

**ESCOLA SUPERIOR ABERTA DO BRASIL – ESAB
CURSO DE PÓS-GRADUAÇÃO LATO SENSU EM
REDES DE COMPUTADORES**

ROBSON LUIZ RAMOS

SYMANTEC ENDPOINT PROTECTION EM REDE WINDOWS

**LONDRINA - PR
2010**

ROBSON LUIZ RAMOS

SYMANTEC ENDPOINT PROTECTION EM REDE WINDOWS

Monografia apresentada ao Curso de Pós Graduação *latu sensu* em Redes de Computadores da Escola Superior Aberta do Brasil como requisito parcial para a obtenção do título de Especialista em Redes de Computadores, sob orientação do Prof. Marcos Alexandre do Amaral Ramos.

**LONDRINA - PR
2010**

ROBSON LUIZ RAMOS

SYMANTEC ENDPOINT PROTECTION EM REDE WINDOWS

Monografia aprovada em ____ de _____ de 2010.

Banca Examinadora

**LONDRINA - PR
2010**

*À Sílvia, minha esposa. À Amanda
e à Daniela, minhas filhas.*

Agradeço aos professores e trabalhadores da Esab pela atenção que me dispensaram durante todo este curso de especialização.

RESUMO

Palavras-chave: Antivirus. Endpoint. Rede.

O presente trabalho acadêmico decorreu de pesquisa exploratória, por meio de estudo de caso, com o objetivo de identificar o modo de implementação do antivírus Symantec Endpoint Protection gerenciado em rede de computadores com sistemas operacionais Microsoft Windows. Especificamente, o estudo abordou a implementação do referido antivírus em rede, a utilização dos seus principais recursos e a identificação de suas principais características capazes de minimizar a inexperiência dos usuários da rede. O estudo partiu da descrição física da rede e do perfil dos usuários, cujas características contribuem para a disseminação de vírus, em face do perigo real que usuários despreparados representam para a rede e, conseqüentemente, para a instituição, devido à potencialidade que os próprios trabalhadores têm para, inadvertidamente, introduzir algum tipo de vírus na rede, de forma a comprometer a segurança e a integridade dos dados. O Estudo abordou, também, os passos para a instalação, a qual se verificou possível de ser realizada remotamente, de forma imperceptível aos usuários. Por fim, este trabalho explorou detalhes dos recursos do Endpoint, com ênfase ao gerenciamento remoto, cuja utilização se revelou num importante aliado ao combate às pragas virtuais, com desempenho altamente satisfatório.

SUMÁRIO

INTRODUÇÃO	7
CAPÍTULO 1 – FUNDAMENTAÇÃO TEÓRICA	10
CAPÍTULO 2 – CARACTERÍSTICAS DA REDE E DOS USUÁRIOS	13
2.1 A REDE	13
2.2 OS USUÁRIOS	16
CAPÍTULO 3 – SOLUÇÃO SYMANTEC PARA REDE WINDOWS	20
3.1 A LICENÇA DE USO	20
3.2 SOFTWARE E DOCUMENTAÇÃO	24
CAPÍTULO 4 – INSTALAÇÃO DO ENDPOINT EM REDE WINDOWS	26
4.1 REQUISITOS MÍNIMOS PARA INSTALAÇÃO	26
4.2 INSTALAÇÃO DO CONSOLE DE GERENCIAMENTO	27
4.3 INSTALAÇÃO DOS CLIENTES GERENCIADOS	34
CAPÍTULO 5 – OS RECURSOS DO ENDPOINT PROTECTION	41
5.1 RECURSOS DE GERENCIAMENTO	41
5.1.1 O Console de Gerenciamento	41
5.1.2 Página Início	42
5.1.3 Página Monitores	44
5.1.4 Página Relatórios	45
5.1.5 Página Políticas	45
5.1.6 Página Clientes	46
5.1.7 Página Admin	47
5.2 RECURSOS DO SOFTWARE CLIENTE	47
5.2.1 Auto-Protect	47
5.2.2 Proteção antivírus e anti-spyware	48
5.2.3 Proteção contra ameaças à rede	49
5.2.4 Proteção proativa contra ameaças	49
5.2.5 Ícone da Área de Notificação	50
5.3 OUTROS RECURSOS	50
5.3.1 Quarentena Central	51
5.3.2 Servidor Live Update	54
CONCLUSÃO	56
REFERÊNCIAS	58

INTRODUÇÃO

O assunto da presente pesquisa é o combate ao vírus de computador em um ambiente de rede específico, localizado na Câmara Municipal de Londrina, por meio da utilização de recursos e ferramentas disponíveis no mercado, tais como o ambiente de rede Windows e a solução Symantec – o Symantec Endpoint Protection – para combate a vírus de computador e outros *malwares*¹. Assim, o fenômeno que enseja a presente pesquisa é a necessidade de se implementar um meio de combater satisfatoriamente os ataques de vírus na rede de computadores de uma instituição que possui características específicas, em face da heterogeneidade dos usuários decorrente da politização da mão-de-obra, fenômeno natural em um legislativo, onde os usuários, em sua maioria, possuem pouco ou quase nenhum conhecimento técnico em informática, mas exigem a disponibilização de ferramentas com potencialidade para introduzir vírus na rede.

O problema da pesquisa traduz-se pela pergunta: como implementar a solução Symantec Endpoint Protection para defesa contra ataques de vírus na rede de computadores com sistemas operacionais Microsoft Windows? Ou seja, é a necessidade de se buscar o conhecimento e a cultura necessários à implantação da ferramenta escolhida pela Câmara, dentre os disponíveis no mercado, como solução para o combate aos ataques de vírus, de forma a utilizar o máximo possível dos recursos, vantagens e facilidades da referida ferramenta.

Justifica-se a escolha do tema porque, embora os manuais tragam orientações gerais e específicas para a implementação do Symantec Endpoint Protection, considera-se interessante e valioso uma abordagem acadêmica, com o intuito de detalhar os passos para a implementação e os recursos disponíveis na ferramenta, sob um método de pesquisa válido.

¹ Utilizar-se-á ao do texto o termo genérico “vírus” para se referir a todos os tipos conhecidos de praga virtual que afete de qualquer forma o funcionamento do computador e a segurança da rede.

O objetivo geral é identificar o modo de implementação da solução Symantec Endpoint Protection em rede de computadores corporativa, com sistemas operacionais Microsoft Windows, para defesa contra ataques de vírus.

Os objetivos específicos são: descobrir como implementar a solução antivírus, com impacto mínimo aos usuários; descobrir como utilizar os principais recursos disponibilizados pelo Symantec Endpoint Protection dentro de uma rede gerenciada por sistema operacional Microsoft Windows; e identificar as principais características do produto Symantec Endpoint Protection capazes de minimizar a inexperience dos usuários da rede.

O trabalho é delimitado ao estudo do Symantec Endpoint Protection em ambiente de rede Windows, com destaques para a implantação, a utilização dos recursos de gerenciamento em rede e a identificação dos recursos capazes de minimizar alguma deficiência técnica dos usuários de rede. Vale anotar que alguns recursos do Symantec Endpoint Protection são mencionados no item 5.3, mas não serão detalhados na presente pesquisa pelo fato não terem sido utilizados nem testados da rede da Câmara.

O método utilizado é a pesquisa do tipo exploratória, com realização de estudo de caso na Câmara Municipal de Londrina e revisão bibliográfica. A coleta de dados se dará por meio de verificação das características da rede, da instalação prática do Symantec Endpoint Protection e das características do sistema instalado. Os dados serão analisados em face do comportamento do ambiente de rede diante da solução Symantec e apresentados em textos ou imagens capturadas durante a instalação e/ou utilização do sistema.

Como a presente pesquisa tem por método o estudo de caso em rede de computadores existentes na Câmara Municipal de Londrina, esta Instituição se citada várias vezes ao longo do texto e poderá, por vezes, ser referida apenas por Câmara, Câmara Municipal ou, ainda, Câmara de Londrina. Também por mera conveniência dissertativa, o Symantec Endpoint Protection será referido apenas por Endpoint, Endpoint Protection ou Symantec Endpoint.

O texto está estruturado de forma a descobrir as principais características da rede, dos usuários e do software Symantec Endpoint Protection, partindo-se da análise de alguns conceitos já sedimentados em literatura, como fundamentação teórica, até chegar aos recursos do referido software, passando por tópicos como a licença de uso, instalações e recursos nele disponíveis.

Ao final, na conclusão, tem-se um resumo acerca dos objetivos buscados com o presente estudo e as impressões práticas com o Endpoint, como consecução de tais objetivos.

CAPÍTULO 1 – FUNDAMENTAÇÃO TEÓRICA

Tanenbaum² alerta para o perigo que usuários despreparados representam para a Rede e, conseqüentemente, para a instituição, chamando atenção, em especial, para a potencialidade que os próprios trabalhadores têm para, inadvertidamente, introduzir algum tipo de vírus na rede, de forma a comprometer a segurança e a integridade dos dados.

Essa é a razão pela qual se preocupou, antes de adentrar no estudo do Endpoint propriamente dito, em descrever as características dos usuários da rede existentes na Câmara, pois, como se verá no capítulo 2, tais usuários possuem algumas características específicas, as quais se transformam em multiplicador de riscos para contaminação por vírus.

Tanenbaum³ também oferece uma ótima definição de vírus de computador, além de conceitos genéricos de redes e componentes de rede de computadores, os quais serão referenciados em especial no capítulo 2, onde, além das características dos usuários já citadas, se descreverá as principais características

² “A capacidade de conectar qualquer computador em qualquer lugar a qualquer outro computador em qualquer lugar é uma faca de dois gumes. É muito divertido para as pessoas navegarem pela Internet quando estão em casa. Para os gerentes de segurança das empresas, trata-se de um pesadelo. Muitas empresas têm grandes quantidades de informações confidenciais on-line – segredos comerciais, planos de desenvolvimento de produtos, estratégias de marketing, análises financeiras etc. A revelação dessas informações para um concorrente poderia ter terríveis conseqüências. Além do perigo das informações virem a público, também há o perigo do vazamento dessas informações dentro da empresa. Em particular, vírus, vermes e outras pestes digitais podem burlar a segurança, destruir dados valiosos e consumir muito tempo dos administradores, que tentam eliminar a confusão causada por eles. Com freqüência, eles são trazidos por funcionários descuidados que querem brincar com algum jogo novo muito divertido”. in TANENBAUM, Andrews. **Redes de computadores**. Rio de Janeiro: Campus, 2003, p. 358.

³ “Os vírus são outra forma de código móvel. Porém, diferentes dos exemplos anteriores, os vírus sempre chegam sem ser convidados. A diferença entre um vírus e o código móvel comum é que os vírus são desenvolvidos para se reproduzir. Quando um vírus chega, seja através de uma página da Web, em um anexo de correio eletrônico ou de algum outro modo, em geral ele começa infectando programas executáveis no disco. Quando um desses programas é executado, o controle é transferido para o vírus que, em geral, tenta se difundir para outras máquinas, por exemplo, enviando cópias de si mesmo por correio eletrônico para todas as pessoas que têm seus nomes no catálogo de endereços da vítima. Alguns vírus infectam o setor de inicialização do disco rígido; assim, quando a máquina é inicializada, o vírus é executado. Os vírus se tornaram um problema enorme na Internet e causam prejuízos de bilhões de dólares. Não existe nenhuma solução óbvia. Talvez uma nova geração de sistemas operacionais, inteiramente baseada em microkernels seguros e rígida divisão dos usuários, processos e recursos em compartimentos estanques possa ajudar a resolver o problema”. In TANENBAUM. Idem, p. 1430.

da rede da Câmara, usando-se termos específicos que suscitam alguma referência conceitual.

Ainda no capítulo 2, serão referenciadas as anotações feitas por Minasi, Anderson, Smith e Toobs⁴, quando mencionado algum recurso do Windows 2000 Server, que é o sistema operacional do Servidor de Rede onde se instalou o Endpoint.

Reportando-se estritamente aos objetivos específicos desta pesquisa, além dos autores acima citados, transitar-se-á, primordialmente, por manuais técnicos do Endpoint, os quais servem de base ao presente estudo de caso. São eles: o Manual de Introdução⁵, o Guia de Instalação⁶, o Guia de Administração⁷, o Guia do Cliente⁸ e o Guia de Implementação da Central de Quarentena⁹, todos eles editados pela Symantec.

O Manual de introdução do Endpoint identifica o produto, com as informações iniciais, especialmente quanto à Licença de Uso e de como obter o software e documentação, que é o assunto tratado no capítulo 3.

O Guia de Instalação será referenciado no capítulo 4, que trata das instalações dos componentes do Symantec Endpoint Protection, o Servidor de Gerenciamento e software-cliente, além de identificar os requisitos mínimos para as instalações.

O Guia de Administração, o Guia do Cliente e o Guia de Implementação da Central de Quarentena serão referenciados no capítulo 5, onde são identificados

⁴ MINASI, Mark; ANDERSON, Christa; SMITH, Brian; TOOMBS, Doug. **Dominando o Microsoft Windows 2000 Server**. São Paulo: Person Education, 2001.

⁵ SYMANTEC. **Introdução ao Symantec Endpoint Protection**. Cupertino: Symantec, 2009.

⁶ SYMANTEC. **Guia de Instalação do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009.

⁷ SYMANTEC. **Guia de Administração do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009.

⁸ SYMANTEC. **Guia do Cliente do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009.

⁹ SYMANTEC. **Guia de Implementação do Symantec Central Quarantine**. Cupertino: Symantec, 2009.

os recursos do Endpoint disponíveis ao administrador e ao usuário do computador cliente, como, por exemplo, o Console de Gerenciamento, Auto-Protect e a Central de Quarentena. Ao final do capítulo 5 serão referenciados os manuais de instalação ¹⁰ e de administração ¹¹ do Live Update, também editados pela Symantec.

¹⁰ SYMANTEC. **Symantec LiveUpdate Administrator 2.2 Getting Started Guide**. Cupertino: Symantec, 2009.

¹¹ SYMANTEC. **Symantec LiveUpdate Administrator 2.2 User's Guide**. Cupertino: Symantec, 2009.

CAPÍTULO 2 – CARACTERÍSTICAS DA REDE E DOS USUÁRIOS

Algumas características da rede e dos usuários são importantes para entender a razão da opção pelo produto Symantec, razão pela qual faz-se uma análise um pouco mais detida neste particular.

2.1 A REDE

A rede de computadores em questão, que serviu de modelo para análise prática da presente pesquisa é a rede de computadores da Câmara Municipal de Londrina, de topologia estrela, composta por microcomputadores que trabalham tanto em rede como independente dela, que segue o modelo Cliente-servidor, descrito por Tanenbaum¹², ou seja, uma típica rede corporativa de médio porte.

Os adaptadores de rede e os swichs são ethernet gigabit conectados por cabeamento estruturado em par trançado simples¹³, categoria seis.

Os servidores de rede estão alocados em sala específica que possui ambiente climatizado automaticamente, sistema de alarme contra incêndio e segurança predial de 24 horas por dia.

Os armários de telecomunicação estão instalados em duas salas individualizadas, em locais estratégicos, em ambos os lados do edifício, de forma a diminuir o comprimento dos cabos da rede secundária.

São sete os microcomputadores que compõem a rede primária, todos com configuração de servidor de rede, com quatro processadores e dedicação exclusiva, sendo: servidor de e-mail; proxie para a primeira conexão externa com

¹² TANENBAUM, op. cit., p. 6.

¹³ “as vantagens do cabeamento 10Base-T eram tão grandes que o Fast Ethernet se baseou inteiramente nesse projeto. Por isso, todos os sistemas Fast Ethernet usam hubs e switches”. In TANENBAUM. Idem, p. 508.

a internet; DHCP e proxie para a segunda conexão externa com a internet; servidor de arquivos; servidor de DNS, gateway e banco de dados; servidor de Backup; e servidor de páginas e arquivos do site da Câmara que utiliza o Microsoft Internet Information Service.

O servidor de e-mail utiliza sistema operacional Linux Mandriva e, por opção técnica, possui controle de usuários independente do domínio Windows, de forma a possibilitar a utilização do webmail pela internet fora das dependências da Câmara.

Uma vez que a Câmara transmite as sessões plenárias *on line* pela internet, existiu a preocupação de segurança, de sorte que se optou por possuir duas conexões externas com a internet, razão pela qual também são dois os servidores proxies, ambos com configuração idêntica, com sistema operacional Linux Ubuntu, sendo que um deles é também servidor DHCP, muito embora o outro possa assumir também a função DHCP, sendo, pois, backup para essa função. Num deles também está conectado o ponto de acesso para conexão de rede sem fio, aberta ao público externo somente para acesso à internet.

O servidor de arquivos, com sistema operacional Linux Mandriva, utiliza a autenticação dos usuários do domínio¹⁴ Windows, acessando o Active Directory por meio da conexão Samba, de forma que os usuários têm acesso em ambiente Windows aos arquivos armazenados em ambiente Linux.

O três últimos servidores de rede ora descrita utilizam sistema operacional Windows 2000 Server, atualizados até o Service Pack 4.

Dois deles estão configurados para serem servidores de Banco de dados e do domínio Windows, com o Active Directory replicado, embora um deles possua capacidade muito superior de armazenamento em discos rígidos em RAID e esteja instalado em sala isolada, noutro extremo do edifício, para servir de backup

diário das funções e arquivos de todos os demais servidores de rede, de sorte que ele, em caso de emergência, pode assumir sozinho, sem solução de continuidade, todas as funções atribuídas aos demais servidores de rede.

O terceiro servidor de rede Windows não é controlador de domínio, contém as páginas e arquivos do site da Câmara e é o que nos interessa em especial, pois nele foi instalado o gerenciador dos Symantec Endpoint Protection e é de onde se coletou a maioria dos dados para o presente estudo. Este servidor foi escolhido, em especial, porque já conta com o Microsoft Internet Information Services¹⁵, o IIS, que é um requisito para a instalação Console de Gerenciamento do Symantec Endpoint Protection.

A rede secundária é composta por 122 computadores *desktop*, todos conectados via *switch*, de forma que existem conjuntos de computadores que formam sub-redes e trocam informações cliente-servidor, entre si, conforme as diversas necessidades dos usuários.

A maioria dos computadores que formam a rede secundária, aproximadamente dois terços, utiliza sistema operacional Windows Vista e o restante Windows XP.

Os computadores com sistema operacional Windows 1998 foram removidos da rede por ocasião da instalação do sistema de antivírus por não serem compatíveis com o Symantec Endpoint, o que contribui para a segurança da rede, uma vez que o Windows 1998 não dispõe de recursos de segurança como o Windows Vista e o Windows XP.

Embora a rede ora estudada possua plataforma lógica dupla, não existiu maior preocupação com relação ao sistema operacional Linux, naquilo que diz respeito

¹⁴ “O grupo de máquinas que faz referência a um conjunto de controladores de domínios para autenticação é chamado coletivamente de *domínio*”. In MINASI, Mark; ANDERSON, Christa; SMITH, Brian; TOOMBS, Doug. Op. Cit., p. 44.

¹⁵ “O Internet Information Services é uma plataforma completa capaz de fornecer as tarefas HTTP (Web), FTP (transferência de arquivos), NNTP (grupos de notícias) e SMTP (e-mail) para uma organização”. In MINASI, Mark; ANDERSON, Christa; SMITH, Brian; TOOMBS, Doug. Op. Cit., p. 936.

à contaminação por vírus de computador, porque estão instalados em servidores dedicados, com acesso restrito aos administradores de rede e, embora utilizem programa de antivírus gratuitos, nunca foram contaminados por vírus em vários anos.

Por outro lado, os computadores com sistema operacional Windows, devido a sua aceitação no mercado mundial, suscita uma preocupação acima da média para os técnicos de informática e para a Administração como um todo, pois os ataques por vírus são diários, e a falta de preparo no combate a essa praga digital causa transtornos de toda ordem, além de grande prejuízo ao erário.

Existe a disposição dos técnicos para migrar todos os sistemas operacionais para Linux, mas, em que pese as adaptações técnicas possam ser implantadas sem muita dificuldade, existe uma grande resistência para mudanças entre os usuários, o que levou à busca por novas soluções no combate a vírus de computadores numa rede Windows.

2.2 OS USUÁRIOS

A rede de computadores da Câmara tem sofrido constantes ataques de vírus ao longo dos anos devido a vários fatores como, por exemplo, a resistência administrativa em adquirir programas de antivírus e o acesso ilimitado aos recursos da rede por usuários despreparados.

Uma Câmara Municipal de porte razoável, como é o caso de Londrina, possui um quadro de servidores e agentes políticos que possuem perfis profissionais extremamente heterogêneos em vários aspectos, em especial, o relacionado com o conhecimento básico de informática, no que diz respeito à segurança da rede contra ataques de vírus de computador.

Os agentes políticos, os vereadores, não raro exibem um perfil exigente em direitos e pouco afeito ao cumprimento de obrigações legais, visto que exercem

um cargo público revestido de relativa autoridade, que faz surgir a idéia de serem uma espécie de diretores imunes ao balizamento técnico.

Assim, não é difícil de imaginar a diversidade de direcionamentos que a Administração toma em relação à informática, como um todo, até que se chegue a um denominador comum que atenda a um requisito mínimo de segurança de rede.

É comum o conflito entre vereadores e servidores efetivos do Departamento de Informática quando assunto se refere ao tipo de serviço, instalação e disponibilidade que são possíveis em equipamentos e rede de computadores da instituição, bem como é muito difícil traçar a linha que separa o interesse da Câmara do interesse privado do vereador que, não raro, pleiteia a disponibilização de recursos lógicos que não estão disponíveis, a não ser por meio de pirataria de software, os quais, obviamente, não podem ser utilizados pela Câmara nem adquiridos oficialmente, por não se justificar o interesse público na sua aquisição.

Limitar o acesso dos vereadores a todos os recursos do sistema operacional tem se revelado uma tarefa muito difícil de ser executada sem uma boa quantidade de confrontos, os quais, infelizmente, acabam por se resolver de forma menos técnica do que politicamente.

Na Câmara existe outra espécie de usuário de rede que são os servidores em cargos de comissão, que assessoram algum vereador, os quais entram no serviço público não pela formação escolar, capacidade e conhecimento técnico, mas pela vontade pura e simples do vereador, sob as mais diversas justificativas para a nomeação, sempre vinculadas a um fundo político qualquer.

Com algumas exceções, os comissionados possuem pouco ou nenhum conhecimento em informática, o que agrava a segurança da rede, especialmente quando eles têm acesso ilimitado aos recursos do sistema operacional do computador que utiliza como terminal de rede.

Fosse noutra empresa qualquer, tais usuários não existiriam ou, se existissem, seria possível investir em treinamento específico para diminuir tal deficiência ocupacional.

Na Câmara, porém, mesmo o treinamento tem se revelado pouco eficiente, uma vez que a rotatividade dos servidores em cargos em comissão é extremamente grande e, conseqüentemente, não é raro um servidor ser exonerado durante alguma fase do treinamento, sem que se possa esperar que aquele que assumir em seu lugar tenha algum conhecimento em informática.

Também os servidores efetivos, cuja rotatividade é próxima de zero, possuem alguma deficiência em informática, mas, nestes casos, é possível solucionar tal deficiência por meio de treinamentos específicos e, dos novos servidores efetivos admitidos, é comum que se exija conhecimentos em informática por ocasião do concurso público.

Além disso, em relação aos servidores efetivos, é mais fácil limitar o acesso aos recursos do sistema operacional do computador utilizado como terminal de rede, dando a eles conta de usuário sem direitos de administrador.

Após a análise da rede, verificou-se que o produto mais adequado às necessidades da Câmara é o Symantec Endpoint Protection, em face de algumas características que são capazes de minimizar a deficiência técnica dos usuários, em especial porque possui um console de gerenciamento remoto das políticas de segurança da rede.

Outra característica importante é que a Symantec possui um sistema de licença corporativa que disponibiliza uma chave única de validação em seu portal na internet, o que torna extremamente fácil a instalação do software sem a necessidade de controle de licenças individualizadas para cada computador, vinculando-se a Câmara ao contrato padrão da Symantec, numa relação comercial de boa-fé.

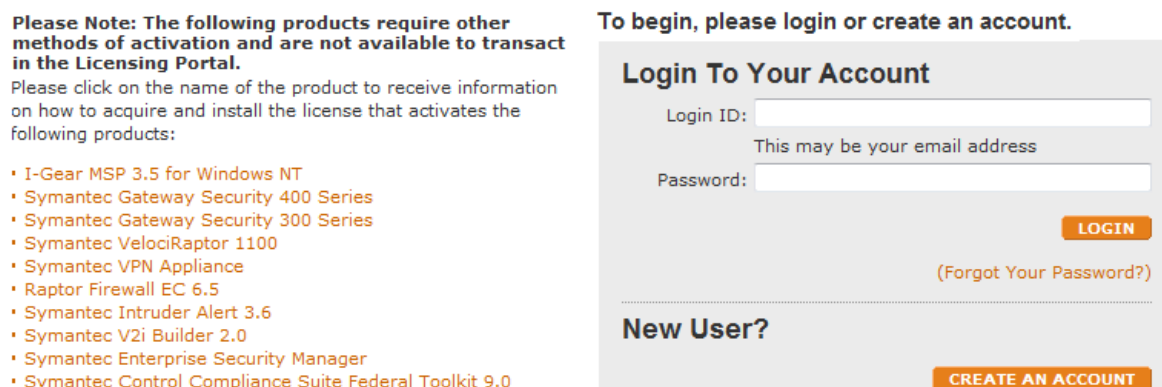
Para a obtenção do software que pode ser instalado em todos os computadores da empresa sem a necessidade de chaves individuais, basta o registro do certificado pela internet, como se verá no próximo capítulo.

CAPÍTULO 3 – SOLUÇÃO SYMANTEC PARA REDE WINDOWS

No manual de Introdução¹⁶ do Endpoint estão relacionados vários endereços de Internet onde é possível obter inúmeras informações úteis, inclusive os links para registro e *download* dos *softwares* e documentação.

3.1 A LICENÇA DE USO

O certificado de licença da Symantec, pelo menos para o Endpoint Protection, é enviado em arquivo PDF, por meio de correio eletrônico ao revendedor que deve repassá-lo ao cliente final, no caso a Câmara Municipal. O certificado contém a identificação do cliente (Customer Number) e o número de série do produto, os quais possibilitam o registro no sítio eletrônico da Symantec, no endereço de internet <https://licensing.symantec.com/acctmgmt/index.jsp>¹⁷, onde é possível encontrar todos os programas e documentação, disponíveis para download após o registro. Para acesso, é necessário efetuar o login, cadastrando-se um nome de usuário vinculado a um e-mail válido e uma senha de acesso.



Please Note: The following products require other methods of activation and are not available to transact in the Licensing Portal.

Please click on the name of the product to receive information on how to acquire and install the license that activates the following products:

- I-Gear MSP 3.5 for Windows NT
- Symantec Gateway Security 400 Series
- Symantec Gateway Security 300 Series
- Symantec VelociRaptor 1100
- Symantec VPN Appliance
- Raptor Firewall EC 6.5
- Symantec Intruder Alert 3.6
- Symantec V2i Builder 2.0
- Symantec Enterprise Security Manager
- Symantec Control Compliance Suite Federal Toolkit 9.0

To begin, please login or create an account.

Login To Your Account

Login ID:

This may be your email address

Password:

LOGIN

(Forgot Your Password?)

New User?

CREATE AN ACCOUNT

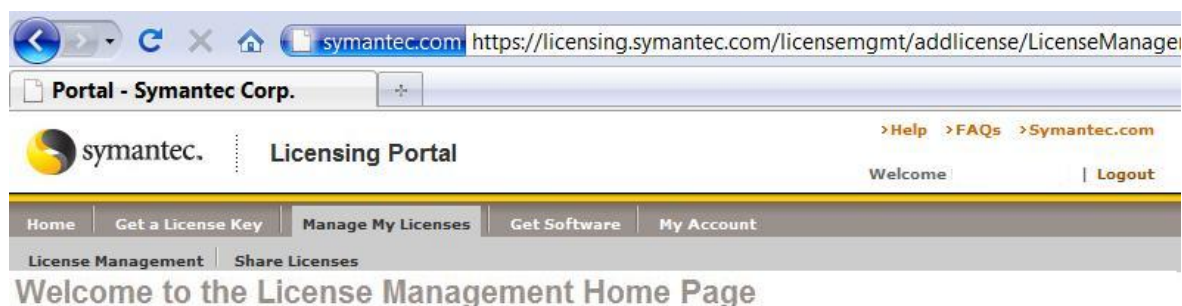
Figura 1 – Página de login no portal de licença da Symantec
Fonte Symantec (2010)

Após logado, o usuário encontrará abas com as opções Home, Get a License Key, Manage My licenses, Get Software e My Account, onde será possível gerenciar a

¹⁶ SYMANTEC. **Introdução do Symantec Endpoint Protection**. Cupertino: Symantec, 2009, p. 19.

¹⁷ Acessado em 2-9-2010.

conta de usuário e as licenças e fazer o download do software e documentação do Symantec Endpoint Protection.



This tool enables you to do the following:

- Add License Information to your personalized License Catalog
- Search for licenses in your License Catalog
- View and edit individual license details including order, ownership, and deployment information
- Define your own User-Defined Fields to customize how you track your licenses
- Share license information with other Licensing Portal users
- View limited License History information

Figura 2 – Página início do portal de licença da Symantec
Fonte Symantec (2010)

Ao clicar na aba “manage my licences” encontra-se uma caixa de diálogo para a inserção do Serial Number e do Customer Number, que constam do certificado de licença fornecido pela Symantec.

Figura 3 – Página para adição de licenças no portal Symantec
Fonte Symantec (2010)

Após inseridos o *serial number* e o *costumer number* serão mostradas todas licenças adquiridas pela empresa e não só aquela cujo o *serial number* foi informado.

Na figura a seguir, foram apagados os *serial number* e o *customer number*, por mera descrição. Para adicionar as licenças, isso basta selecionar as desejadas adicionar e clicar no botão “Add Licenses”.

Portal - Symantec Corp.

symantec. Licensing Portal

>Help >FAQs >Symantec.com

Welcome | Logout

Home Get a License Key Manage My Licenses Get Software My Account

License Management Share Licenses

Select Licenses To Add

Select the Licenses you wish to add to your license catalog for
Serial Number
Customer Number

Select All Clear All

SKU	Quantity	Product Description	Fulfilled	Serial Number	License Key Required	License Keys
<input checked="" type="checkbox"/>	112	SYMC ENDPOINT PROTECTION 11.0 RENEWAL ESSENTIAL- 12 MONTHS EXPRESS BAND D	N		No	
<input checked="" type="checkbox"/>	10	SYMC ENDPOINT PROTECTION 11.0 RENEWAL ESSENTIAL- 12 MONTHS EXPRESS BAND D	N		No	

Select All Clear All

Add Licenses Cancel

Figura 4 – Página para seleção de licenças a serem adicionadas
Fonte Symantec (2010)

O portal apresenta, então, a confirmação de que suas licenças foram adicionadas com sucesso, conforme se vê na imagem abaixo.

symantec. Licensing Portal

>Help >FAQs >Symantec.com

Welcome | Logout

Home Get a License Key Manage My Licenses Get Software My Account

License Management Share Licenses

Licenses Added Confirmation

You have added licenses for
Serial Number
Customer Number

Please select one of the links below to continue adding licenses to your license catalog or to view your recently added licenses.

[View Licenses Just Added](#)

[Add More Licenses To Your Catalog](#)

Figura 5 – Página que confirma a adição de licenças
Fonte Symantec (2010)

Clicando-se na opção “View Licenses Just Added” será informado as licenças que foram recém adicionadas, as quais devem ser registradas. Para registrar a licença é necessário exibir os detalhes da licença adicionada, clicando em “View Details”.



The screenshot shows the Symantec Licensing Portal interface. At the top, there's a navigation bar with links like Home, Get a License Key, Manage My Licenses, Get Software, and My Account. Below this, a search results section is displayed. It shows a table with columns: Date, License Description, Quantity Purchased, Host ID, Serial Number, Customer Name / (Number), and SAN. Two licenses are listed, both dated 26-Aug-2010, for SYMC ENDPOINT PROTECTION 11.0 RENEWAL ESSENTIAL- 12 MONTHS EXPRESS BAND D. The first license has a quantity of 112, and the second has a quantity of 10. Both are for CAMARA MUNICIPAL DE LONDRINA. A 'View Details' link is provided for each license.

Date	License Description	Quantity Purchased	Host ID	Serial Number	Customer Name / (Number)	SAN	Action
26-Aug-2010	SYMC ENDPOINT PROTECTION 11.0 RENEWAL ESSENTIAL- 12 MONTHS EXPRESS BAND D	112			CAMARA MUNICIPAL DE LONDRINA (50379070)		View Details
26-Aug-2010	SYMC ENDPOINT PROTECTION 11.0 RENEWAL ESSENTIAL- 12 MONTHS EXPRESS BAND D	10			CAMARA MUNICIPAL DE LONDRINA (50379070)		View Details

Figura 6 – Página que exibe as licenças adicionadas
Fonte Symantec (2010)

Finalmente, para efetuar o registro da licença adicionada basta clicar em “Register this License” e o portal pedirá a confirmação de registro, que deve ser feita clicando em “Complete Registration”.



The screenshot shows the 'License Details' page. On the left, there's a sidebar with links: Get A License Key, Register This License, License Management, Email License Details, and Get Software. The main content area shows the license key required (No) and a 'GET SOFTWARE' button. Below this, there's an 'Order Details' section with fields for Customer Name, Customer Number, Order Number, and Quantity Purchased. The 'License Key Details' section shows the Product (SKU), Product Version, Serial Number, Date Added, and License Key Required (No).

Order Details	
Customer Name:	CAMARA MUNICIPAL DE LONDRINA
Customer Number:	50379070
Order Number:	174036
Quantity Purchased:	112

License Key Details	
Product (SKU):	SYMC ENDPOINT PROTECTION 11.0 RENEWAL ESSENTIAL- 12 MONTHS EXPRESS BAND D (14042786)
Product Version:	11.0
Serial Number:	14042786
Date Added:	08-26-2010
License Key Required:	No

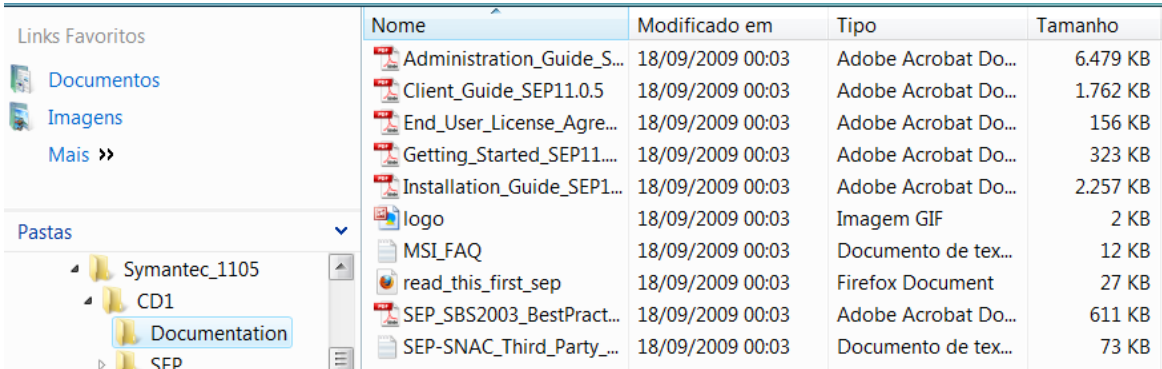
Figura 7 – Página com os detalhes das licenças a serem registradas
Fonte Symantec (2010)

3.2 SOFTWARE E DOCUMENTAÇÃO

Após efetuado o registro, o software pode ser baixado clicando-se no botão “Get Software” (veja imagem anterior) que redirecionará para a página de download, onde se escolherá a versão no idioma desejado que, no presente caso, é o “Brazilian Portuguese”.

Embora a versão atual do Endpoint seja a 11.0.6, a versão instalada na Câmara é a anterior, 11.0.5, a qual, do ponto de vista didático acadêmico, não possui diferenças significativas, e a atualização pode ser feita automaticamente, sem qualquer complicação, bastando, para tanto, a instalação da versão 11.0.6.

Depois de descompactado o arquivo baixado, verifica-se a estrutura de pastas divididas em dois CDs. No CD1 estão os arquivos de instalação do Symantec Endpoint Protection e toda a documentação do sistema, que é composta por Guia de Administração, Manual do Cliente, Licença Final de Uso, Instruções iniciais, Manual de Instalação, entre outros, conforme se observa pela imagem abaixo.



Nome	Modificado em	Tipo	Tamanho
Administration_Guide_S...	18/09/2009 00:03	Adobe Acrobat Do...	6.479 KB
Client_Guide_SEP11.0.5	18/09/2009 00:03	Adobe Acrobat Do...	1.762 KB
End_User_License_Agre...	18/09/2009 00:03	Adobe Acrobat Do...	156 KB
Getting_Started_SEP11...	18/09/2009 00:03	Adobe Acrobat Do...	323 KB
Installation_Guide_SEP1...	18/09/2009 00:03	Adobe Acrobat Do...	2.257 KB
logo	18/09/2009 00:03	Imagem GIF	2 KB
MSI_FAQ	18/09/2009 00:03	Documento de tex...	12 KB
read_this_first_sep	18/09/2009 00:03	Firefox Document	27 KB
SEP_SBS2003_BestPract...	18/09/2009 00:03	Adobe Acrobat Do...	611 KB
SEP-SNAC_Third_Party_...	18/09/2009 00:03	Documento de tex...	73 KB

Figura 8 – Descrição da pasta de documentação do Endpoint
Fonte: Autoria Própria

Entre os programas estão incluídos o Symantec Endpoint Protection, o Console de Gerenciamento dos clientes do Symantec Endpoint Protection Small Business Edition para proteção dos computadores que executam sistemas operacionais tanto de 32 quanto de 64 bits e o Administrador e servidor do Symantec

LiveUpdate, que efetua o gerenciamento centralizado das atualizações dos produtos Symantec.

No CD2 estão os programas da Central de Quarentena, que executa o gerenciamento da quarentena dos arquivos infectados de forma centralizada, e os programas de antivírus para plataforma Linux, que estão inclusos no pacote de programas, além de alguns utilitários do Endpoint.

Embora o Symantec Antivírus para o sistema operacional Linux possa ser utilizado sem restrições de uso, cada instalação conta como uma licença utilizada, devendo ser considerada no total de instalações efetuadas na rede.

CAPÍTULO 4 – INSTALAÇÃO DO ENDPOINT EM REDE WINDOWS

4.1 REQUISITOS MÍNIMOS PARA INSTALAÇÃO

Como a maioria dos sistemas computacionais, o Symantec Endpoint também exige requisitos mínimos de plataforma para cada um de seus recursos¹⁸, os quais poderão variar conforme a opção escolhida de instalação, se 32 ou 64 bits.

Basicamente, para instalação em 32 bits do Console de Gerenciamento, do Banco de Dados Interno, do Console de Quarentena e do Servidor de Quarentena Central será suficiente um computador com processador Pentium III, processador com 1 gigahertz de velocidade, 1 gigabite de memória RAM, 8 gigabites de espaço livre em disco rígido (4 para o console de gerenciamento e 4 para o banco de dados interno), adaptador de vídeo e monitor com resolução de 640x480 pixels, sistema operacional Windows 2000 server com Service Pack 3 (ou Windows XP), Internet Explorer 6 e IP estático.

Os requisitos para instalação em 32 bits do cliente do Symantec Protection são os mesmos dos exigidos para instalação do console de gerenciamento, com exceção do espaço mínimo livre em disco rígido, que é de apenas 600 megabites.

As instalações do Console de Gerenciamento, do Banco de Dados Interno, do Console de Quarentena e do Servidor de Quarentena Central, em 64 bits, como era de se esperar, exigem requisitos mais estritos, além de variar conforme o sistema operacional do computador, não oferecer suporte para os processadores Itanium e não poder ser instalado no Windows 2000 server, pelo fato de este não oferecer suporte para 64 bits.

A velocidade mínima do processador deverá ser de 2 gigahertz se o sistema operacional for o Windows Small Business Server 2008 Premium Edition e de 2,5

¹⁸ SYMANTEC. **Guia de Instalação do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009, pags. 25-46.

gigahertz, caso o sistema operacional seja o Windows Essential Business Server 2008 Premium Edition.

Em 64 bits, a velocidade de 1 gigahertz é aceita somente com os processadores Intel Xeon e Pentium IV que tenham com suporte para EM64T e com os processadores AMD Opteron e Athlon, os dois de 64 bits.

A memória RAM mínima é de 1 gigabite para a maioria dos sistemas operacionais e de 4 gigabites para as versões do Windows Server 2008. O espaço mínimo livre em disco rígido e as resoluções mínimas de adaptador de vídeo e de monitor são os mesmos da instalação em 32 bits. Ou seja, 8 gigabites e 640x480 pixels, respectivamente. Também exige Internet Explorer 6 e IP estático.

Para instalação em 64 bits do Cliente do Symantec Protection as diferenças nos requisitos mínimos em relação aos requisitos para o Console de Gerenciamento são o espaço livre em disco rígido, que é de apenas 700 megabites, e as resoluções do adaptador de vídeo e de monitor, que são maiores: 1024x768 pixels.

Na Câmara Municipal, optou-se pela instalação de 32 bits porque o sistema operacional do servidor é o Windows 2000 Server, o que, de plano, inviabiliza a instalação de 64 bits.

4.2 INSTALAÇÃO DO CONSOLE DE GERENCIAMENTO

Antes de iniciar a instalação do Console de Gerenciamento, é necessário instalar o serviço de informação da internet (IIS – Internet Information Service) no computador que irá receber a instalação do Console de Gerenciamento. O Internet Information Services é um serviço que faz parte do pacote de instalação do Windows 2000 Server e é requisito indispensável para a instalação e funcionamento do Console de Gerenciamento do Symantec Endpoint Protection.

Aliás, esta foi a principal razão pela escolha do Servidor de Internet, que já possuía o serviço de informação da internet instalado, para servir também o Console de Gerenciamento do Endpoint. Na Câmara, o Console de Gerenciamento também foi instalado no servidor de backup, por questões óbvias de segurança, para eventual redundância dos recursos do Endpoint.

Para a instalação do Console de Gerenciamento inicia-se pelo programa “setup”, encontrado na raiz do CD1, que apresentará a tela inicial abaixo, na qual deverá ser selecionado o botão “Instalar o Symantec Endpoint Protection Manager”.



Figura 9 – Tela inicial de instalação do Endpoint
Fonte Symantec (2010)

Na tela seguinte selecione “avançar”, aceite os termos do contrato de licença e selecione “avançar” novamente. Neste momento o programa de instalação permite que se escolha o local de instalação. Selecione o local, que pode ser o padrão sugerido pela instalação e clique em avançar.

Neste ponto, como se vê na figura abaixo, o instalador irá requerer o tipo de site que será usado pelo Console de Gerenciamento, e dará as opções “site personalizado” ou “site padrão”. Recomenda-se criar um site personalizado, com porta número 8014, para que o Endpoint possa utilizar todos os seus recursos de

segurança. Além disso, é necessário que a porta 8014 (ou qualquer outra designada para site do Endpoint) não esteja bloqueada por algum *firewall* existente na rede ou no próprio servidor onde o Endpoint é instalado.

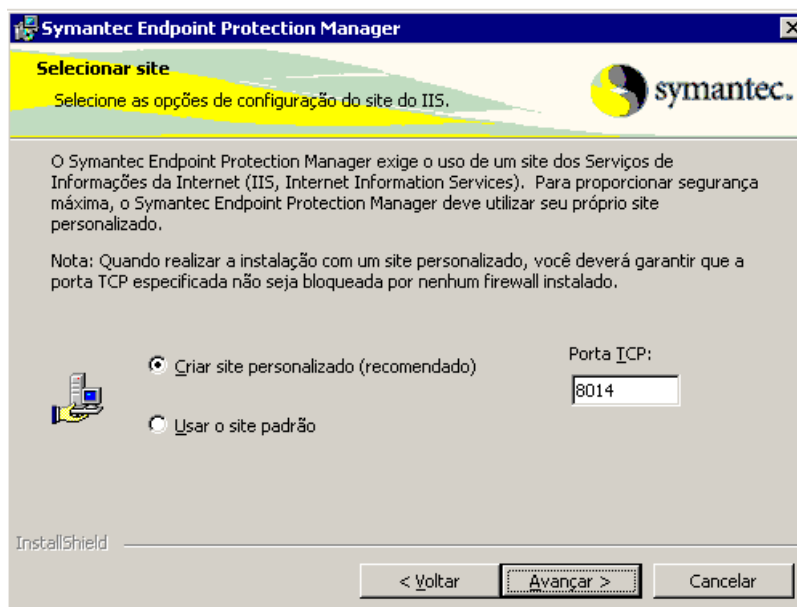


Figura 10 – Tela de opção para criar o site Endpoint
Fonte Symantec (2010)

Em seguida, deve-se selecionar o botão “Instalar” e aguardar o término da instalação, que levará alguns minutos.

Após, basta selecionar o botão “Concluir” para completar a instalação e iniciar a configuração do Servidor de Gerenciamento.

A tela a seguir apresenta duas opções para a configuração do servidor: simples ou avançado.

No caso da Câmara, que possui mais de cem computadores na rede, optou-se pelo modo avançado de configuração.



Figura 11 – Tela que define o tipo de configuração
Fonte Symantec (2010)

Seleciona-se, então, a quantidade de computadores da rede entre as opções apresentadas pelo programa instalador.

A correta seleção é importante porque é nesse momento que o sistema define o tamanho do Banco de Dados interno, com intervalos de quantidade de computadores com boa margem de segurança. No caso da Câmara optou-se pelo intervalo entre 100 e 500 computadores.

Na sequência, pede-se a opção para criação do site do Endpoint, que poderá ser: um site primário, novo, com um servidor de gerenciamento e um banco de dados; somente um servidor de gerenciamento, que utilizará um banco de dados já existente na rede e será um gerenciador redundante e para balanceamento de carga; ou, por fim, um novo servidor de gerenciamento e um novo banco de dados para replicação total.

Na Câmara Municipal foi instalado um site primário num dos servidores de rede e, em seguida, instalado no servidor de Backup outro Console de gerenciamento com banco de dados para replicação, o qual poderá assumir os serviços em caso de falha no servidor primário, além de servir para balanceamento de carga.

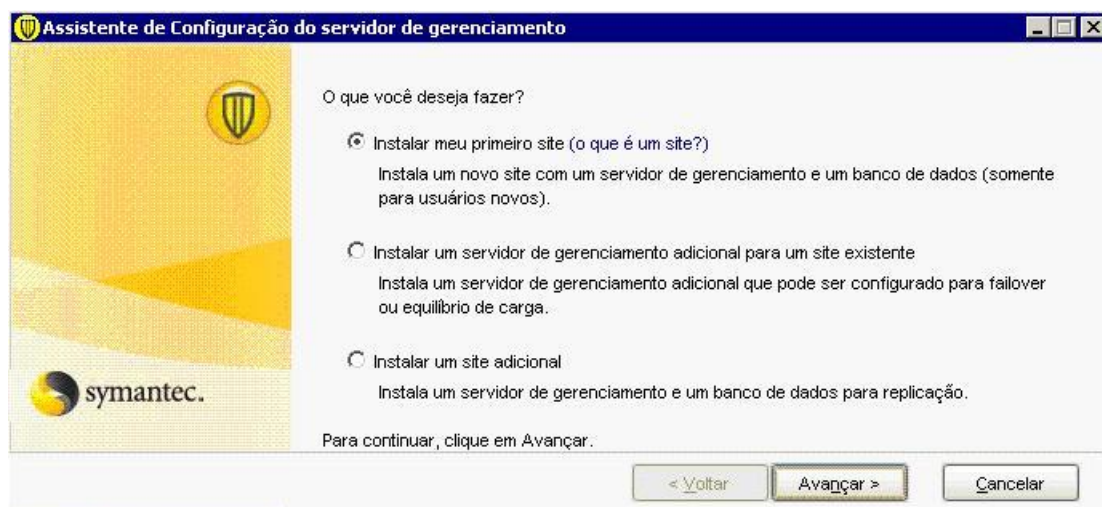


Figura 12 – Tela com opção para os tipos de site do Endpoint
Fonte Symantec (2010)

Recomenda-se manter as configurações padrões sugeridas pelo programa instalador para o nome servidor, a porta do servidor, a porta do console Web e o local de dados do servidor, conforme se vê na figura abaixo.

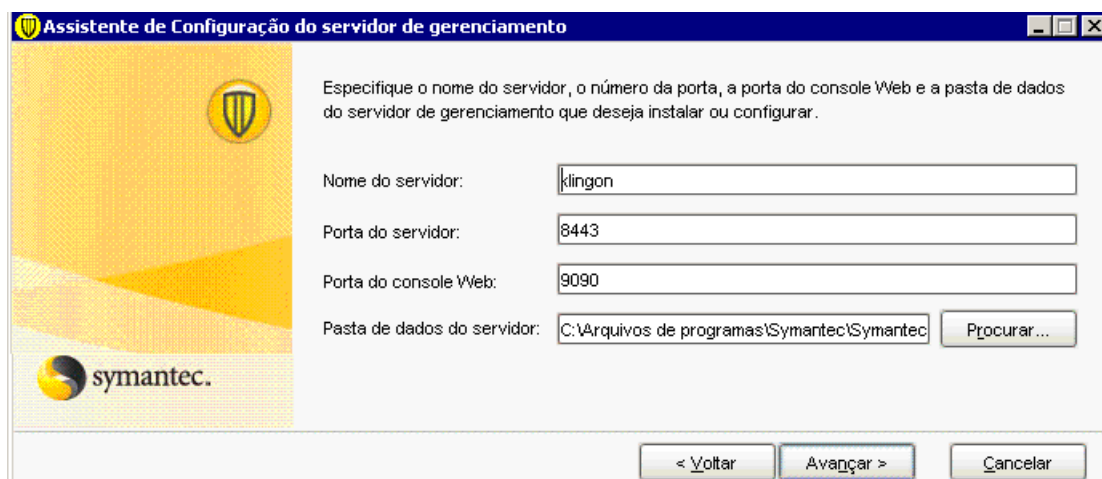


Figura 13 – Tela para informação do nome do servidor e porta
Fonte Symantec (2010)

O nome do site deve ser, de preferência, o mesmo nome do servidor sugerido pelo programa instalador.

Caso a instalação seja de um Console e Banco de Dados adicionais, o programa instalador irá solicitar o nome do Servidor a ser replicado e nome do usuário com direitos para replicar dados. (figura abaixo).

A imagem mostra a janela "Assistente de Configuração do servidor de gerenciamento" do Symantec. O título da janela é "Assistente de Configuração do servidor de gerenciamento". À esquerda, há um painel amarelo com o ícone de um escudo e o logotipo "symantec.". À direita, há um formulário com o seguinte texto: "Especifique o nome do servidor e as credenciais do administrador do Symantec Endpoint Protection Manager para o servidor de gerenciamento com o qual deseja replicar os dados.".

O formulário contém os seguintes campos:

- Servidor de replicação: Plutao
- Porta do servidor de replicação: 8443
- Nome do administrador: administrator
- Senha: [campo com pontos para ocultar a senha]

Na parte inferior da janela, há três botões: "< Voltar", "Avançar >" e "Cancelar".

Figura 14 – Tela para informação do usuário e senha do administrador
Fonte Symantec (2010)

Eventualmente, o instalador não conseguirá verificar o certificado do site a ser replicado, mas a replicação pode ser forçada, selecionando a opção "replicar assim mesmo". Na sequência, deverá ser escolhido o banco de dados a ser utilizado pelo Servidor de Gerenciamento, que poderá ser o Banco de Dados Interno do Endpoint ou um servidor SQL que se tenha disponível na empresa.

A imagem mostra a janela "Assistente de Configuração do servidor de gerenciamento" do Symantec. O título da janela é "Assistente de Configuração do servidor de gerenciamento". À esquerda, há um painel amarelo com o ícone de um escudo e o logotipo "symantec.". À direita, há um formulário com o seguinte texto: "Selecione o tipo de banco de dados que deseja usar:".

O formulário contém duas opções de seleção:

- ☒ Banco de dados interno
Sugerido para organizações com mais de 5.000 computadores-cliente.
- ☐ Microsoft SQL Server

Na parte inferior da janela, há três botões: "< Voltar", "Avançar >" e "Cancelar".

Figura 15 – Tela com opção dos tipos de bancos de dados
Fonte Symantec (2010)

Na Câmara Municipal, utilizou-se o Banco de Dado Interno do Endpoint, uma vez que ele suporta os dados de até cinco mil computadores, que é um número muito superior à quantidade de máquinas existentes na rede da Câmara. Outro fator

interessante em se utilizar o banco de dados interno do Endpoint é não sobrecarregar o servidor de banco de dados SQL utilizado para outros serviços da empresa.

Nada impede, entretanto, que se utilize um banco de dados SQL externo desde que sejam respeitadas as regras de configuração¹⁹ específicas para o Endpoint, as quais não foram abordadas no presente estudo, uma vez que há a exigência de banco de dados externo somente se existirem mais de cinco mil computadores.

O programa instalador pedirá a inserção de uma senha para uso do Banco de Dados Interno e passará a criá-lo, o que deverá demorar vários minutos, especialmente se for caso de replicação de banco de dados já existente.

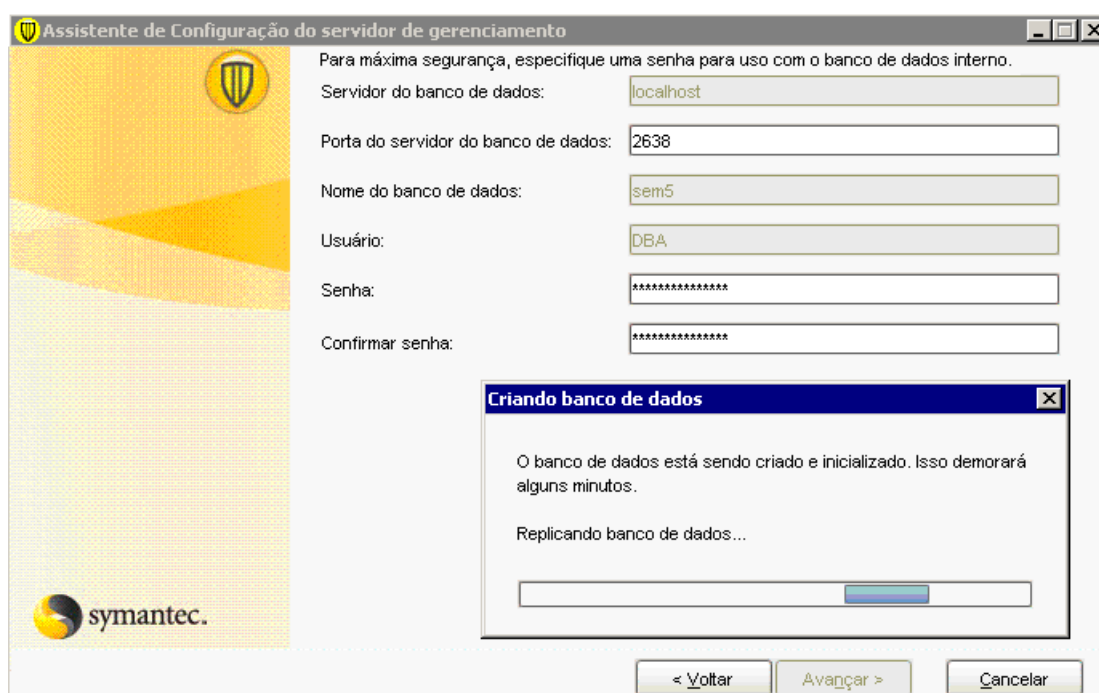


Figura 16 – Tela com notificação da replicação do banco de dados
Fonte Symantec (2010)

¹⁹ SYMANTEC. Guia de Instalação do Symantec Endpoint Protection e do Symantec Network Access Control. Cupertino: Symantec, 2009, pags. 68-78.

Terminada a replicação, deve-se selecionar a opção “Concluir”, e a configuração estará terminada e o Console de Gerenciamento do Endpoint estará pronto para ser usado.

4.3 INSTALAÇÃO DOS CLIENTES GERENCIADOS

É possível que se instale o Endpoint não gerenciado em computadores da rede, mas essa não seria uma escolha interessante quando se sabe que o recurso de gerenciamento remoto é a característica que torna o Endpoint uma ferramenta atrativa às redes de computadores corporativas. O Endpoint pode ser instalado nos computadores clientes diretamente pelo CD de instalação. Neste caso, para que o computador seja reconhecido como cliente gerenciado do Servidor de Gerenciamento Endpoint, em um determinado momento da instalação informa-se a condição de cliente gerenciado e o nome do servidor do qual será cliente.

A instalação remota, a mais recomendada por ser realizada de modo insensível ao usuário da rede, é feita a partir do Console de Gerenciamento do Endpoint, após o devido *login* de acesso, utilizando-se o usuário e senha definidos para o Banco de Dados durante a instalação do Servidor de Gerenciamento do Endpoint.

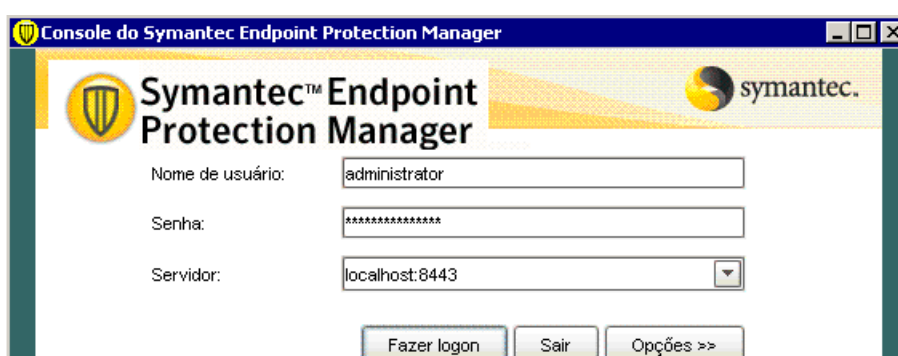


Figura 17 – Login no Console de Gerenciamento
Fonte Symantec (2010)

O primeiro passo para a instalação do cliente é a criação de um pacote de instalação, o qual deve ser armazenado em uma pasta que será informada durante o processo de instalação remota do cliente.

Para criar um pacote de instalação deve-se acessar o Console de Gerenciamento, na guia Admin, e executar a tarefa “Exportar pacote de instalação do Cliente”, definindo-se a pasta que conterá o pacote de instalação, com as seleções adequadas, especialmente a que “Altera para cliente gerenciado”, conforme se vê na figura a seguir.

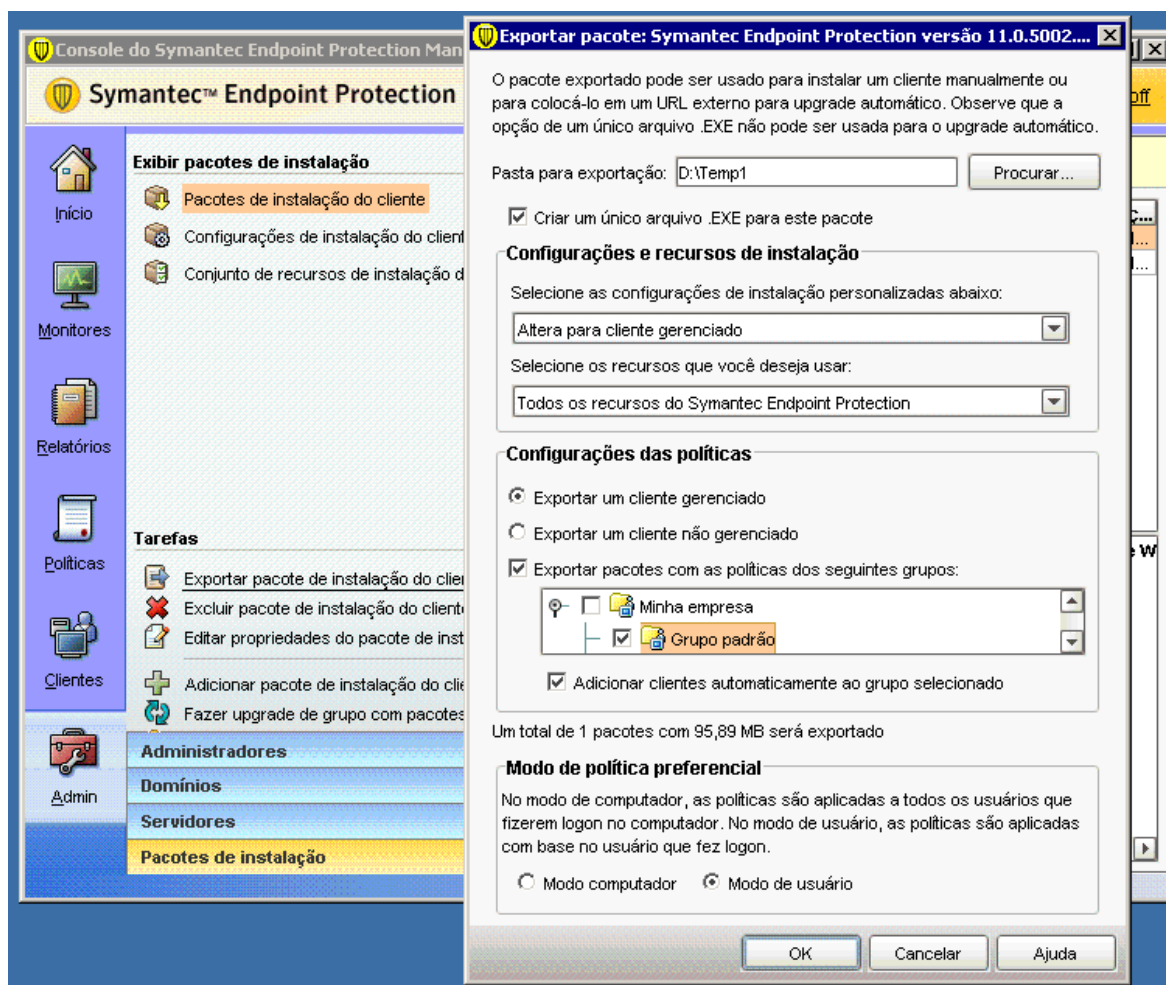


Figura 18 – Tela para exportação de pacote de instalação do cliente
Fonte Symantec (2010)

Antes de proceder à instalação remota do Symantec Ednpoint Protection nos clientes de rede, é necessário habilitar a “Conexão Remota” ou, até mesmo, desabilitar o *firewall* em todos eles e desinstalar qualquer outro antivírus ou outra versão Symantec, para que o instalador remoto funcione adequadamente.

No Windows XP é necessário desativar o compartilhamento simples de arquivo e no Windows Vista é necessário desativar o Assistente de Compartilhamento de Arquivos e ativar a Descoberta de Rede. Em qualquer caso, deve-se usar uma conta de usuário com poderes de administração do domínio Windows.

É possível a instalação remota em vários clientes simultaneamente, utilizando-se de faixas de IP ou a seleção de vários computadores identificados no domínio. Entretanto, tal prática não é a mais interessante, uma vez que isso dificulta a análise de eventual falha na instalação.

Assim, o ideal é que a instalação remota seja feita individualmente, ou em poucas máquinas simultaneamente, de forma que se possa acompanhar e resolver qualquer falha verificada.

Uma das formas de se configurar o software-cliente é usando Assistente de Migração e implementação, clicando-se em Iniciar, Programas, Symantec Endpoint Protection Manager, Assistente de Migração e implementação. Deve-se escolher a opção implementar o cliente e selecionar o botão avançar (imagem abaixo).

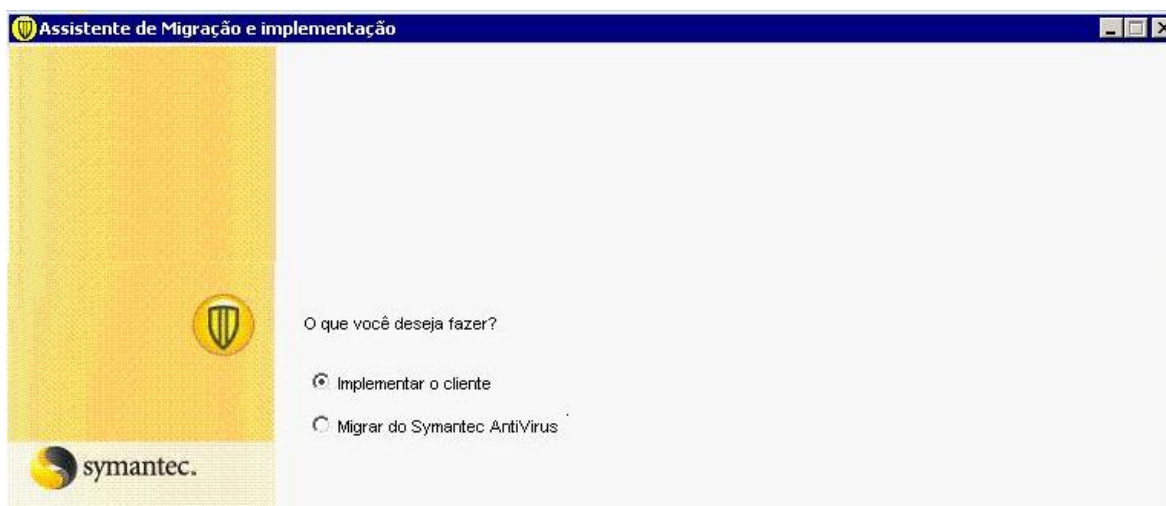


Figura 19 – Tela com opções para implementar ou migrar os clientes
Fonte Symantec (2010)

Deve-se, então selecionar um pacote existente para instalação e concluir.

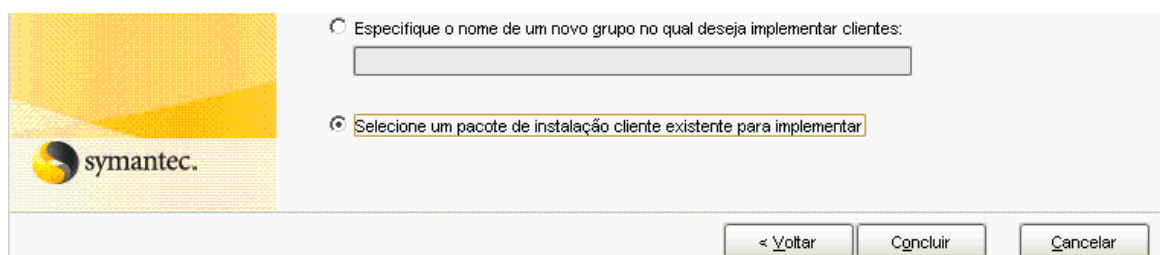


Figura 20 – Tela para seleção de pacote
Fonte Symantec (2010)

Informa-se o local onde foi armazenado o pacote de instalação previamente exportado, conforme se vê na figura abaixo.

Note-se que é possível especificar o número máximo de implementações simultâneas. A sugestão padrão do programa é 10, muito embora possa optar, posteriormente por instalação individualizada do cliente.

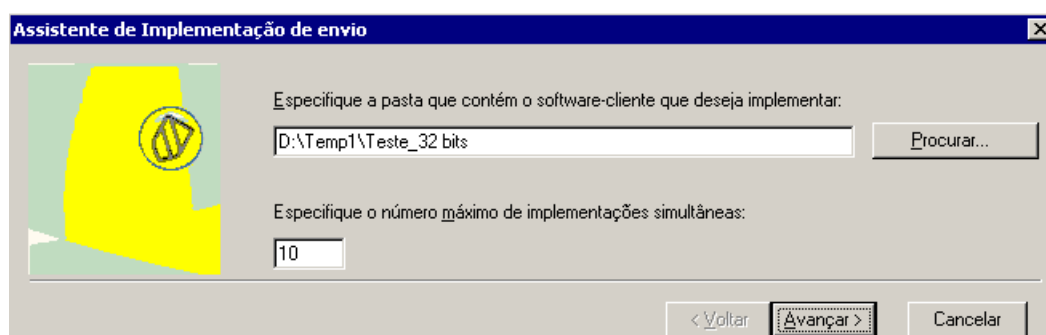


Figura 21 – Tela para informar o local do pacote de instalação
Fonte Symantec (2010)

O passo seguinte é selecionar, dentre os disponíveis na rede os computadores os quais se deseja implementar o cliente Endpoint. O Assistente de Implementação exigirá um usuário com poderes de administrador de domínio nesse momento.

A seleção pode ser feita clicando-se no botão esquerdo do mouse sobre o nome do computador desejado e, depois, sobre o botão adicionar, conforme se vê na figura abaixo.

Para excluir um computador da seleção clica-se com mouse sobre o botão remover.

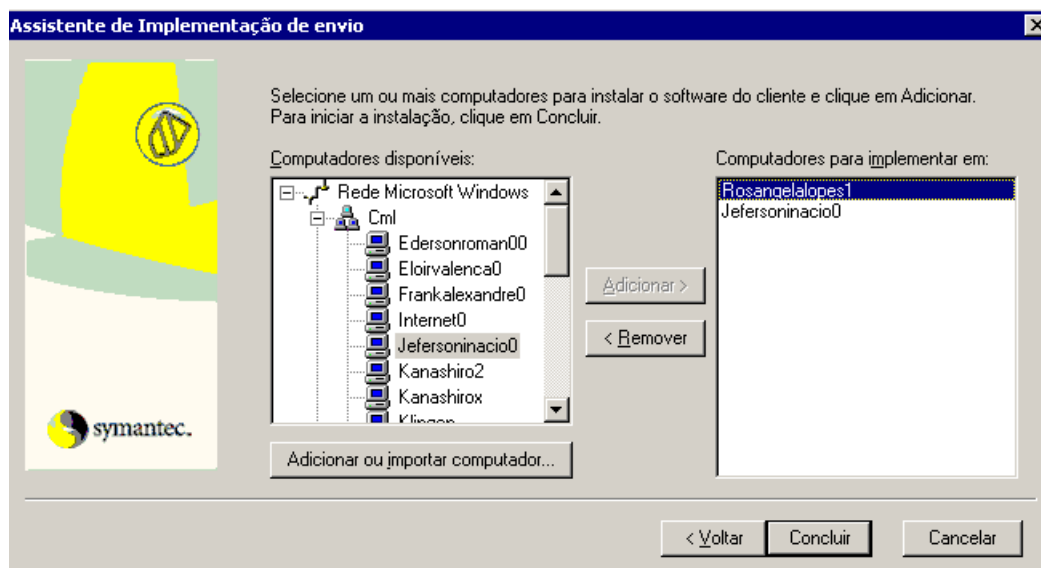


Figura 22 – Tela para seleção de computadores a serem instalados
Fonte Symantec (2010)

Clicando-se em concluir o Assistente de Implementação enviará o pacote de instalação aos computadores selecionados. A instalação se dará de forma imperceptível ao usuário, caso se tenha escolhido a instalação em modo silencioso quando da exportação do pacote de instalação.

Depois de completada a instalação no computador cliente, ele estará disponível para ser gerenciado remotamente pelo Console de Gerenciamento instalado no servidor.

Outro modo de instalar o software-cliente é por meio da descoberta de computadores não gerenciados, na guia “Clientes” do Console de Gerenciamento. Com este utilitário, é possível detectar computadores que não têm o software-cliente para, em seguida, instalá-lo. Uma deficiência desse utilitário é que ele não reconhece de forma correta os sistemas operacionais Windows 2000, causando alguma imperfeição na instalação do software-cliente, o que pode ser corrigido utilizando o Assistente de Implementação de Envio, já mencionado anteriormente neste tópico.

O utilitário para descoberta de computadores não gerenciados exige completo conhecimento prévio acerca dos computadores existentes na rede, pois, como ele detecta computadores não-conhecidos e exibe dispositivos que podem não ser computadores válidos para instalação do software-cliente como, por exemplo, interfaces de roteador.

Para instalar o software-cliente por meio deste utilitário deve-se clicar na guia “Clientes”, do Console de Gerenciamento, e, depois, em “Encontrar computadores não gerenciados”. Será exibida uma janela onde é possível pesquisar os computadores existentes na rede. A pesquisa pode ser feita por intervalo de IP ou por nome do computador reconhecido pelo domínio.

A pesquisa deve ser feita informando-se o domínio Windows desejado e um usuário com poderes de administrador do domínio. É possível instalar computadores individuais ou vários ao mesmo tempo, por meio de seleção específica para ambas as opções.

Devido à delimitação do tema e dos objetivos, esta pesquisa não se aprofundou a respeito da instalação do *software*-cliente por outros meios como, por exemplo, a importação de arquivo texto²⁰, usando o Assistente de Implementação de Envio, e a instalação do *software*-cliente por meio de utilitários disponíveis em programas de terceiros²¹ compatíveis com o Endpoint.

Outros produtos de terceiros, como o Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS) e Novell ZENworks, também são reconhecidos pela Symantec como compatíveis para a instalação do *software*-cliente do Endpoint Protection.

²⁰ “Em vez de selecionar computadores durante a instalação do Assistente de Implementação de envio, você pode importar uma lista de computadores de um arquivo de texto”. In SYMANTEC. **Guia de Instalação do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009, p. 109.

²¹ “O *software*-cliente da Symantec aceita instalação com ferramentas de terceiros para implementar o *software*-cliente. Esse suporte, contudo, requer conhecimentos avançados das ferramentas de gerenciamento do Windows ou de terceiros. As redes em grandes escalas são mais passíveis de beneficiarem-se com o uso dessas opções avançadas para instalar o *software*-cliente da Symantec”. Idem, In SYMANTEC. Idem, pp.109-110.

O Altiris²² é um exemplo de *software* de terceiros, embora a empresa Altires agora faça parte da Symantec.

²² “Você pode instalar e implementar o software-cliente da Symantec usando software da Altiris, que agora faz parte da Symantec. O Altiris fornece um componente de instalação do software-cliente da Symantec integrado gratuito do Symantec Endpoint Protection, que inclui capacidades de instalação padrão, gerenciamento de clientes integrado e relatórios de alto nível. O software da Altiris permite que organizações de tecnologia da informação gerenciem, protejam e sirvam ativos de TI heterogêneos. Também aceita entrega de software, gerenciamento de caminho e muitos outros recursos de gerenciamento. O software da Altiris ajuda a TI a alinhar serviços para atingir objetivos de negócios, entregar segurança pronta para auditoria, automatizar tarefas e reduzir os custos e a complexidade do gerenciamento”. In SYMANTEC. **Guia de Instalação do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009, p. 109.

CAPÍTULO 5 – OS RECURSOS DO ENDPOINT PROTECTION

O Symantec Endpoint Protection possui recursos de servidor, disponíveis para os administradores para que possam gerenciar o Endpoint na rede, e recursos de cliente, disponíveis a nível local e que são acessíveis total ou parcialmente pelo usuário do computador cliente. Os direitos de acesso aos recursos do software-cliente podem (e devem) ser definidos pelo administrador da rede quando da sua instalação.

Os recursos de gerenciamento compreendem o Console de Gerenciamento, o Banco de Dados Interno, a Quarentena Central e o Servidor de LiveUpdate.

Os principais recursos do software-cliente são o Auto-Protect, a Proteção Antivírus e Anti-Spyware, a Proteção Contra Ameaças à Rede e a Proteção Proativa Contra Ameaças.

5.1 RECURSOS DE GERENCIAMENTO

5.1.1 O Console de Gerenciamento

O Console de Gerenciamento, conforme se verifica no Guia de Administração²³ do Endpoint, é o utilitário que permite ao usuário o acesso à maioria dos recursos do sistema. Pode-se fazer o *logon* no Console de Gerenciamento tanto remotamente, por meio de um computador com os recursos para acesso remoto, quanto diretamente, no computador onde foi instalado o Console.

O conjunto de recursos disponíveis no Console de Gerenciamento depende diretamente dos direitos do usuário que efetuou o *logon* e, por isso, recomenda-se

²³ SYMANTEC. **Guia de Administração do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009, pp. 41-46.

a utilização de usuário com poderes de administração do domínio Windows que se pretende gerenciar. A Câmara Municipal possui somente um domínio Windows, de forma que todos os administradores têm direitos amplos em toda rede.

O modo de acesso remoto é mais interessante pela dinâmica de uso, uma vez que o servidor onde se instalou o Console de Gerenciamento pode estar localizado em outro local, muitas das vezes distante do usuário, como é o caso da Câmara Municipal, onde as salas dos servidores tem espaço físico próprio.

É possível fazer logon remotamente pelo IP ou pelo nome do servidor por meio da Conexão de Área de Trabalho Remota do Windows ou por meio da máquina virtual JAVA, digitando-se no navegador da internet o endereço *http://nome do host:9090* ou *http://endereço/IP:9090*.

O logon no Console pode ser efetuado acionando-se o programa “Console do Symantec Endpoint Protection Manager”, que pode ser encontrado na pasta “Programas”, no menu “iniciar” do Windows. Deve-se usar o usuário especificado durante a instalação do Servidor de Gerenciamento.

Por meio de uma interface gráfica, o Console pode ser usado para gerenciar políticas e computadores, para monitorar o status da proteção e para criar e gerenciar contas de administrador. O Console de Gerenciamento está dividido em seis páginas (ou guias): Início, Monitores, Relatórios, Políticas, Clientes e Admin.

5.1.2 Página Início

A página “Início” exibe em duas colunas com sete janelas pequenas o estado de segurança da rede, onde se obtém inventários sobre as detecções de vírus, detecções de riscos, computadores atualizados ou desprotegidos e informações de ameaças.

Na primeira coluna, a primeira janela contém o resumo das ações por contagem de detecções e apresenta as quantidades de vírus que foram limpos, suspeitos, bloqueados, postos em quarentena, excluídos, infectados recentemente e ainda infectados, o que dá ao administrador da rede uma ótima base para avaliar o desempenho da segurança da rede no que diz respeito ao combate a vírus de computador.

A segunda contém um gráfico que exibe as quantidades de riscos, ataques e infecções ocorridos nas últimas 12 horas, fornecendo parâmetros de análise sobre o comportamento da defesa da rede, onde se pode observar a relação da quantidade de infecções com as quantidades de riscos e ataques efetivos.

A terceira apresenta o resumo do status com o estado dos computadores clientes, que informa quantos deles estão com algum componente do Endpoint desativado.

Na segunda coluna, a quarta janela permite verificar quantas distribuições de definições de vírus e assinaturas de prevenção de intrusões foram feitas nas últimas doze horas.

A quinta, Security Response, informa as respostas oferecidas às maiores ameaças e às últimas ameaças por vírus de computador, além de conter links que remetem às páginas da Symantec na internet que contém as informações mais recentes sobre respostas a ameaças por vírus.

A sexta traz um resumo dos aplicativos observados e as ocorrências das detecções de ameaças.

Por fim, a sétima janela exibe três relatórios considerados “favoritos”, os quais podem ser redefinidos pelo usuário do Endpoint. Clicando-se sobre as descrições, o sistema abre uma outra janela com o relatório contendo gráficos e dados relativos à opção escolhida, relatório este que pode ser analisado em tela, armazenado em disco ou impresso.

5.1.3 Página Monitores

Pela página “Monitores” é possível monitorar registros de eventos e os computadores gerenciados por meio de gráficos de riscos, registros de eventos, estados de comandos e notificações emitidos.

A página “Monitores” está estruturada em quatro guias: resumo, logs, status do comando e notificações.

Na guia “Resumo” encontram-se os gráficos com os resumos da verificação proativa de ameaças, proteção contra ameaças à rede, conformidade e status do site Endpoint. Os gráficos contêm vários níveis de detalhamento: distribuição de riscos, novos riscos, riscos por origem, riscos por invasor, riscos por grupo, principais alvos atacados (por grupo), tipos de eventos de ataque, principais ocorrências de ataque (por origem), eventos de segurança (por gravidade), falha no estado de conformidade da rede, distribuição do estado de conformidade, falha de conformidade (por cliente), detalhes da falha de conformidade, principais geradores de erro (por servidor e por cliente) e falhas de replicação ao longo do tempo.

Na guia “Logs” obtém-se os registros do estado do computador em um determinado intervalo de tempo desejado. São registros (*logs*) como auditoria, controle de dispositivos e aplicativos, conformidade, status do computador, proteção contra ameaças à rede, verificação proativa de ameaças TruScan, risco, verificação e sistema.

Na guia “Status do comando” podem ser observados os estados em que se encontram os comandos emitidos aos computadores clientes em um período que pode ser de um a trinta dias, conforme a seleção do usuário.

O gráfico mostra o percentual dos comandos que foram ou não recebidos, concluídos, rejeitados, cancelados, que estão em andamento ou que apresentaram erro.

Na guia “notificações” são exibidas os alertas gerados pelo Console de Gerenciamento, referentes a alguma ocorrência na rede, como alerta de segurança do cliente, computadores não gerenciados, definição de vírus desatualizada, detecção de aplicativo forçado ou comercial, epidemia de risco, evento com risco único, evento de sistema, falha de autenticação, integridade do servidor, lista de clientes alterada, novo aplicativo reconhecido, novo pacote de software, novo risco detectado e enforcer (enforcer é uma opção do Symantec Network Access Control, não disponível no Endpoint Protection)²⁴ desligado.

5.1.4 Página Relatórios

Em “Relatórios” estão as informações atualizadas acerca do Servidor de Gerenciamento, dos computadores clientes e de todas as atividades da rede detectadas pelo Endpoint, as quais podem ser filtradas conforme as especificações desejadas, com resumos diários ou semanais.

O Console possui inúmeros relatórios: estado do computador, auditoria, controle de dispositivos e aplicativos, conformidade, proteção contra ameaças à rede, risco, verificação e sistema. O usuário pode definir um intervalo de tempo para a filtragem do relatório desejado, o qual será exibido na tela, salvo em disco, ou impresso.

5.1.5 Página Políticas

A página “Políticas” contém as políticas de segurança aplicadas a um computador ou a grupo de computadores. As políticas podem ser ajustadas, criadas, editadas ou excluídas.

²⁴ Um Enforcer é utilizado pelo Symantec Network Access Control para permitir ou negar acesso à rede corporativa. Há quatro tipos de Enforcers: Gateway Enforcer, LAN Enforcer, DHCP Enforcer e Integrated Enforcer. Trata-se de um recurso não disponível no Symantec Endpoint Protection.

O Console traz algumas políticas que são implementadas no sistema durante a instalação do Servidor de Gerenciamento e dos clientes.

São definidas políticas padrão para o antivírus e anti-spyware, firewall, prevenção de intrusões, controle de dispositivos e aplicativos, LiveUpdate e Exceções centralizadas.

As políticas possuem componentes que levam em consideração os modelos de verificação agendada, as listas de servidores de gerenciamento, as listas de impressões digitais de arquivos, os grupos de host, os serviços de rede, os adaptadores de rede, além de outros dispositivos de hardware aos quais se deseja aplicar políticas e condições de uso.

Além dessas políticas pré-estabelecidas, é possível que sejam importadas ou criadas outra pelo usuário, conforme a sua necessidade.

5.1.6 Página Clientes

Na página “Clientes” é onde se encontram os recursos do Console para gerenciamento dos clientes, onde é possível criar, excluir, editar propriedades, aplicar as políticas de segurança aos clientes, executar comandos em computadores ou grupo de computadores, ativar detector não gerenciado e procurar clientes.

Pode-se, também a partir da página “Clientes”, implementar software-cliente em computadores não gerenciados, como já citado anteriormente.

Com um simples toque na tecla direita do mouse, o usuário emite comandos ao computador cliente para verificação de vírus, atualização de conteúdo e definições de vírus, reiniciar, ativar o auto-protect e ativar ou desativar a proteção contra ameaças à rede.

5.1.7 Página Admin

Pela página “Admin” gerencia-se as configurações, licenças e contas de administrador, onde é possível criar, editar e excluir de tais contas.

Pode-se, ainda, exibir e editar as propriedades do Servidor de Gerenciamento e as configurações de e-mail e de servidor *Proxy*, agendar a atualização, adicionar, excluir e exportar o pacote de instalação do cliente, fazer upgrade de novo pacote de instalação e definir a coleta de informações sobre o usuário.

5.2 RECURSOS DO SOFTWARE CLIENTE

As configurações padrão do cliente Endpoint oferecem proteção antivírus e anti-spyware, proteção proativa contra ameaças e proteção contra ameaças à rede. É possível alterar as configurações padrão conforme as necessidades do usuário e da empresa, uma vez que alguns recursos disponíveis pela configuração padrão do Endpoint podem não ser interessantes ou mesmo úteis diante da realidade da empresa ou do cliente. É possível, ainda, verificar vírus, ameaças conhecidas e riscos à segurança do computador, monitorar assinaturas conhecidas de ataque nas portas, monitorar o comportamento suspeito de programas no computador e proteger o computador contra ataques à rede, além de recursos com várias abordagens de segurança, que incluem o Auto-Protect ativo, a Proteção Antivírus e Anti-spyware, a Proteção Contra Ameaças à Rede e Proteção Proativa Contra Ameaças.

5.2.1 Auto-Protect

A instalação padrão configura o Auto-Protect para ser carregado para a memória quando o computador é iniciado e é executado continuamente na busca por ameaças que possam estar contidas em arquivos recebidos pelo computador por

qualquer meio, como disquetes, discos ópticos, e-mails, internet etc. Se o cliente for gerenciado, é comum que o administrador configure uma verificação completa a cada período, enquanto que no cliente não gerenciado, por padrão, a verificação é feita automaticamente quando o computador é ligado.

Quando ocorre uma detecção de vírus ou ameaça, o Auto-Protect²⁵ notifica o usuário com um alerta na tela do computador. Se a verificação foi disparada pelo usuário ou agendada pelo administrador, uma caixa de diálogo mostra os resultados da verificação enquanto o programa é executado. Na configuração padrão, feita pela instalação, o Endpoint verifica os riscos à segurança e remove para a quarentena os arquivos infectados.

É possível desativar a verificação de riscos à segurança no Auto-Protect, muito embora isso não seja recomendado, a não ser que o usuário tenha pleno conhecimento do que faz, até porque um mesmo risco só é notificado três vezes pelo Auto-Protect antes de passar a ser ignorado por ele, por entender-se que não se trata de um risco real.

Como o Auto-Protect também verifica os e-mails, pode ocorrer que o recebimento de grandes arquivos ocasione uma lentidão no sistema, especialmente em computadores mais antigos. Neste caso, pode ser interessante desabilitar a verificação de e-mails.

5.2.2 Proteção antivírus e anti-spyware

A proteção antivírus e anti-spyware é um recurso que visa proteger o computador

²⁵ “O Auto-Protect é a melhor defesa contra ataques de vírus. Sempre que você acessa, copia, salva, move ou abre um arquivo, ele verifica o arquivo para garantir que não haja um vírus anexado. O Auto-Protect verifica extensões de arquivos que contêm código executável, bem como todos os arquivos .exe e .doc. O Auto-Protect pode determinar o tipo de um arquivo mesmo quando um vírus altera sua extensão. Por exemplo, um vírus pode alterar a extensão de um arquivo para uma que não se inclua entre as extensões que o Auto-Protect foi configurado para verificar. Você pode ativar ou desativar o Auto-Protect se o administrador não bloquear a configuração”. **Guia do Cliente do Symantec Endpoint Protection e do Symantec Network Access Control**. Cupertino: Symantec, 2009. pág. 68.

contra vírus e riscos conhecidos, com o intuito de detectar e remover rápida e eficazmente o vírus, impedindo que se alastre pela rede.

É composta pelo Auto-Protect, tratado no tópico anterior, e pela ferramenta de verificação. As verificações podem se dar quando o computador é ligado ou podem ser executadas periodicamente por agendamento ou por solicitação do usuário do computador.

5.2.3 Proteção contra ameaças à rede

Trata-se de um firewall do Endpoint que denega acesso indevido aos recursos da rede, monitorando as tentativas sistemáticas de identificação de portas e outros ataques de rede conhecidos, de forma a bloquear, ou não, seletivamente, os serviços, portas e recursos de rede.

O firewall do Endpoint possui várias regras padrão, as quais podem ser editadas ou adicionadas, conforme a necessidade da empresa. Aliás, alguns recursos de mapeamento do Windows Vista precisam de permissão específica no *firewall* do Endpoint, conforme se verificou durante a instalação do software-cliente.

5.2.4 Proteção proativa contra ameaças

A Symantec desenvolveu um recurso de análise heurística da estrutura dos arquivos que representam ameaças em potencial. Com esse recurso, é possível detectar um vírus ou uma ameaça ainda que sejam desconhecidos do Endpoint, que tomará as ações necessárias para tratar o arquivo, tendo por base o seu comportamento ou sua estrutura.

A proteção proativa tem o potencial de detectar aplicativos comerciais cujos comportamentos já são conhecidos, por serem usados com objetivos maliciosos,

como, por exemplo, os programas de acesso remoto ou os programas que registram as teclas pressionadas pelo usuário, os keyloggers.

5.2.5 Ícone da Área de Notificação

Um recurso simples, mas interessante, é o ícone da área de notificação, no canto inferior direito da área de trabalho, que faz as indicações do estado do Endpoint no computador cliente. Um clique com o botão direito do mouse sobre ícone o exibe algumas opções de comandos do Endpoint.





	O cliente é executado sem problemas. Está off-line ou é autogerenciado. Os clientes autogerenciados não são conectados a um servidor de gerenciamento.
	O cliente é executado sem problemas. Está conectado e comunica-se com o servidor. Todos os componentes da política de segurança protegem o computador. O ícone mostra um ponto verde.
	O cliente tem um problema menor. Por exemplo, as definições de vírus podem estar desatualizadas. O ícone mostra um ponto amarelo com um ponto de exclamação preto.
	O cliente não é executado, tem um problema principal ou tem pelo menos uma tecnologia de proteção desativada. Por exemplo, a Proteção contra ameaças à rede pode estar desativada. O ícone mostra um ponto branco com um esboço vermelho e uma linha vermelha sobre o ponto.

Figura 23 – Aparências do ícone de notificação
Fonte Symantec (2010)

5.3 OUTROS RECURSOS

Existem, ainda, alguns outros recursos do Symantec Endpoint Protection, como a Quarentena Central e o Servidor LiveUpdate e algumas outras ferramentas disponíveis para o ambiente Windows, como o programa que auxilia na instalação do software-cliente (ClientRemote), o programa de migração de outras versões de produtos Symantec (SCFMigrationTool), o componente de integração do Endpoint com outros produtos Symantec (Symantec Endpoint Protection Integration Component) e o programa para auxiliar na solução de problemas do Endpoint (SupportTool).

Uma anotação que deve ser feita diz respeito ao Symantec Antivírus para Linux, com recursos de gerenciamento e de cliente, que faz parte do pacote de software Endpoint, muito embora não seja um recurso integrado a ele. Uma vez que este estudo diz respeito ao Endpoint em ambiente Windows, não se aprofundará nos referidos recursos para Linux.

5.3.1 Quarentena Central

A Quarentena Central²⁶ é formada pelo Servidor de Quarentena e pelo Console de Quarentena. O Servidor de Quarentena armazena os vírus e os riscos à segurança dos computadores clientes do Endpoint Protection e os encaminha à Symantec, enquanto o Console de Quarentena gerencia o Servidor de Quarentena.

Eles podem ser instalados no mesmo computador, ou não, mas deve-se obedecer a uma ordem de instalação: primeiro instala-se o Console de Quarentena e, em seguida, o Servidor de Quarentena. Os programas de instalações estão disponíveis no CD2 do Symantec Endpoint Protection.

Durante a instalação, deve-se anotar e guardar o número da porta e o endereço IP (ou o nome de host) do computador em que o Servidor de Quarentena foi

²⁶ “Quando o Symantec Endpoint Protection encontra um item infectado, que não pode ser reparado com as definições de vírus atuais, bloqueia o acesso ao mesmo. Depois, o produto empacota o item com todos os arquivos de sistema e configurações afetados e move o pacote para a quarentena local. A quarentena local é um local especial reservado para arquivos infectados e efeitos colaterais relacionados do sistema. Após vírus e outras ameaças serem isolados em uma quarentena local, não podem se disseminar nem danificar o computador. O Symantec Endpoint Protection pode encaminhar automaticamente os pacotes que contêm arquivos infectados e seus efeitos colaterais relacionados de uma quarentena local para a quarentena central. A quarentena central é um repositório central. A quarentena central consiste de dois componentes: o servidor de quarentena e o snap-in do Microsoft Management Console (MMC). Além de verificar se há vírus nos arquivos, os clientes do Symantec Endpoint Protection verificam se há riscos à segurança, como spyware, adware, ferramentas de hacker e programas de brincadeiras. Também é possível encaminhar esses arquivos infectados à quarentena central. No entanto, as ameaças detectadas e colocadas em quarentena pela proteção proativa contra ameaças são enviadas com um mecanismo diferente”. In SYMANTEC. **Guia de Implementação do Symantec Central Quarantine**. Cupertino: Symantec, 2009, p. 9.

instalado, pois essas informações serão necessárias no momento da configuração dos clientes para envio de dados à Quarentena Central, tanto para escuta do Servidor de Quarentena quanto para a remessa pelos clientes.

A configuração dos clientes é feita por meio de política de antivírus aplicada a um grupo específico. Isso pode ser feito no Console de Gerenciamento, adicionando-se uma nova política ou editando uma política já existente em “Itens em quarentena”, para “Permitir que os computadores clientes enviem os itens em quarentena automaticamente para um Servidor de Quarentena”.

Mais detalhadamente, a Central de Quarentena é um sistema complexo desenvolvido para interligar dinamicamente os usuários e a empresa Symantec, com o intuito de agilizar as respostas para os novos vírus que surgem diuturnamente. Esse sistema possui os seguintes componentes:

- O Security Response, que centraliza na empresa Symantec a análise automática das amostras, verificando e analisando os dados enviados pelos usuários. O Security Response também é responsável por criar e distribuir novas definições de vírus;
- O Gateway, também na Symantec, que é o intermediário entre o Security Response e a Quarentena central do usuário. O Gateway possui um repositório das novas definições de vírus que agiliza as respostas aos usuários, pois as amostras recebidas dos usuários somente serão repassadas ao Security Response caso não possam ser reparadas no gateway.
- O Console de Quarentena, que faz ligação entre o usuário com o Gateway da Symantec para receber as atualizações de definições de vírus. Também é usado para efetuar as configurações das operações do Servidor de Quarentena;

- O Servidor de Quarentena é quem recebe os arquivos infectados e efeitos colaterais dos servidores e clientes da rede, repassando-os ao Console de Quarentena, que os repassará ao Gateway, caso não consiga repará-los com as novas definições de vírus que recebeu anteriormente da Symantec;
- O Agente da Quarentena é o dispositivo que controla a comunicação entre o Console de Quarentena e o Gateway, para que o usuário tenha as definições mais atualizadas do Gateway;
- O Verificador da Quarentena verifica as amostras que chegam ao Servidor de Quarentena antes que possam ser enviadas ao Gateway da Symantec; e, por fim,
- O Defcast: Componente que verifica a seqüência das definições de vírus dos servidores e clientes da rede. Trabalha em conjunto com o Agente de Quarentena.

A Quarentena Central é importante porque faz com que o usuário do Endpoint Protection interaja dinamicamente com a Symantec, acelerando a descoberta de novos vírus e a produção das respostas.

A principal deficiência dos programas de antivírus é justamente o intervalo de tempo que decorre entre o surgimento de uma nova praga virtual até a produção de uma resposta adequada. Com esta perspectiva, é fácil perceber que o receio que normalmente existe em automatizar a remessa de dados potencialmente sigilosos do usuário à Symantec cede espaço à necessidade de mais rapidez no combate ao vírus de computador, o que torna a Quarentena Central um recurso extremamente válido e importante disponível à empresa. Na Câmara Municipal de Londrina, a Quarentena Central foi implementada.

5.3.2 Servidor Live Update

O LiveUpdate é um utilitário do Symantec Endpoint Protection que efetua atualização dos computadores clientes com as mais recentes definições de antivírus, assinaturas de detecção de instruções e correções do produto.

O LiveUpdate em computadores clientes não gerenciados normalmente está configurado para obter as atualizações diretamente dos servidores da Symantec, via conexão da internet.

Nas redes onde os computadores clientes são gerenciados, o LiveUpdate obtém as atualizações do Servidor de Gerenciamento, pois esta configuração é padrão após a instalação do Servidor Endpoint.

Em redes de grande porte onde os computadores clientes são gerenciados, podem ocorrer problemas com a largura de banda nos gateways de Internet. Neste caso, é possível instalar um ou mais servidores LiveUpdate que receberão (em momento pré-agendado) as atualizações para, em seguida, repassá-las aos demais computadores da rede.

O Guia de instalação do LiveUpdate traz uma boa definição desta ferramenta, reproduzida abaixo, em tradução livre²⁷:

“O Administrador de Atualizações da Symantec é um programa para redes corporativas que possibilita o gerenciamento de atualizações em múltiplos servidores centrais, chamados centro de distribuições. Usando o Administrador de Atualizações da Symantec, é possível baixar as atualizações para uma pasta específica, e então encaminhá-las para os servidores de atualizações para que

²⁷ “The Symantec LiveUpdate Administrator is an enterprise Web application that allows you to manage Symantec updates on multiple internal Central LiveUpdate servers, called Distribution Centers. Using the Symantec LiveUpdate Administrator, you download updates to the Manage Updates folder, and then send the updates to production distribution servers for LiveUpdate clients to download, or to testing distribution centers, so that the updates can be tested before they are distributed to production. You can download and distribute updates on schedule, allowing you to create a low maintenance, reliable system that can be set up once, and then run automatically. Updates can also be manually downloaded and distributed as needed”. In SYMANTEC. **Symantec LiveUpdate Administrator 2.2 Getting Started Guide**. Cupertino: Symantec, 2009, p. 7.

os clientes da rede possam baixá-los, ou para um centro de testes de distribuição para que as atualizações possam ser testadas antes de serem distribuídas. É possível agendar as atualizações e distribuições, o que permite uma baixa manutenção, devido a um sistema confiável que pode ser configurado uma única vez para funcionar automaticamente. As atualizações também podem ser feitas manualmente e distribuídas conforme necessário.”

Na Câmara de Londrina, o servidor LiveUpdate foi testado, mas não foi implementado, uma vez que o Servidor de Gerenciamento tem respondido a contento à demanda de atualizações dos computadores da rede.

As principais funções e configurações do servidor LiveUpdate podem ser encontradas no Guia do Usuário²⁸, que acompanha o software do Endpoint.

²⁸ SYMANTEC. **Symantec LiveUpdate Administrator 2.2 User's Guide**. Cupertino: Symantec, 2009.

CONCLUSÃO

O presente estudo iniciou-se com o objetivo de identificar o modo de implementação da solução Symantec Endpoint Protection em rede de computadores corporativa com ambiente Windows, por meio de outros objetivos específicos que era descobrir como implementar o Endpoint Protection e como utilizar os seus principais recursos, além de identificar as principais características capazes de minimizar a inexperience dos usuários da rede.

Num primeiro momento, fez-se uma descrição da rede e dos usuários, cujas características suscitaram algumas preocupações de ordem técnica ao combate a vírus de computador. Depois, foram analisados o produto Endpoint, desde a sua aquisição, com as características próprias de licenciamento e obtenção do *software* e documentação. Seguiu-se, então, a identificação dos passos para a instalação dos recursos do Endpoint, bem como dos requisitos para a instalação. Por fim foi feita a análise dos principais recursos disponíveis, tanto ao administrador da rede quanto ao usuário do computador cliente.

Levando-se em consideração a experiência prática com o Symantec Endpoint Protection na Câmara Municipal de Londrina, foi possível extrair algumas conclusões, sendo a principal delas a de que o recurso de gerenciamento de antivírus permite uma melhor performance no combate a vírus de computador, bem como a outras pragas digitais encontradas na rede mundial de computadores, a internet.

Foi possível instalar todos os clientes sem que houvesse qualquer percalço ou solução da continuidade dos serviços e, o que é melhor, sem que isso fosse sensível ao usuário do computador.

Verificou-se, também, que o Endpoint possui um *firewall* que se revelou mais eficiente que o firewall do Windows XP e Windows Vista.

Quando se implementou o Endpoint e se limitou os direitos dos usuários, retirando deles os direitos de administrador do computador local, verificou-se que a contaminação por vírus imediatamente baixou a quase zero na Câmara, transcorrendo a maior parte do mês de agosto de 2010 sem que se detectasse uma única ocorrência sequer. Isso era inimaginável antes da instalação do Endpoint Protection, pois era comum a contaminação diária em algum computador da rede.

Conclui-se, portanto, que os objetivos foram alcançados, e pode-se dizer que, com este estudo, existe na empresa o conhecimento necessário para a implementação do Symantec Endpoint Protection sem impacto aos usuários, os quais, em sua maioria, sequer sabem da existência do antivírus no computador que utiliza, uma vez que o administrador do Servidor de Gerenciamento do Endpoint tem ferramentas que permitem a ele combater o vírus comandando ações remotamente nos computadores clientes, todos executados silenciosamente.

Ressalta-se que esta pesquisa apresenta contribuições para a ciência, na medida em que detalha a implementação e o uso de uma solução tecnológica, servindo, inclusive, de referência quanto a dados coletados num caso concreto. À comunidade acadêmica destaca-se a abordagem do tema – gerenciamento de antivírus em rede – relativamente novo, apresentado sob um método de pesquisa válido. À sociedade fica o testemunho da eficácia na adoção de medidas combativas de pragas virtuais como incentivo para a adoção de ferramentas específicas disponíveis no mercado. Por fim, em contribuição para o desenvolvimento da tecnologia, a abordagem acadêmica da pesquisa tem o condão de disseminar a idéia adotada na solução Symantec, de sorte que outras empresas e instituições percebam a necessidade de investir em pesquisas para o surgimento de novas tecnologias, proprietárias ou não, que combatam eficientemente as pragas virtuais que atacam as redes de computadores diuturnamente.

REFERÊNCIAS

SYMANTEC. Guia de Instalação do Symantec Endpoint Protection e do Symantec Network Access Control. Cupertino: Symantec, 2009.

_____. **Guia de Administração do Symantec Endpoint Protection e do Symantec Network Access Control.** Cupertino: Symantec, 2009.

_____. **Guia do Cliente do Symantec Endpoint Protection e do Symantec Network Access Control.** Cupertino: Symantec, 2009.

_____. **Guia de Implementação do Symantec Central Quarantine.** Cupertino: Symantec, 2009.

_____. **Introdução ao Symantec Endpoint Protection.** Cupertino: Symantec, 2009.

_____. **Symantec LiveUpdate Administrator 2.2 Getting Started Guide.** Cupertino: Symantec, 2009.

_____. **Symantec LiveUpdate Administrator 2.2 User's Guide.** Cupertino: Symantec, 2009.

MINASI, Mark; ANDERSON, Christa; SMITH, Brian; TOOMBS, Doug. **Dominando o Microsoft Windows 2000 Server.** São Paulo: Person Education, 2001.

TANENBAUM, Andrews. **Redes de computadores.** Rio de Janeiro: Campus, 2003.