



Eric Ogren

92 Robert Road

Stow, MA 01775

m: 978-618-9240

eric@ogrengroup.com

Lumension: a Case Study in Proactively Managing Endpoint Risk

An Ogren Group Security Business Analysis

March 2009

Executive Summary

The Ogren Group, an industry analyst and research firm formed to help virtualization and security vendors find success in the market, found that EC Suite, a major processor of credit card transactions for e-commerce organizations, saved considerable time and effort in their IT and security operations as a direct result of their preventive security measures and procedures using Lumension solutions.

As a credit card processor, security is at the top of the list of IT concerns for EC Suite. The company's team of security experts is challenged to apply best of breed products to protect a global company encompassing 380 employees, over 450 computers, and 7 data centers. The company achieves this level of productivity with an integrated effort of security and IT organizations to proactively prevent attacks that can result in loss or theft of consumer credit card data, and to aggressively manage the patching of vulnerabilities before a security event can disrupt the business.

It is the integrated approach to preventing malicious code from exploiting a vulnerability and executing code that compromises systems and steals confidential data that is the real cost savings here. EC Suite's preventive security measures and procedures led them to aggressively meet the following challenges:

- **EC Suite security did not feel confident that signature-based anti-virus products were sufficient to prevent malicious code from executing in the EC Suite network.** EC Suite, having deployed Lumension Endpoint Protection™ and Lumension Data Protection™ to its Microsoft Windows devices, is blocking roughly one zero day malicious code attack per month before the attack can spread through the network. This reduces the risk of sensitive data loss and of disruption to business productivity. *EC Suite estimates a monthly savings in recovery operations of a significant 50 hours per month.*
- **EC Suite's overall preventive security effort in removing vulnerabilities could not be maintained as the business grew.** EC Suite's prior solution for managing vulnerability patching required heavy IT involvement such as testing patches, packaging patches for deployment, verifying that patches were applied to 100% of the infrastructure, and different approaches were needed for Unix and Windows platforms. Lumension Vulnerability Management™ has streamlined the effort and the timeliness of ensuring compliant endpoint configurations. *EC Suite manages endpoint risk with approximately 25% of the resources they would need without Lumension – a savings the Ogren Group estimates as two full time employees.*
- **EC Suite's previous vulnerability management solution frequently left up to 20% of patched devices inoperable.** With Lumension Vulnerability Management, EC Suite has minimized the number of devices that IT must manually fix due to problems arising after patching. *For EC Suite, this annually saves approximately \$100 per protected device.*

The key business return findings are:

- **258.3%** rate of return in the first year
- **964.0%** average rate of return over three years
- **6-9 month** payback period

This Ogren Group Security Business Analysis has been commissioned by Lumension. This Security Business Analysis offers a quantifiable study of the business benefits realized by EC Suite in their use of Lumension solutions. The security business analysis includes time and expense savings over competing approaches, as well as less qualitative improvements in security coverage. The Ogren Group conducted multiple interviews with decision makers at EC Suite and Lumension in researching material for *EC Suite: a Case Study in Proactively Managing Endpoint Risk*. More information on the methodology used to develop this report can be found in the Appendix.

EC Suite: team approach to proactive security

EC Suite is best recognized as a major processor of credit card transactions for Internet oriented e-commerce organizations, with associated business lines in shared hosting, dedicated hosting, co-location and content delivery services. The company's high transaction volume, driven by thousands of websites and millions of page hits per day, places EC Suite among only 330 Tier 1 businesses as classified by the Payment Card Industry (PCI) . The very nature of the EC Suite business makes security a competitive differentiator and elevates security to a boardroom issue.

Some of the challenges that EC Suite faces on a daily basis range from Trojan downloaders, spyware, and intentional or unintentional information leakage. A breach resulting in disclosure of customer credit card data or a major disruption in high performance credit card processing services could lead to a disastrous loss of business to EC Suite. The company's IT and security teams have responded to the security challenges with a proactive approach to protecting the EC Suite infrastructure and information, partnering with Lumension to reduce the risk of a significant security incident.

EC Suite operates its business on a dynamic network of approximately 450 computers. A staff of 380 employees is supported by seven processing centers distributed world-wide, with its major facilities in Phoenix, Boston, and Malta. The enterprise is a thriving business built upon secure, high performance processing for Internet-oriented organizations.

Of special interest is the integrated process followed by security and IT teams to preserve a continuously compliant infrastructure. The Ogren Group rarely sees this high level of coordination and cooperation between internal departments. The integrated process, with a foundation in Lumension Endpoint Protection, Lumension Data Protection, and Lumension Vulnerability Management for the entire EC Suite infrastructure, allows EC Suite to expand its business without compromising security. Security is a "bet your business" proposition for EC

Suite, and the security and IT teams proactively meet those security challenges. The process begins with receipt of patches from Lumension:

1. The security team performs comprehensive vulnerability assessment research to determine the risk level and applicability of each patch based on EC Suite's particular requirements. Patches that do not apply to the EC Suite environment are simply discarded.
2. The security team adjusts application controls with Lumension Endpoint Protection to prevent exploits identified in the patches from running. Endpoint Protection identifies the presence of unauthorized software, such as new code embedded by malicious activity, and blocks its execution without knowing specifics about the attack. Updating the whitelist for Endpoint Protection is necessary to keep the fingerprints of authorized software up to date.
3. EC Suite IT applies the patches that have passed through the security team filters. IT tests the patches on selected machines before broadly deploying the patches throughout the business.

The corporate sensitivity to maintaining a secure business environment has led EC Suite to Lumension. Lumension Endpoint Protection preserves approved configurations while beating back malicious attacks, Lumension Data Protection protects against confidential data being copied onto removable media, and Lumension Vulnerability Management plugs vulnerabilities that could undermine the integrity of the endpoint. **Using Lumension solutions, EC Suite can complete distribution of priority patches and endpoint application control policies within three days, which the Ogren Group considers impressive performance.**

Lumension: preventive security

Lumension offers security solutions for enforcing enterprise policies for the protection and control of the server and endpoint computing infrastructure. Lumension solutions are utilized by IT and security teams to control and maintain software configurations to ensure a compliant business infrastructure, prevent unauthorized changes to IT-approved configurations, and protect against data leakage via malicious software, applications, and removable devices.

The primary elements of EC Suite's preventive security program leverage an integrated Lumension solution suite focused on setting and maintaining IT-approved configurations, and controlling changes to those compliant configurations. The specific Lumension solutions that form the core of EC Suite's preventive security initiative are:

- **Lumension Vulnerability Management** – ensures that endpoint software configurations are compliant, and takes the costs out of applying patches to remediate vulnerabilities. IT centrally manages approval and distribution of software patches to reduce the company's exposure to financial and business risk due to malware penetration.
- **Lumension Endpoint Protection** – applies whitelisting capabilities to ensure that the endpoint only runs approved software. Any executables that do not appear on the

Endpoint Protection whitelist, such as day-zero attacks that sneak by signature defenses, are not allowed to run. Targeted attacks or malware that can result in leakage of sensitive data or disruption of the business are also denied by default.

- **Lumension Data Protection** –is utilized by EC Suite to monitor and control the movement of sensitive data onto removable media devices, including USB sticks, mobile phones, and MP3 players. Unauthorized devices and unauthorized data transfers are prevented with detailed auditing providing insight into what data is being written to and from removable devices. In a business where protecting consumer credit card information is everything, Lumension assists IT in enforcing data use policies and protecting against confidential data walking out the door.

Costs

Enterprises will experience one-time acquisition costs for Lumension software and servers to administer the proactive security solutions. Enterprises will also have ongoing annual maintenance charges for solution upgrades and technical support as well as subscription fees for the automated patch services.

The Ogren Group uses the following values in derivation of expenses and cost savings for this Security Business Analysis:

- EC Suite issues 4 to 7 patches every 1 to 2 weeks. For this analysis, the Ogren Group will use an average of 3 patch sessions per month, 36 patch sessions per year.
- There are 22 work days per month; 264 work days per year. At 8 hours per day, this yields 2,112 work hours per year.
- **EC Suite estimates a fully loaded security team member cost of \$70,000 per year bringing the hourly rate of security and IT team members to \$33.**
- Numbers have been rounded to the nearest \$100 to enhance readability.

Hardware

EC Suite drives the Lumension solution from 2 production servers, with an additional 2 servers in a test lab that can be used in production if required for business continuity. These servers are typically Quad-Core processors with 2Gb of memory and 30Gb of storage. **Servers of this class cost roughly \$900 apiece for a total of \$3600 hardware acquisition costs.**

Lumension software

EC Suite purchases software licenses and maintenance contracts from Lumension to proactively protect their business infrastructure. Enterprises pay a one-time license fee for software installed on protected computers.

EC Suite also purchases an annual subscription service to ensure delivery of product patches throughout the year, as well as a maintenance contract for technical support services and product upgrades. Subscription fees and maintenance contracts are ongoing expenses for the life of the solutions.

Lumension Vulnerability Management licenses	\$20,200
Lumension Endpoint Protection and Data Protection licenses	\$25,700
Total Lumension software licenses	\$45,900
Total Lumension annual maintenance subscriptions	\$11,200

Lumension Endpoint Protection – keeping up to date

Lumension Endpoint Protection features a whitelist approach where only approved applications are allowed as a means of thwarting day zero attacks. Instead of a long list of attack signatures that anti-virus products feature, Lumension Endpoint Protection operates on a shorter list of applications that are allowed to run.

The list of permitted applications has to be updated at each patch session, which is an incremental effort performed by the security team and is thus considered an incremental expense. Whitelists need to be updated whenever a patch modifies the fingerprint of an approved application. EC Suite expends approximately 4 person-hours per patch cycle maintaining the whitelist.

Hours required to update whitelist per patch session	4 hours
Number of patch sessions per year	36
Total hours updating whitelist per year	144
Total annual expense for updating Lumension Endpoint Protection whitelist	\$4,800

Benefits

Cost savings due to patch quality

EC Suite’s experience with a competing product from a major vendor was that approximately 20 machines required manual attention after patches were applied, at a cost of 2 hours per touched machine. Lumension saves EC Suite 40 person-hours of effort for each patch operation due to the quality of the patch process.

Hours saved due to patch quality	40 hours
Number of patch sessions per year	36
Total hours saved due to patch quality	1440
Total annual cost savings due to patch quality	\$48,000

Cost savings due to blocking attacks

Lumension Endpoint Protection has sharply reduced the number of security incidents attributable to malicious code. According to EC Suite, Lumension Endpoint Protection, which ensures that an endpoint can only run approved executables, has been blocking roughly one zero day attack per month. EC Suite’s security team estimates that the proactive security approach to blocking attacks before they can ripple through the business is saving approximately 50 hours per month.

Number of zero day attacks blocked per month	1
Hours saved due to blocking attacks per month	50 hours
Total hours saved due to blocking attacks per year	600
Total annual cost savings due to blocking attacks	\$19,800

Cost savings due to headcount

EC Suite estimates that with Lumension Endpoint Protection, Lumension Data Protection, and Lumension Vulnerability Management they maintain their technical infrastructure with approximately 25% of the effort they used with a competing vendor's solution, **resulting in a headcount savings of roughly 2 full time employees**. This is a substantial savings in operational expenses gained by Lumension technology that provides EC Suite:

- The ability to manage a diverse collection of Unix and Windows machines from a single Lumension management console. The same preventive security solutions are used for production, office, and development environments reducing operational efforts in testing, packaging, and distributing patches.
- Greater assurance that 100% of EC Suite's endpoints are compliant with the most up-to-date patches to close vulnerability gaps, updates for approved applications, and controls for sensitive data usage.
- Reduced cycle time to deploy patches received from Lumension. EC Suite receives operating system and application patches from Lumension. EC Suite experience shows IT and security teams require less testing per patch, minimal packaging of patches for distribution, and far fewer system refreshes after problematic patches.

Cost savings due to integrated data protection

EC Suite internal requirements are to restrict access to removable devices, such as USB sticks, smart phones, and MP3 players, to only those employees with an expressed business need. The preventive security policy denies access for unauthorized usage, and further ensures that all authorized usage is transparently encrypted to prevent data loss. Lumension Data Protection is included in the suite of products deployed by EC Suite. Including Lumension Data Protection in the suite of products saves EC Suite the costs of purchasing additional device control software and special security-enabled USB memory sticks. The Ogren Group estimates the incremental costs would have been \$80 per each of the 100 employees granted permission to access removable devices.

Number of affected employees	100
Est. cost of software and memory stick	\$80
Total cost savings due to integrated data protection	\$8,000

Cost savings due to reduction in help desk calls

EC Suite’s help desk was receiving approximately 15 endpoint attack-related help desk calls per week before deployment of Lumension Endpoint Protection. The end-user initiated help desk calls were often legitimate problems with system performance or troublesome software installations. Since most of the help desk calls were based on a legitimate problem, EC Suite IT and security would spend an average of one hour responding to each call and correcting the problem. *Lumension Endpoint Protection has reduced the number of help desk calls to roughly four per week, a savings of 11 help desk calls per week.*

Fewer number of help desk calls due to Lumension Endpoint Protection	11 calls per week
Estimated time spent per help desk call	1 hour
Total hours saved due to reduction in help desk calls	520 hours
Total annual cost savings due to reduction in help desk calls	\$18,900

EC Suite Security Business Statement

The Security Business Statement shows an impressive 258.3% rate of return in the first year for EC Suite’s investment in Lumension, with a 964.0% average rate of return over the first three years of the solution. The year-over-year cost savings of over \$226,700 are derived from a relatively pain-free vulnerability patch process with high quality patches, unique integration of application control whitelisting technology with data protection that prevents new attacks from penetrating the network and data leakage via removable devices, and an automated approach to keep security in tune with business requirements. Once the software licenses are purchased, the only annual expenses to offset the impressive cost savings are for subscription service, solution maintenance and whitelist upgrades estimated at \$16,000.

<i>Security Business Statement</i>	
Acquisition cost savings	
Integrated data protection	\$8,000
Total acquisition cost savings	\$8,000
Annual cost savings	
Blocking zero day attacks	\$19,800
No manual corrections of patches	\$48,000
Headcount savings (2 full time employees)	\$140,000
Reduced help desk calls	\$18,900
Total annual cost savings	\$226,700
Acquisition expenses	
Server Hardware	\$3,600
Lumension software licenses	\$45,900
Total acquisition expenses	\$49,500
Annual expenses	
Lumension software maintenance	\$11,200
Endpoint Protection Solution whitelist update	\$4,800
Total annual expenses	\$16,000
Total first year return	\$169,200

EC Suite rates of return

EC Suite generated a 258.3% rate of return in the first year of operations with Lumension solutions. This roughly equates to a six month payback period given time allowed to implement the solution.

Cost savings achieved from using Lumension Endpoint Protection, Lumension Data Protection, and Lumension Vulnerability Management solutions	\$226,700
Less: total acquisition expenses	\$49,500
Less: Total annual expenses	\$16,000
Total year 1 return	\$169,200
Year 1 rate of return	258.3%

Over a three year interval, EC Suite can expect an average rate of return of 964.0%. The key attribute in this calculation is the low year-over-year expense of maintenance and whitelist support, while still realizing the cost savings of reduced headcount, vulnerability management efficiencies, and lost time recovering from malicious attacks.

	Year 1	Year 2	Year 3
Cost savings achieved from using Lumension Endpoint Protection, Lumension Data Protection, and Lumension Vulnerability Management solutions	\$226,700	\$226,700	\$226,700
Cost savings due to integrated data protection	\$8,000	\$0	\$0
Less: total acquisition expenses	\$49,500	\$0	\$0
Less: Total annual expenses	\$16,000	\$16,000	\$16,000
Total annual return	\$169,200	\$191,800	\$191,800
Annual rate of return	258.3%	1317%	1317%
Three year average rate of return	964.0%		

The Ogren Group was conservative in calculating the average rate of return. Increases in salaries or growing the solution with additional endpoints would improve the return. Enterprises are advised to include their own business factors when repeating rates of return for their business environment.

Gains in operational efficiencies

The automated process of blocking attacks and patching vulnerabilities brings operational efficiencies that are difficult to quantify, but are still important considerations in choosing a proactive security program. For example, Lumension improves the cycle time between receipt of a patch and distribution to approximately three days. This enhances the security profile and contributes to fewer successful attacks and fewer calls to the help desk from end-users, but does not directly impact the bottom line. These benefits include:

- **Lessen the risk of confidential data leakage:** Every measure EC Suite can take to keep confidential data, such as consumer credit card information, secure is important to the business. Estimates of financial loss due to leakage of consumer credit card data have cost TJX approximately \$250 million and cost Cardsystems, Inc. its business. EC Suite's preventive measures and processes include controls over unauthorized applications that exploit vulnerabilities to steal data and controls over removable devices such as smart phones, USB flash drives, and MP3 players that can carry confidential data. Of unique importance is the ability of Lumension Data Protection to automatically disable wireless connectivity when the endpoint is physically attached to the network.
- **Least disruptive to the business:** The integration of Lumension's solutions allows IT and security to automate and schedule staged deployments in the off-hours when end-users will not be disrupted. Endpoints and servers are patched and Lumension Endpoint Protection whitelist profiles are updated without end-user assistance to help ensure end-user productivity.
- **Complete coverage of infrastructure:** Lumension Vulnerability Management automates detection of devices and delivery of patches to ensure complete coverage of their technical infrastructure. Prior experiences showed EC Suite with gaps in their vulnerability coverage - IT would manually discover computers that were not patched to a compliant level.
- **Common controls over server and desktop endpoints:** Lumension Endpoint Protection enforces application controls to both Windows servers and desktops. The common management interface reduces training time while allowing EC Suite's security team to customize configuration control policies for classes of server and desktop endpoints.
- **Improved patch cycle time:** The performance of deploying critical patches to all affected machines has improved to three days. Lower priority patches are held, and are easily packaged for distribution when high priority patches are ready. This is attributable to the quality of patches delivered by Lumension, and automated distribution of patches.
- **Treat security as standard operating procedure:** Lumension Vulnerability Management brings operational efficiencies that allow EC Suite to treat patching as a standard business operation. No longer does EC Suite security have to scramble on "Patch Tuesday". High priority patches are deployed in three days, dramatically shrinking the time from vulnerability to exploit; medium and low priority patches are easily added to higher priority patch packages.

- **Confidence in business expansion:** EC Suite's proactive security enables the business to grow without adding large incremental security expenses. IT and security teams automate control over end point configurations and vulnerability patching allowing the business to evolve without burdensome security overhead.
- **Reduce administrative training:** Lumension Vulnerability Management is used for Windows and Linux operating environments, as well as applications such as Adobe and Firefox among others. This consolidation of patch activity makes it easier for IT to deploy patches from a common administrative interface without having to learn additional security management tools.
- **Reduce effort of PCI and GLBA compliance reporting:** EC Suite undergoes twice a year audits for compliance with the Payment Card Industry Data Security Standard and an annual Gramm-Leach-Bliley Act audit for its bank partnerships. Lumension reporting capability documents the coverage of application and data controls within the technical infrastructure simplifying the effort expended by EC Suite in compliance reporting.

Conclusions

The Lumension solution set, as evidenced by EC Suite, makes a compelling business case for an integrated solution of vulnerability management, data protection, and endpoint protection. EC Suite's preventive security approach has yielded a stronger security profile against malicious attacks, reduced overall IT and security operational expenses, and enhanced operational efficiencies. The primary direct savings come from Lumension Endpoint Protection to thwart malicious attacks at the endpoints and Lumension Vulnerability Management to rapidly close vulnerabilities in the infrastructure, while Lumension Data Protection prevents leakage of confidential data that could be ruinous to the business.

The Ogren Group finds that Lumension is a critical partner in EC Suite's preventive security initiative, helping IT and security control the environment against attacks that seek to steal confidential data or can disrupt business processing. In addition to bolstering the security profile, EC Suite's consolidation of endpoint risk management with Lumension is resulting in impressive cost savings. **The Ogren Group *Security Business Statement* makes the payback for EC Suite very clear. For an upfront investment of \$44,500 and annual expenses of \$16,000, the business will save \$207,800 for a first year rate of return of 243.5% and an averaged three year rate of return of 880.3%.** This places the payback period on the order of 6-9 months, and makes managing endpoint risk with Lumension an attractive proposition.

The Ogren Group believes that enterprises should look at automated tools that integrate security and IT functions, such as those offered by Lumension. Adopting preventive security solutions to manage endpoint risk will improve security coverage of all devices in the network and multiple applications, and it will save operational expenses associated with attacks or inferior products. That's a good combination that works for EC Suite.

Appendix: Security Business Analysis

Purpose

Security is notoriously difficult to justify on a financial return basis since security products are seldom tied directly to revenue. This makes operational efficiency metrics and payback cycles more appropriate for security vendors than questionable return on investment calculations.

The Ogren Group Security Business Analysis examines an organization's experiences with a security technology with an eye towards quantifying operational efficiencies and payback durations. More intangible benefits are included to give the reader a full picture of the benefits delivered by the security vendor. It is the goal of this report to enable the reader to envision the technology in their own environment and to understand the benefits possible by aligning security with business processes.

Methodology

The Ogren Group conducted two in-depth interviews of EC Suite personnel to capture their experiences with Lumension technology. The interviews covered organizational responsibilities, impact on operational efforts, and upfront costs.

The Ogren Group interviewed executives of Lumension for detailed product background, corporate strategy, and product pricing information.

Disclosures

- The Ogren Group maintains editorial control over this report and its findings and does not accept changes to the report that contradict Ogren Group research. Lumension has reviewed and provided feedback to the Ogren Group.
- The Ogren Group makes no assumptions as to the benefits that other enterprises will realize. The Ogren Group recommends that other enterprises use their own estimates to estimate the cost savings within their specific environment.
- The Ogren Group Security Business Analysis has been commissioned by Lumension.