Managed Products*
Deploying the enterprise-wide, client-server software in the Trend Micro Smart Protection portfolio and the Trend Micro Control Manager within the enterprise is not complex but requires some careful planning and assessments. (Refer to the Deployment and Best Practices in the appendix for additional considerations.) For the ease of planning, Trend Micro provides the following two basic recommendations as a starting point for deployment scenarios:

1. Single-site deployment: refers to the distribution of child Trend Micro Control Manager Child servers and its managed products from a single console located within a central office. If the Enterprise has several branch offices connected by fast, reliable, low-cost local and wide-area network connections between sites, the single-site deployment is still applicable to this environment, see Figure 6.

2. Multiple-site deployment: refers to the distribution of Trend Micro Control manager Child servers and its managed products within an Enterprise that has a main corporate office and branch offices in different geographical locations, see Figure 7.

![Figure 5: Trend Micro Control Manager Parent – 2 Child Servers and Managed Products](image)
The basic questions to be answered in the planning phase are, “How many Trend Micro Control Manager servers and managed products are required? Is cascading a requirement?” The IT administrator will need this information to decide what type of site deployment will be required and where servers should be placed within the corporate for optimum communication and management.

The follow table provides approximate Trend Micro site sizing recommendations deploying the Smart Protection Complete products. The actual number of these products and servers can be found in the Installation, Deployment, and Best Practices found in the appendices.
<table>
<thead>
<tr>
<th>Products/Endpoints</th>
<th>Small Enterprise</th>
<th>Medium Enterprise</th>
<th>Large Enterprise</th>
<th>Very Large Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoints</td>
<td>&lt; 500</td>
<td>501-2,500</td>
<td>2,501-5,000</td>
<td>&gt;5,000</td>
</tr>
<tr>
<td>TMCM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OSCE</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>-Integrated DLP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>-TMSM (Mac)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>-VDI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TMEAC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TMEE</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TMMS (Mobile)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ServerProtect (W)</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ServerProtect (L)</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>TMVP/IDF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WFBS-SVC</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TMIM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMEX</td>
<td>SMEX or SMLN</td>
<td>SMEX or SMLN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMLN</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PortalProtect</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IMSVA</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IWSVA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IWSaaS</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>HES</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Services</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 3: Smart Protection Complete Deployment Guidelines

Section V. Best Practices Considerations

This section discusses best practices considerations for the Smart Protection Complete portfolio. There are available Best Practices Deployment Guides that detail the steps, processes, and procedures (see Appendix).

The Smart Protection Complete portfolio consists of 20 solutions that address protection against the changing threat landscape and for data protection and confidentiality. What does Trend Micro recommended for deploying these 20 solutions? This section will provide guidance and why this order is the best practices for deploying the Smart Protection Complete.

It's helpful to think of enterprise security in terms of three layers of defense. The first line of defense is to protect the endpoints that surround the data at the heart of the enterprise. Stopping threats at the endpoints can prevent...
intrusion to the host. For this, we start with Trend Micro™ OfficeScan™, with its protection for physical and virtual desktops. To this, you can add additional end-point solutions, as we’ll describe shortly.

But protecting the endpoints isn’t enough. Because data moves through the layers of the enterprise system all the time, and security threats can move with them, you need the second and third layers of protection as well. The second layer of defense to deploy protects the network. Trend Micro’s solutions include Email Security™ and Secure Web Gateway™. The third layer of defense is protection of the heart of the enterprise data itself, the host. For this, Trend Micro starts with Data Loss Prevention, Application Control, and Encryption.

First Layer of Defense: the Endpoints

For the first layer defense, end-user protection starts with OfficeScan™. The modular architecture of OfficeScan™ provides the flexibility to add modules to extend your endpoint protection., For instance, Trend Micro Integrated Data Loss Protection, protects user data from being stolen on and off the network. The module protects from data-stealing malware and protects against data leaks via USB drives and other media. You can add addition client-level security with the Trend Micro intrusion Defense firewall Module.

Additionally, you should not ignore your Macs, which are no longer immune to malware, spyware, and other security threats, and can even pass along Windows malware to PCs. Trend Micro Security for Mac Module protects your Macs from these threats.

Increasingly, physical and virtual desktops aren’t the only end-points where enterprise data is used in today’s bring-your-own-device environment. When deployed with OfficeScan, Trend Micro Mobile Security™ extends your endpoint protection to iOS and Android smartphones and tablets— enabling centralized management, policy deployment, and visibility of all endpoint security through Trend Micro Control Manager™. Trend Micro Mobile Security™ integrates mobile device antimalware, mobile app management, mobile device management (MDM), and data protection to help you manage BYOD.

Trend Micro Mobile Security protects intrusion from multitude of messaging applications -- ICQ, Yahoo Messenger, Skype, Windows Live, and MSN Messenger, to name a few. And for the Enterprise standardizing on Micro Office Communicator is the Trend Micro for Instant Messaging Security™.

At the same the IT Administration is deploying endpoint protection via OfficeScan, you may want to consider Worry-Free Business Security Services™, Trend Micro's hosted service for your Windows, Mac, and Android devices that is a snap to install and easy to manage. There are three paradigms found within many enterprise companies: mergers and acquisitions within the Enterprise communities; second, downsizing within the enterprise companies and cost cutting activities reducing brick and mortar working facilities; and third, flexible working hours and environments, in essence distance workers. These three scenarios have one thing in common – workers who rarely or never come to a traditional company facility. And in most cases VPN technologies were used to allow distance work to access
company resources such as e-mail. However, with recent enhancement with Microsoft Exchange most enterprises have replaced VPN access with HTTP/s capabilities.

When endpoint protection was deployed on the distance work, in a lot of cases, getting logs and status information and sending configuration information to the endpoint was difficult. **Worry-Free Business Security Services solves** these problems by having the endpoints communicate with a cloud-based server for both sending logs and status information. And at the same time, obtain configuration information in real-time.

Another risk involves the users themselves. You also risk losing private company data that resides on the machines of users who may be doing things they shouldn’t be doing. **Trend Micro Endpoint Application Control** prevents unwanted and unknown applications and malware from executing on your corporate endpoints. **Endpoint Application Control** uses flexible, easily managed policies, whitelisting and blacklisting capabilities, as well as a global, cloud-powered application database.

In the Enterprise, there is also a need for data integrity and confidentiality to keep information secure, an issue that is further amplified as more and more employees bring their own computing devices to work in the name of productivity. Ensuring that sensitive data is secured in the case of device loss has never been more difficult. **Trend Micro Endpoint Encryption** encrypts data on a wide range of devices—PC and Macintosh laptops, desktops, CDs, DVDs, USB drives and any other removable media. This solution combines enterprise-wide full disk, file/folder, and removable media encryption with granular port and device control to prevent unauthorized access and use of private information.

**Second Layer of Defense: the Network**

The next layer of defense is at the network. Industry analysts have indicated over the years that users spend 70-80% of the time accessing e-mail and web-based activities. To protect this information Trend Micro has e-mail and web protection solutions, **ScanMail** and **Secure Web Services**.

**Trend Micro offers ScanMail** solutions for Microsoft Exchange™ and for IBM Lotus/Domino Server™. In addition, to reduce the junk that reaches messaging services Trend Micro recommends putting protection at the perimeter. A perimeter-based solution can eliminate 70-80% of the junk and malicious content by a gateway or cloud-based solution. Trend Micro solutions for e-mail gateway and cloud-based are **Trend Micro InterScan Message Security Virtual Appliance** and its **Trend Micro Hosted E-mail Services**. Similarly, for web or HTTP activities are the web gateway solutions, **Trend Micro InterScan Web Security Virtual Appliance** and **Trend Micro InterScan Web Security** offered as services.

**Third Layer of Defense: The Host**

The inner layer of defense protects is at the host from threats that get through (or past) the first two lines of defense. Host data includes the information located on file servers and enterprise applications such as Microsoft Sharepoint. For these environments Trend Micro's solutions include **Trend Micro ServerProtect** for Windows and Linux and **Trend Micro PortalPortect Security** for Microsoft Sharepoint servers. These solutions provide comprehensive real-time protection for enterprise web-servers and file-
servers, preventing them from spreading viruses, spyware, and other Web threats to internal or external endpoints. The final solution within the Smart Protection Complete portfolio is to deploy **Trend Micro Control Manager** to provide IT administrators with the centralized ability to monitor and manage the security posture as well as the centralized ability to administer and configure the complete set of Trend Micro solutions.

**Deploying Extra Protection for Data Integrity and Confidentiality**

Organizations with higher security needs, such as government agencies, the military, or groups working with highly proprietary information may require additional protection. In addition to Smart Protection Complete, you can add **Trend Micro™ Enterprise Data Protection** for insuring data integrity and confidentiality. Enterprise Data Protection includes products with flexible deployment options to fit your security needs:

1. Trend Micro™ Integrated Data Loss Prevention
2. Trend Micro™ Endpoint Encryption
3. Trend Micro™ Email Encryption Gateway

**Trend Micro™ Integrated Data Loss Prevention** software provides a network and endpoint solution combined with a workflow-navigation engine to easily identify, track, and secure your business-critical data from gateway to endpoint. Optional modules integrate with OfficeScan, InterScan Messaging Security, InterScan Web Security, ScanMail, and PortalProtect to instantly extend data protection throughout your network.

Government agencies and military sometimes require encryption of data on the user's computers. **Trend Micro™ Endpoint Encryption** encrypts data stored on computers, including PCs, laptops, and notebooks, as well as on removable media, including CDs, DVDs, and USB drives. **Trend Micro™ Endpoint Encryption** allows for full disk encryption, or encryptions of individual folders and files encryption, as well as granular device control, data management, and key management.

For organizations that require secure email communications, **Trend Micro™ Email Encryption Gateway** automates policy-based email encryption for data protection that doesn’t rely on end user discretion. You can avoid the headaches of key management with our hosted key service and eliminate the need for recipients to install client software.

**Section V.1 Deploying Multiple Applications**

Within the Smart Protection Complete Suite there are 14 on-premise applications. The following questions arise:

1. Does the IT administrator need 14 separate systems for deployment?
2. Can multiple applications be installed together?
3. If no, which ones cannot be combined?
4. What is the recommended system sizing?
Refer to the Performance and Sizing Guide for the individual products. At the time of this writing Trend Micro is in the process of characterizing multiple application deployment and it should be available in 2014 Q4. However, until the documents are available the following guidelines can be used.

The following products can be installed in any combination. It is recommend that a minimum of 3-4 products maximum be installed on the same bare metal or virtualized.

Control Manager – in large-scale deployment it is recommended that Control Manage be installed on a separate server and with its database on a separate system.

OfficeScan – in large-scale deployment it is recommended that it be installed with only two other applications and its performance rating is reduced by 50%. For example, the maximum number of clients supported by OfficeScan 11.0 is 50,000 endpoints. If you decide to deploy with additional applications the recommended endpoints supported be reduced by 50% or 25,000 endpoints.

The following product, excluding installation with OfficeScan, can support any combination with a recommended limit of 4 applications.

1. Application Control
2. Endpoint Encryption
3. Mobile Security
4. Vulnerability Protection (formally named as IDF)
5. Instant Messaging Security
6. PortalProtect Security
7. ServerProtect for Windows

ServerProtect for Linux

For the messaging products, in large-scale deployment, it is recommended they be installed on dedicated servers. Performance numbers for Exchange 2010 indicated that its performance is greater virtualized than on bare metal. However, if virtualized it is recommended that the other virtual environments be DHCP, WINS, and/or DNS servers.

1. ScanMail for Microsoft Exchange
2. ScanMail for IBM Lotus Domino that they be install

For gateway products such as e-mail and web applications for small and medium size deployment they can be installed on the same servers or virtualized. However, for large-scale deployment it is recommended that these applications be installed on dedicated servers immediate behind the firewall or other perimeter applications.

Section VI. Licensing

The New Trend Micro Customer Licensing Portal (CLP) helps administrators manage accounts, customer information, and subscriptions, seat count, deployment packages, downloads, and many more
administrative features. In addition, from the Customer License Portal administrator can directly access the web consoles for Trend Micro solutions that you manage, including on-premise and cloud-base Services.

Traditionally Trend Micro uses the Online Registration System that allows Enterprise and Small/Medium Business customers register, activate, renew, or merge multiple licenses for their Products and Services. With the introduction of the Complete User Protection initiative Trend Micro will introduce a more robust application called Customer Licensing Portal. The following table outlines the differences between Online Registration System and Customer Licensing Portal.

Table 4 summarizes the benefits of the New Trend Micro Customer Licensing Portal and illustrates the difference between the traditional Trend Micro Online Registration System.

<table>
<thead>
<tr>
<th></th>
<th>Online Registration System</th>
<th>Customer License Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Activation Codes</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Renewal</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>License Merging</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Account Information</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Account Manager</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Manage Customers</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Subscriptions Types</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Deployment Packages</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manage Downloads</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Seat Count Management</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 4: Online Registration System vs. Customer Licensing Portal
Appendix I. Smart Protection Complete Acronyms

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Manager</td>
<td>TMCM</td>
</tr>
<tr>
<td>OfficeScan</td>
<td>OSCE</td>
</tr>
<tr>
<td>-Integrated Data Loss Prevention</td>
<td>iDLP</td>
</tr>
<tr>
<td>-Mac Security</td>
<td>TMSM (Mac)</td>
</tr>
<tr>
<td>-Virtual Desktop Infrastructure</td>
<td>VDI</td>
</tr>
<tr>
<td>Application Control</td>
<td>TMEAC</td>
</tr>
<tr>
<td>Endpoint Encryption</td>
<td>TMEE</td>
</tr>
<tr>
<td>Trend Micro Mobile Security</td>
<td>TMMS (Mobile)</td>
</tr>
<tr>
<td>ServerProtect for Windows</td>
<td>ServerProtect (W)</td>
</tr>
<tr>
<td>ServerProtect for Linux</td>
<td>ServerProtect (L)</td>
</tr>
<tr>
<td>Vulnerability Protection (formally named as IDF)</td>
<td>TMVP/IDF</td>
</tr>
<tr>
<td>Worry-Free Business Security Services</td>
<td>WFBS-SVC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trend Micro Smart Protection Complete – Additional Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Messaging Security</td>
</tr>
<tr>
<td>ScanMail for Microsoft Exchange</td>
</tr>
<tr>
<td>ScanMail for IBM Lotus Domino</td>
</tr>
<tr>
<td>PortalProtect Security</td>
</tr>
<tr>
<td>InterScan Messaging Security Virtual Appliance</td>
</tr>
<tr>
<td>InterScan Web Security Virtual Appliance</td>
</tr>
<tr>
<td>InterScan Web Security as a Services</td>
</tr>
<tr>
<td>Hosted Email Services</td>
</tr>
<tr>
<td>Services</td>
</tr>
</tbody>
</table>

Table 5: Product Portfolio

For additional understand on the New Trend Micro Customer Licensing Portal the reader can refer to the following information:

Appendix II, in this document, Licensing Information Product


( http://docs.trendmicro.com/all/smb/clp/vALL/en-us/clp_ug.pdf )

Trend Micro Customer Licensing Portal Online Help

( http://docs.trendmicro.com/all/smb/clp/vALL/en-us/clp_olh/intro_text.html )
Appendix II. Licensing Information Product

Appendix II.1 New Users
Trend Micro, existing and New, Customers can use the Trend Micro Customer Licensing Portal to manage their Trend Micro Security applications. For New Customers an account needs to be created. Select the corresponding status and follow the wizard.

Figure 9: Existing or New User
Appendix II.2 Account Registration Form

Fill out the form to register your products or services

Are you a reseller acting on behalf of a customer?
- Yes
- No

Account Profile
- Account ID:
  Use 4 to 25 alphanumeric characters, underscore, or hyphens.
- Password:
  Use 4 to 25 characters.
- Confirm password:
- Time zone: (UTC-08:00) Pacific Time (US & Canada)
- Language: English - United States (English - United States)

Primary Contact
- Company name:
- Contact person:
  - First name
  - Last name
- Email address:
- Contact number:
  - Area code
  - Number
  - Extension
- Address:
- Postal code/city:
- State/province:
- Country: United States
  - Send email notification before product maintenance expires
  - Add a secondary contact

Figure 10: Account registration form

Need to have an example of what the deployment package looks like with the binaries and Activation code.
Appendix II.3 Existing Customers Account

When existing Trend Micro Customers log into the Trend Micro Customer License Portal, they can see the Products, Services, and Licensing information in one centralized console, as shown in the figure below.

Customer can see the status of the Trend Micro Security application and determine what products have been deployed. The Trend Micro Customer Licensing has two additional features for IT administrators. There are selections that allow IT administrators to either Deploy (download and deploy) or just to Download Only the Trend Micro Security applications. The deployment packages are fully self-contained with binaries and access to associated activation keys.

The Deploy feature allows IT administrators, from the server of interest, to log into the Trend Micro Customer Licensing Portal to select and deploy the Security application.

The Download Only feature allows IT administrators to download the installation package and then transfer this information to the server of interest.

![Customer Licensing Portal](image)

Figure 11: Customer Licensing Portal
Appendix II.4 Creating the Deployment Kit

From the Trend Micro Customer Licensing Portal the IT administrator selects the product and/or products to install. Once the selection has been made the “Get Deployment Kit” will be enabled.

The deployment kit or package will automatically generate with the necessary binaries and activation codes:
Appendix II.5 Accessing the Activation Keys

One of the most difficult tasks for the IT administrators is managing the activation keys for products. The Trend Micro Customer Licensing Portal easily assists in this task. The IT administrator can access the activation key(s) from the Trend Micro Customer Licensing Portal or a screen will allow them to access the activation key during installation.
Appendix II.5 Issues during Installation Time

What happens if the IT administrator has issues during product installation time? For example, if the system of interest does not meet the minimum system requirements. The Deployment Kit will manage these and other installation issues with user-friendly messages and links on where to get immediate assistance.
Each time the Trend Micro™ Smart Protection Deployment Kit attempts to download, install, and launch an on-premise product, it checks a set of rules.

The Smart Protection Deployment Kit may interrupt the download, installation, or deployment of a product when a rule check returns information about:

- Product installation issues (see Product Installation Issues)
- Unmet component requirements (see Software Dependencies)
- Product incompatibilities or server resource conflicts (see Product Exclusions)

Figure 16: Troubleshooting during Product Deployment
Appendix III. List of Smart Protection Complete Deployment Guides

Control Manager

OfficeScan
- Integrated Data Loss Prevention
- Mac Security
- Virtual Desktop Infrastructure

Application Control

Endpoint Encryption

Mobile Security

ServerProtect for Windows

ServerProtect for Linux

Vulnerability Protection (formally named as IDF)

Worry-Free Business Security Services

Instant Messaging Security

ScanMail for Microsoft Exchange

ScanMail for IBM Lotus Domino

PortalProtect Security

InterScan Messaging Security Virtual Appliance

InterScan Web Security Virtual Appliance

InterScan Web Security as a Service

Hosted Email Services
Appendix IV. List of Smart Protection Complete Best Practices

Control Manager

OfficeScan

- Integrated Data Loss Prevention

- Mac Security

- Virtual Desktop Infrastructure

Application Control

Endpoint Encryption

Mobile Security

ServerProtect for Windows

ServerProtect for Linux

Vulnerability Protection (formally named as IDF)

Worry-Free Business Security Services

Instant Messaging Security

ScanMail for Microsoft Exchange

ScanMail for IBM Lotus Domino

PortalProtect Security

InterScan Messaging Security Virtual Appliance

InterScan Web Security Virtual Appliance

InterScan Web Security as a Service

Hosted Email Services
Appendix V. References

This will be the placeholder for the references to the official Best Practices and Sizing Guides.

Appendix VI: Product Matrix Features

| Features | Control Manager | ServerProtect for Web | ServerProtect for Linux | ServerProtect for RACF | ServerProtect for CICS | ServerProtect for IMS | Security for Mac | Endpoint Application Control | Endpoint Encryption | Mobile Security | iDLP | ScanMail for Exchange | ScanMail for IBM Domino | PortalProtect Security | iM Security | IMSVA | HES | IWSVA | IWSaaS |
|----------|----------------|-----------------------|-------------------------|-------------------------|-------------------------|-----------------------|----------------|--------------------------------|-----------------|----------------|------|----------------------|----------------------|---------------------|-------------|-------|-----|-------|
| Centralized Updates | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Comprehensive Logs | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Authentication | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Device management | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Central administration | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Behavior Monitoring | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| White Listing | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Firewall Security | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Security Risk Protection | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Active Directory Integration | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| URL Filtering | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Digital Assets Protection | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Server Protection | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| XML and Anti-Rootkit module | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Intrusion Prevention | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Hyper-V Installation Support | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Real-Time Statistics and Alerts | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Enhanced Web Reputation | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Smart Scan | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Encryption | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Android Protection | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| IDS Protection | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| FTP Scanning | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Content Caching | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Policy for File Movement | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Enforce rules and standards | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Application Control | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Email Security | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Spam Prevention | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Advanced Threat Scan Engine | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |

Table 6: Product Matrix Features