

VAI TRÒ BẢO MẬT THÔNG TIN TRONG CHÍNH PHỦ ĐIỆN TỬ

Trình bày: Đỗ Anh Tuấn - TP. Dự Án

Nội dung



Giới thiệu sơ lược về Sunmedia

.....



Vai trò bảo mật thông tin trong chính phủ điện tử

.....



Giải Pháp bảo mật hạ tầng- Sunmedia

.....



Tóm lược

.....

INTRODUCTION

✓ *SUN MEDIA được thành lập ngày 03 tháng 05, 2007.*

✓ *Hiện có trụ sở chính tại TP. Hồ Chí Minh và hai chi nhánh tại Hà Nội và Đà Nẵng.*



✓ *SUN MEDIA là nhà phân phối cung cấp hàng đầu các giải pháp truyền thông tích hợp như*

- *Hệ thống Hội nghị truyền hình,*
- *Âm thanh hội nghị,*
- *Data Center,*
- *Hạ tầng công nghệ thông tin,*
- *Phần mềm ứng dụng...*

Lĩnh Vực Kinh Doanh

Tích Hợp Hệ Thống

- Hệ thống An Ninh Mạng
- Hệ Thống Trung Tâm Dữ Liệu (Data Center)
- Hệ Thống Hạ Tầng Công Nghệ Thông Tin
- Hệ thống camera giám sát

Truyền Thông Hợp Nhất

- Xây dựng hệ thống hội nghị truyền hình
- Hệ thống cung cấp dịch vụ VoIP
- Hệ thống tổng đài, Call Center, Asterisk

SUN MEDIA

Dịch vụ Chuyên Nghiệp

- Dịch vụ thay thế tạm thời các thiết bị phần cứng, sản phẩm.
- Dịch vụ Managed Service
- Dịch vụ IT Outsourcing
- Dịch vụ bảo hành, bảo trì, hỗ trợ kỹ thuật

Phát Triển Phần Mềm

- Phần mềm doanh nghiệp
- Phần mềm ứng dụng trên nền Web
- Phát triển các trang Web cao cấp và thiết kế đồ họa
- Những ứng dụng phần mềm Client - Server

Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

KHÁCH HÀNG (Khối Chính Phủ)

❖ *Projects:*

INFORMATION & COMMUNICATION DEPARTMENT OF:

Gia Lai
Province

Dak Lak
Province

Can Tho
Province

Long An
Province



Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

KHÁCH HÀNG

❖ *Retails:*



Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>



Giới thiệu sơ lược về Sunmedia

.....



Vai trò bảo mật thông tin trong chính phủ điện tử

.....



Giải Pháp bảo mật hạ tầng- Sunmedia

.....



Tóm lược

.....

CNTT là 1 trong 4 trụ cột phát triển chính phủ điện tử



**An toàn, bảo mật thông tin
là một trong 3 nhân tố trong xu hướng phát triển CPĐT.**

New Trend



Report conducted confidentially by IDG Vietnam



Survey: ☒
Excellent: ☐
Good: ☐
Fair: ☐
Poor: ☐

Source: Research Unit – IDG Vietnam

Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

Định hướng UDCNTT năm 2013 tại các Bộ, ngành hướng dẫn giải pháp đảm bảo an toàn thông tin



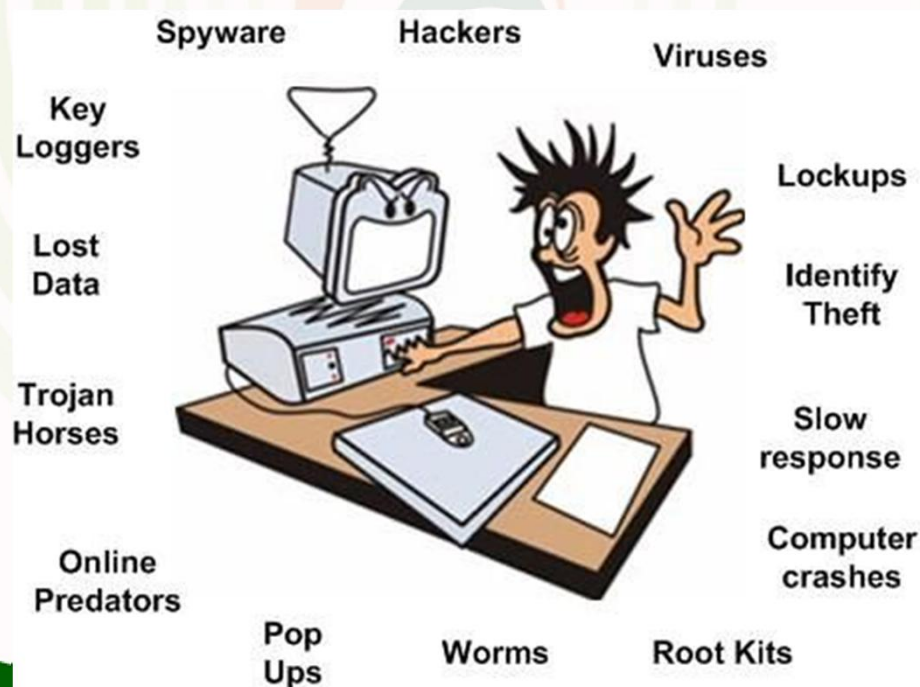
- **Hệ thống thư điện tử và HTTT quản lý VB&ĐH:**
 - ✓ Bảo đảm tối thiểu 35% văn bản, tài liệu chính thức trao đổi giữa các CQNN được trao đổi hoàn toàn dưới dạng điện tử.
 - ✓ Quán triệt thực hiện Chỉ thị số 15/CT-TTg.
- **Cổng/trang thông tin điện tử:**
 - ✓ Bảo đảm 80% các cơ quan quản lý nhà nước (cấp Cục hoặc tương đương) có cổng/trang thông tin điện tử cung cấp đầy đủ thông tin
 - ✓ Cung cấp được ít nhất 20% số dịch vụ công được ưu tiên cung cấp mức độ 3.
- **Triển khai các hệ thống thông tin chuyên ngành:** Ưu tiên triển khai các hệ thống thông tin chuyên ngành trên diện rộng, tạo nền tảng cho các ứng dụng CNTT
- **Triển khai ứng dụng các giải pháp bảo đảm an toàn thông tin:** Tăng cường triển khai QL ATTT theo Tiêu chuẩn quốc gia TCVN ISO/IEC 27001:2009; sd chữ kí số,...
- **Đào tạo nguồn nhân lực CNTT đặc biệt về ATAN TT,** quản lý đầu tư

(nguồn Bộ TTTT 2012)

ATTT đặt ra nhiều thách thức với CPĐT

Số liệu thống kê 2011:

- Chỉ có 35% cơ quan, tổ chức đã xây dựng và áp dụng chính sách ATTT.
- Các Cổng/Trang thông tin điện tử của cơ quan Nhà nước còn tồn tại nhiều lỗ hổng, chưa áp dụng những giải pháp đảm bảo ATTT phù hợp.
- Những vụ việc mất ATTT, vấn nạn thư rác, mất dữ liệu, tấn công xâm nhập gia tăng ở mức báo động về số lượng, đa dạng về hình thức và ngày càng tinh vi hơn.



(Theo ICTnews 2012)

ATTT cần được thực hiện song song với xây dựng CPĐT



Chương trình quốc gia về ứng dụng CNTT trong hoạt động của cơ quan Nhà nước.

ATTT là 1 trong 5 trụ cột để phát triển CNTT:

1. Hạ Tầng
2. Công Nghiệp
3. Ứng Dụng
4. Nguồn Nhân Lực
- 5. ATTT**

“Khi xây dựng CPĐT, ATTT phải được xem xét trên mọi khía cạnh. *ATTT cần được thực hiện song song với xây dựng CPĐT*”

Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

ATTT có ý nghĩa sống còn đối với CPĐT

Ông Đào Đình Khả, GD Trung tâm Chứng thực chữ ký số quốc gia (Cục Ứng dụng CNTT - Bộ TT&TT)

CPĐT buộc phải đặt trên môi trường online để đem lại hiệu quả cao nhất cho Chính phủ và người dân. Cụ thể, trong quá trình hoạt động của CPĐT và tương tác với người dân, nguy cơ bị rò rỉ dữ liệu rất cao bởi những người không có thẩm quyền, vì văn bản phải đi qua rất nhiều server khác nhau. Các hệ thống thông tin, website ngừng hoạt động vì bị tin tặc tấn công, chiếm quyền điều khiển hay dữ liệu bị thay đổi là những nguy cơ mất an toàn thông tin đối với CPĐT. "Vì thế, **ATTT có ý nghĩa sống còn đối với CPĐT**"

(Theo ICTnews 2012)

Vai trò bảo mật thông tin trong chính phủ điện tử

1. CNTT là 1 trong 4 trụ cột phát triển chính phủ điện tử
2. An toàn, bảo mật thông tin là một trong 3 nhân tố trong xu hướng phát triển CPĐT.
3. Định hướng UDCNTT năm 2013 tại các Bộ, ngành: hướng dẫn giải pháp đảm bảo an toàn thông tin
4. ATTT đặt ra nhiều thách thức với CPĐT
5. ATTT cần được thực hiện song song với xây dựng CPĐT
6. ATTT có ý nghĩa sống còn đối với CPĐT



Giới thiệu sơ lược về Sunmedia

.....



Vai trò bảo mật thông tin trong chính phủ điện tử

.....



Giải Pháp bảo mật hạ tầng- Sunmedia

.....



Tóm lược

.....

Các rủi ro về bảo mật, An toàn thông tin



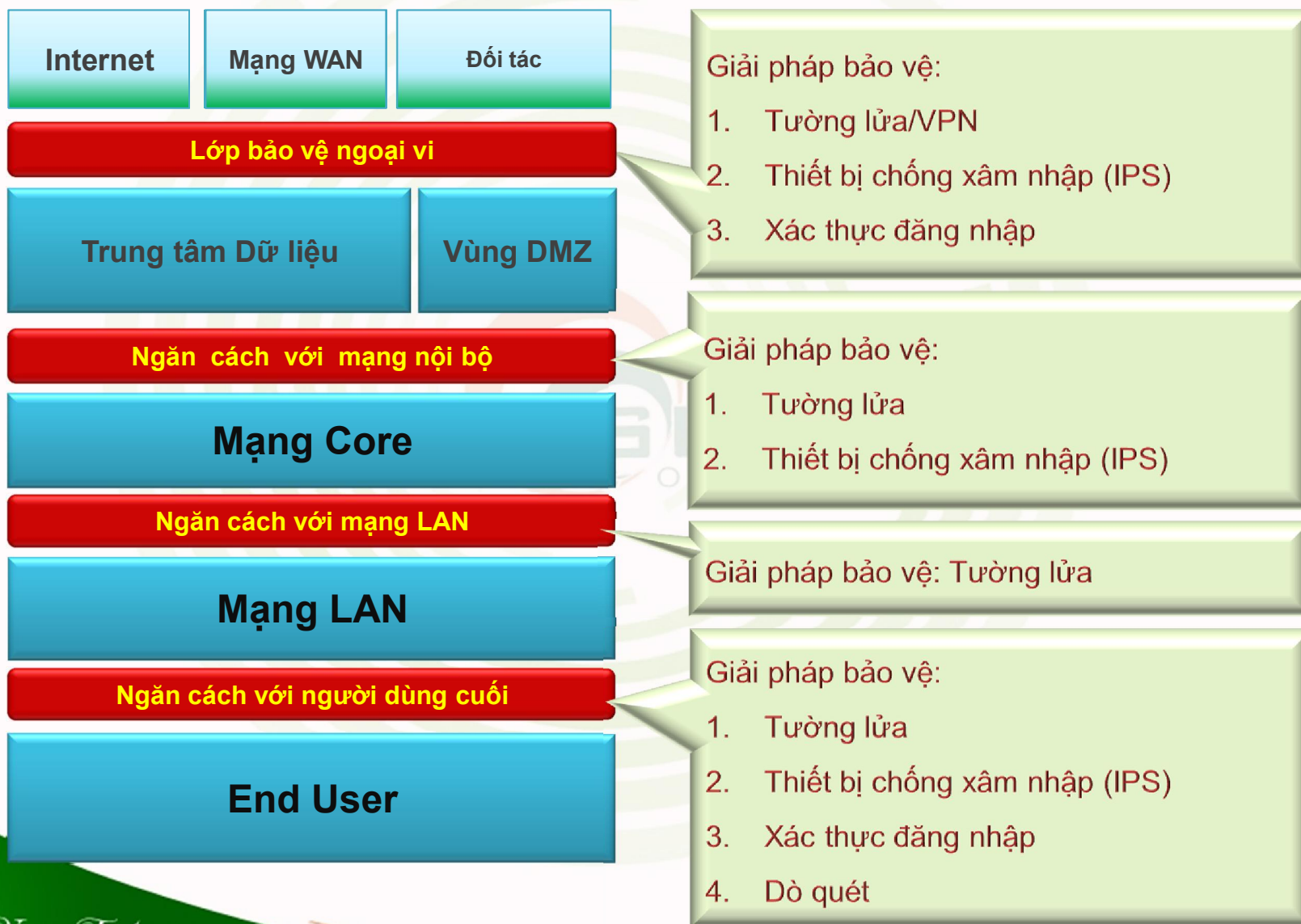
Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

Các rủi ro về bảo mật, An toàn thông tin

KHẢO SÁT TÌNH HÌNH TRIỂN KHAI CÁC HOẠT ĐỘNG ĐẢM BẢO AN TOÀN THÔNG TIN SỐ (ATTTS)	DOANH NGHIỆP HN 109		DOANH NGHIỆP HCM 299		Nhà nước 119		Tổng cộng 527	
11. Các tấn công mà cơ quan/tổ chức của quý vị gặp phải kể từ tháng 1 năm 2011								
Sự xâm nhập hệ thống từ người bên ngoài vào mạng bên trong	26	24%	67	22%	17	14%	110	21%
Sự xâm nhập hệ thống từ những người bên ngoài nhưng nắm rõ bên trong (ví dụ: do nhân viên cũ còn giữ mật khẩu, ...)	3	3%	32	11%	4	3%	39	7%
Xâm nhập hệ thống bởi người trong tổ chức (ví dụ: từ máy để bàn bên trong mạng xâm nhập trái phép vào máy chủ, ...)	8	7%	21	7%	3	3%	32	6%
Hệ thống nhiễm phải trojan hay rootkit (những mã độc hại - malware không tự lây lan được)	44	40%	72	24%	46	39%	162	31%
Hệ thống nhiễm phải virus hay worm (những mã độc hại - malware tự lây lan)	58	53%	109	36%	53	45%	220	42%
Các kiểu tấn công làm suy giảm hiệu năng mạng (ví dụ: dò quét (scan) mạng với cường độ cao gây quá tải)	14	13%	34	11%	32	27%	80	15%
Tấn công từ chối dịch vụ (DOS)	27	25%	28	9%	17	14%	72	14%
Thay đổi diện mạo, nội dung website (trang chủ)	4	4%	37	12%	9	8%	50	9%
Phá hoại dữ liệu hay hệ thống (ví dụ: cố tình xóa dữ liệu quan trọng, ...)	6	6%	21	7%	5	4%	32	6%
Không gặp phải tấn công nào	32	29%	97	32%	29	24%	158	30%

Khuyến cáo mô hình cần bảo vệ



Giải pháp nào cần thiết cho bạn?

KHẢO SÁT TÌNH HÌNH TRIỂN KHAI CÁC HOẠT ĐỘNG ĐẢM BẢO AN TOÀN THÔNG TIN SỐ (ATTT)	DOANH NGHIỆP HN 109		DOANH NGHIỆP HCM 299		Nhà nước 119		Tổng cộng 527	
IV. <u>Biện pháp kỹ thuật thông dụng nhất</u>								
25. Theo như quản trị hệ thống của tổ chức quý vị (hay chính là quý vị), tổ chức của quý vị đang sử dụng các công nghệ đảm bảo ATTT nào?								
Bộ lọc chống thư rác (Anti-Spam)	77	71%	156	52%	55	46%	288	55%
Phần mềm chống virus (Anti-Virus)	103	94%	234	78%	112	94%	449	85%
Chứng chỉ số, chữ ký số (Digital Certificate, Digital Signature)	29	27%	89	30%	15	13%	133	25%
Mạng riêng ảo VPN	42	39%	130	43%	36	30%	208	39%
Mã hoá (Encryption)	28	26%	110	37%	35	29%	173	33%
Đặt mật khẩu cho tài liệu	38	35%	94	31%	42	35%	174	33%
Hệ thống phát hiện xâm nhập (IDS) trên máy chủ	29	27%	89	30%	27	23%	145	28%
Hệ thống phát hiện xâm nhập (IDS/IPS) trong mạng	26	24%	70	23%	31	26%	127	24%
Tường lửa (Firewall)	83	76%	176	59%	91	76%	350	66%
Công cụ đánh giá tính toàn vẹn của tài liệu	1	1%	10	3%	6	5%	17	3%
Sinh trắc học (Biometrics, ví dụ kiểm tra vân tay, ...)	3	3%	13	4%	7	6%	23	4%
Thẻ thông minh, mật khẩu dùng 1 lần (One-time-password (OTP), ...)	3	3%	33	11%	6	5%	42	8%
Mật khẩu có thể được sử dụng lại (Reusable password)	12	11%	23	8%	10	8%	45	9%
Kiểm soát truy cập (Access Control, ví dụ thẻ ra vào phòng máy chủ, ...)	30	28%	85	28%	24	20%	139	26%
Lọc nội dung Web	26	24%	78	26%	33	28%	137	26%
Hệ thống quản lý log file (Log Management)	39	36%	86	29%	58	49%	183	35%
Hệ thống quản lý sự kiện an ninh (SIEM- Security Incident & Event Management)	10	9%	26	9%	7	6%	43	8%
Hệ thống quản lý mật khẩu đặc quyền	11	10%	32	11%	13	11%	56	11%
Hệ thống quản lý chống thất thoát dữ liệu (Data Loss Protection)	10	9%	29	10%	5	4%	44	8%
Quản lý danh tính (Identity Management)	12	11%	29	10%	16	13%	57	11%
Dò quét đánh giá an ninh mạng	12	11%	40	13%	19	16%	71	13%
Dò quét đánh giá an ninh ứng dụng	11	10%	30	10%	15	13%	56	11%
Quản lý bản vá (Patch Management)	34	31%	41	14%	35	29%	110	21%
Khác	5	5%	8	3%	3	3%	16	3%

Giải pháp nào cần thiết cho bạn? (VD tham khảo)



Kiểm soát truy cập: Thiết lập cơ chế kiểm soát chứng thực người dùng nhiều vòng trước khi cho phép truy cập vào hệ thống. Không chỉ giới hạn trong việc xác thực người dùng, Đơn vị còn triển khai hệ thống NAC (Network Admission Control) Cisco để kiểm soát mọi máy tính truy cập vào hệ thống mạng. Các máy móc thiết bị kết nối mạng chưa đảm bảo các tiêu chuẩn về mặt an ninh (do đơn vị quy định) đều bị chặn lại hoặc cô lập và thông báo với người quản trị.

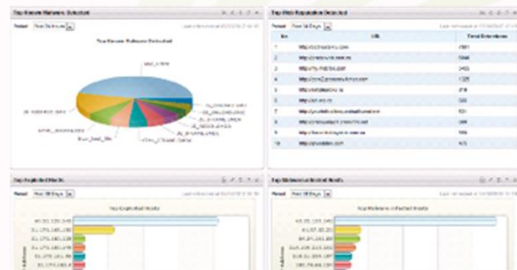
Firewall: Hiện đơn vị có hơn 100 firewall các loại được triển khai ở vùng core banking, vùng ngân hàng điện tử và tại các chi nhánh tạo ra các vùng biên giữa các hệ thống để hạn chế và giám sát luồng thông tin giữa các hệ thống, ngăn chặn các kết nối bất hợp pháp. Các firewall được sử dụng và triển khai hiệu quả với các chính sách kết nối khắt khe nhằm đảm bảo an toàn hệ thống.

Giải pháp nào cần thiết cho bạn? (VD tham khảo)



- Lọc nội dung: sử dụng các công cụ phần mềm lọc bỏ và cấm các truy xuất vào các nguồn thông tin hoặc tài liệu không thích hợp cho công việc.
- Xây dựng các hệ thống phòng chống và phát hiện xâm nhập.
Các hệ thống quét Virus, antispyware, antispam...
- Thực hiện các cơ chế mã hoá thông tin, xây dựng hạ tầng PKI.
- Thường xuyên dò tìm, phát hiện lỗ hổng hệ thống.
- Thiết lập hệ thống cung cấp bản vá lỗ hổng bảo mật.
- Xây dựng cơ chế dự phòng và phục hồi hệ thống đảm bảo tính liên tục của hệ thống.

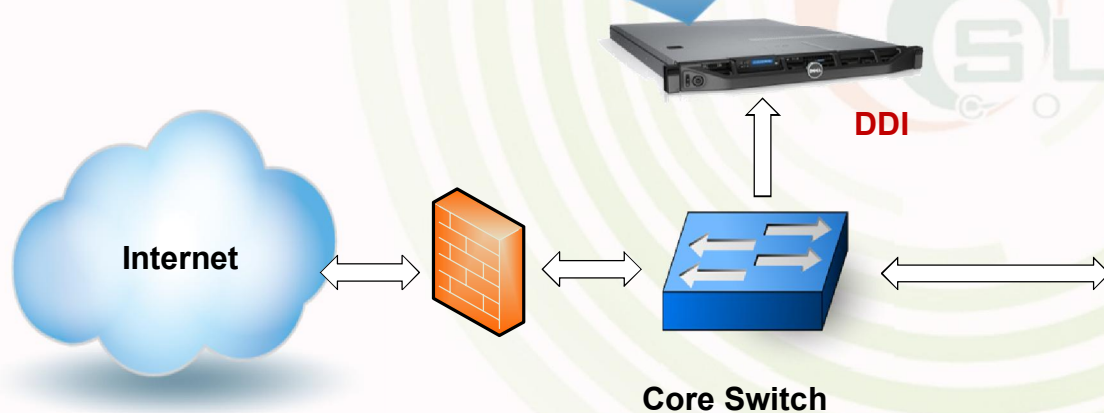
Dịch vụ: Đánh giá hạ tầng bảo mật



Phân Tích, Báo cáo

Đánh giá hạ tầng bảo mật thông qua:

1. Giám sát lưu lượng mạng
2. Phát hiện threat thông minh
3. Phân tích và báo cáo thời gian thực



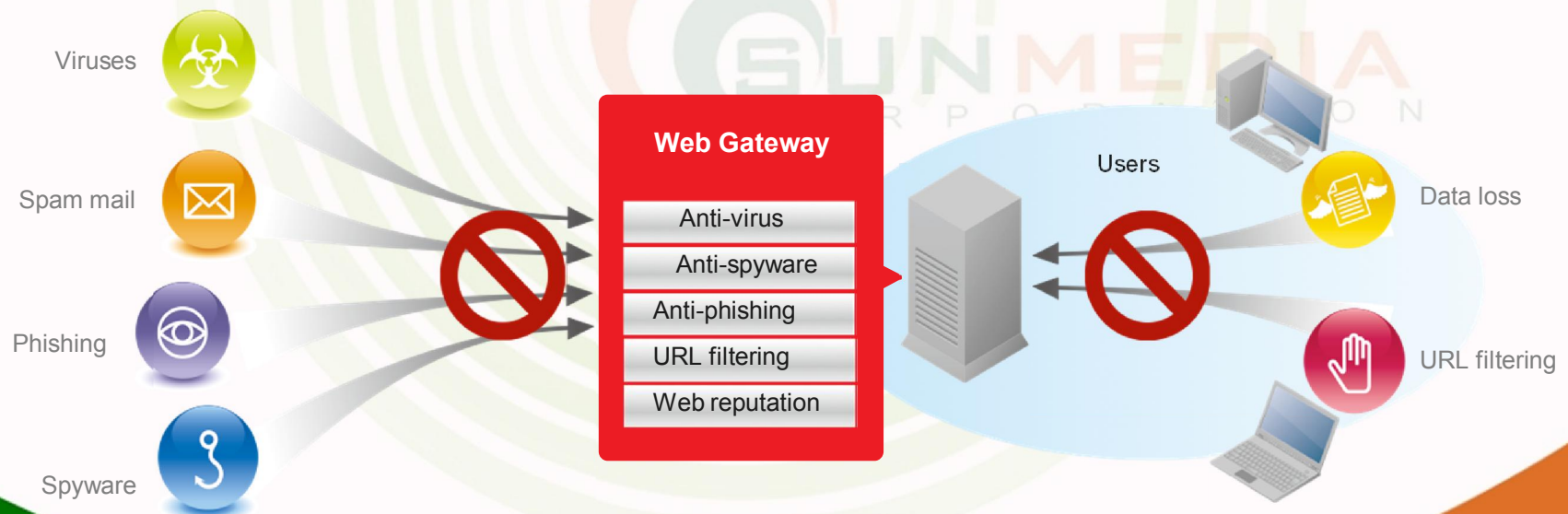
Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

Giải Pháp: Web Gateway

Web Gateway lọc chặn Virus, Spyware, Phishing, trước khi chúng có thể thâm nhập vào hệ thống, ngăn chặn nguy cơ mất dữ liệu.

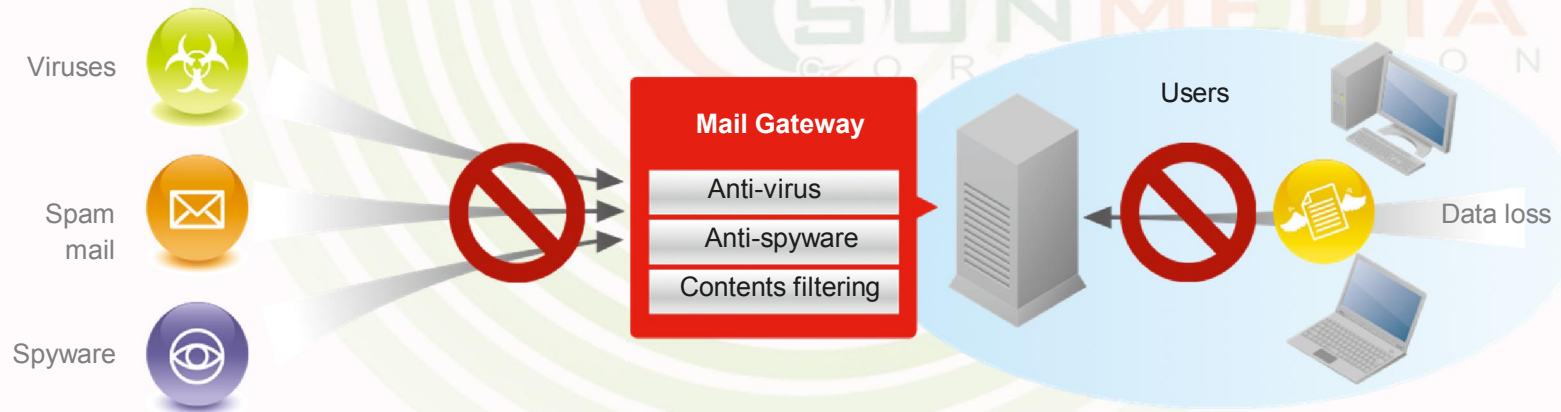
Web Gateway tự động bảo vệ chống lại các mối đe dọa web khi người dùng truy cập internet. Bằng cách kết hợp với điều khiển ứng dụng, quét phần mềm độc hại, kiểm tra web reputation theo thời gian thực, lọc URL, và phát hiện chống botnet, Web Gateway bảo vệ mạng của doanh nghiệp khỏi các mối đe dọa từ Internet.



Giải Pháp: Mail Gateway

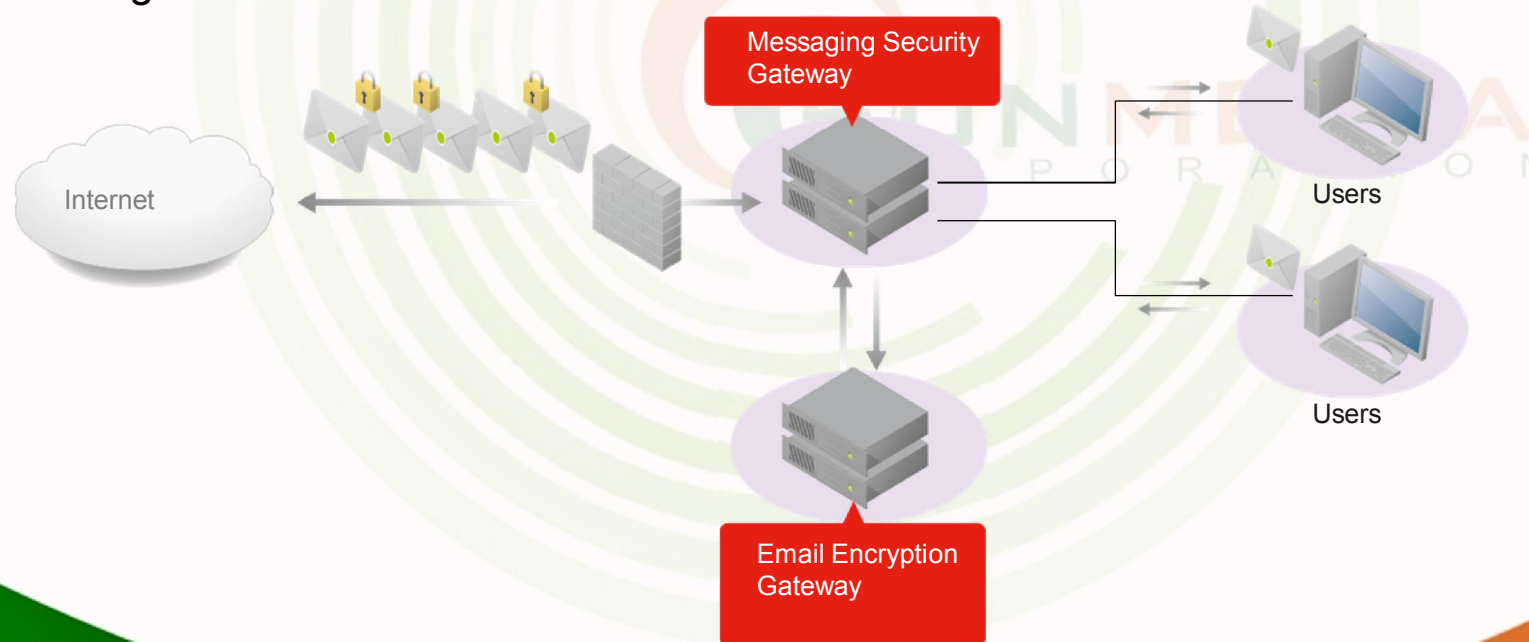
Mail Gateway lọc chặn Virus, Spam mail, Spyware trước khi chúng có thể thâm nhập vào hệ thống của bạn.

Mail Gateway được tích hợp khả năng phòng chống thư rác nhiều lớp và chống lừa đảo (anti-phishing) sử dụng bộ lọc mã độc và phần mềm gián điệp. Khả năng lọc nội dung (content filtering) của Mail Gateway giúp doanh nghiệp dễ dàng thiết đặt các chính sách kiểm soát việc tuân thủ CNTT của người dùng và ngăn chặn rò rỉ dữ liệu



Giải Pháp: Mã hóa Mail Gateway

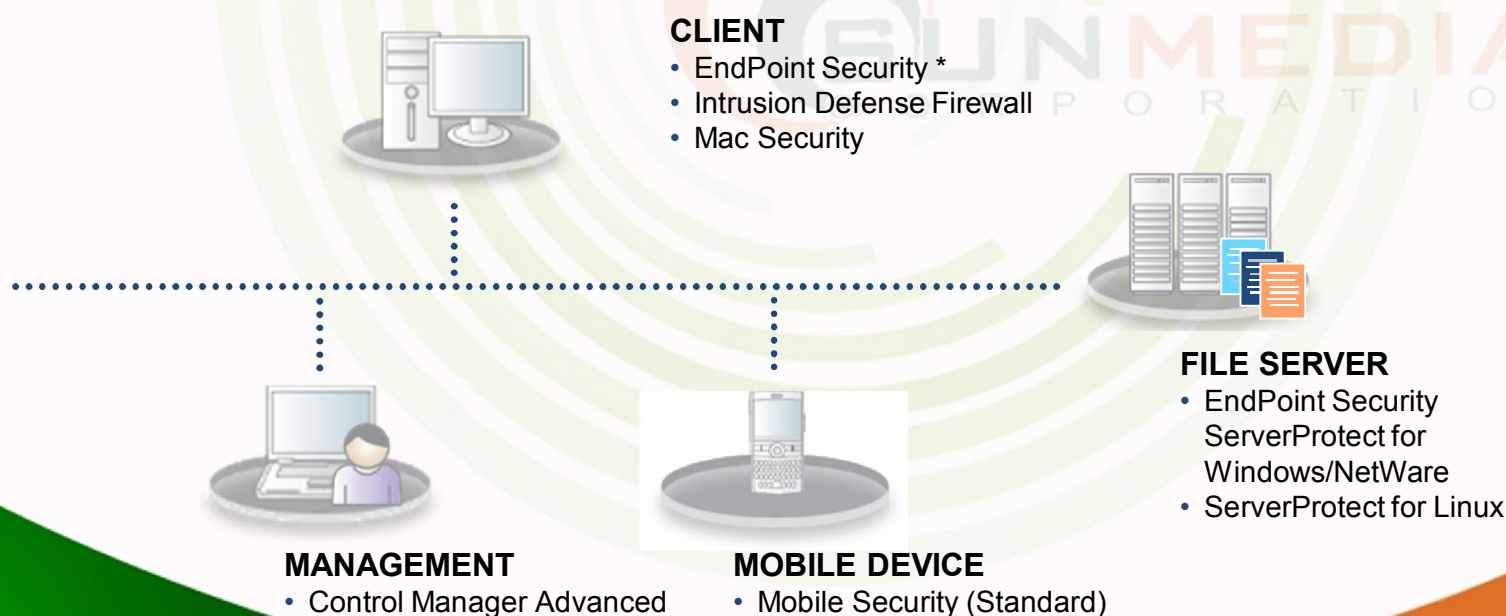
- Email Encryption Gateway cung cấp giải pháp mã hóa tích hợp với hạ tầng mail sẵn có, giải pháp cung cấp khả năng triển khai và quản trị đơn giản.
- Email Encryption Gateway giải pháp đơn giản bảo vệ mail quan trọng khi gửi ra bên ngoài tổ chức



Giải Pháp: Security for Endpoint

Lợi ích của giải pháp **Security for Endpoint**

- Ngăn chặn virus trên các máy trạm
- Khả năng chống bùng nổ virus trong mạng nội bộ
- Khả năng kiểm soát việc truy cập Web của Client
- Khả năng quản lý tập trung toàn bộ hệ thống phòng chống virus
- Khả năng ngăn chặn Client truy cập tới các trang web “độc hại” trên Internet

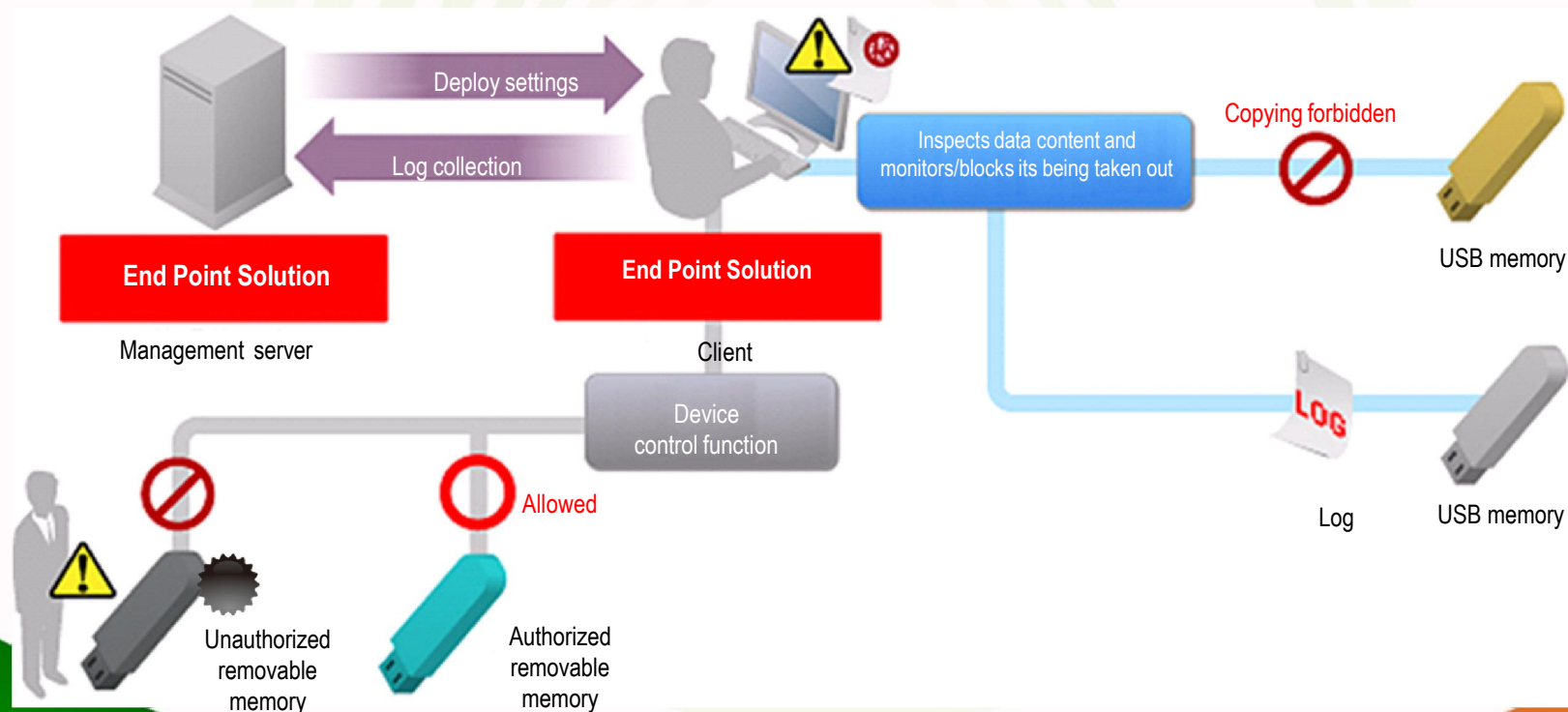


Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>

Giải Pháp: Kiểm soát thiết bị ngoại vi (Device Control)

Lợi ích của giải pháp: Kiểm soát được thiết bị ngoại vi nào được phép sử dụng trong đơn vị hay tổ chức. (có thể chặn việc ghi dữ liệu lên thiết bị ngoại vi, ngăn chặn mất dữ liệu quan trọng)



Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>



Giới thiệu sơ lược về Sunmedia

.....



Vai trò bảo mật thông tin trong chính phủ điện tử

.....



Giải Pháp bảo mật hạ tầng- Sunmedia

.....



Tóm lược

.....

Lời Kết



“Chính phủ điện tử không phải và không bao giờ là một cuộc dàn trận về công nghệ. Sự đầu tư đồng loạt về công nghệ phải là khâu cuối cùng...”, “việc thay đổi tư duy, từ tư duy điều khiển sang tư duy phụng sự, nô bộc và hướng đến xây dựng một dịch vụ công hoạt động hiệu quả hơn dành cho người dân thực sự rất quan trọng. Các bạn sẽ không bao giờ có được chính phủ điện tử nếu không thay đổi được tư duy căn bản này.”

(Ông Mel Blunt từng là cố vấn cao cấp của Chính phủ về Cải cách hành chính, đồng thời là Cố vấn kỹ thuật cao cấp Chương trình phát triển Liên Hợp Quốc tại Việt Nam)

Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>



Trân trọng cảm ơn

Set Up Your Future

Website : <http://www.smediavn.com> , <http://www.smedia.vn>