FORTRA™

WHITE PAPER (VULNERABILITY MANAGEMENT)

Calculating the Financial Impact of a VM Program

How Fortra Vulnerability Management Solutions Improve Security, Compliance and Operations

Return on investment on IT security infrastructure purchases (solutions and products) has traditionally been hard to quantify. However, there are some compelling aspects of securing an organization's infrastructure that can be identified and quantified. This discipline will continue to evolve as organizations focus on managing and balancing their security expenses and strive to control the accelerating growth in their security investments. This is the necessary next step in the maturing discipline of information security, where the initial focus has been about protection, and where organizations are now striving to optimize security and minimize risk to the business at the least possible cost.

These changes are the next evolution in a security environment that continues to evolve. Enterprises have continued to increase their reliance on their IT networks for most business processes and for housing every component of business critical information (financial information, supply chain details, customer information, intellectual property, etc.) This is in addition to being the communication channel by which the enterprise operates and communicates with customers, partners and internally. This shift toward corporate and global network usage is driven by numerous factors that fundamentally improve an organization's ability to conduct business in a more efficient and effective manner, with a lower cost of operations.

This increasing reliance on corporate and global networks is in an environment where the volume of reported vulnerabilities that can introduce security risk is growing. Important to note is that resulting network threats are becoming more sophisticated, emanating from well-funded organizations interested in extracting maximum financial benefit or inflicting maximum economic damage. This new breed of threat is driven by attackers that are well-armed with business knowledge, willing to aim for longer term impacts and have global reach, presence and ability to evade authorities.

Regulatory oversight has increased dramatically, and organizations are still feeling the pressure to implement and pay for the ongoing audits of their internal process controls. While network security controls are a component of overall compliance, they remain a very important point of scrutiny because of the widespread use of an enterprise's IT network and the implications of weak controls on the operations, business continuity and market value and customer perception.

Typically, enterprises employ a variety of security tools. Overall these investments have tended to be reactive products that have helped identify and alert when there are issues, but have done little to take a proactive approach to helping enterprises measure, manage and reduce their network security risk, in an operationally effective way.

Fortra has taken a proactive approach to security risk and compliance management, and is an innovator and leader in the market.

Fortra's solutions help organizations answer these important questions:

- How secure and compliant is our network?
- Which top issues must we address today to improve security and achieve compliance?
- Who is accountable and how are they doing?

The following table highlights some areas of consideration in cost justifying an enterprise-class security risk and compliance management solution.

VULNERABILITY MANAGEMENT BUSINESS IMPACTS

Issue	Fortra Provides the Capability to:	Supporting Facts	Financial Impact
Comprehensive network discovery and risk prioritization	• Maintain a continuous profile of all networked devices on the network • Determine the most vulnerable applications and areas of highest risk • Identify what should not be on the network (e.g. rogue devices, unauthorized applications and spyware) • Automate the data collection process without installing an agent on every system	• Fewer than 35% of companies have an accurate accounting of their IT assets[1] • The rate of change in an enterprise network is very high, which introduces new points of risk daily	• Shift from manual process of data collection to automated profiling will save significant time and dramatically increase confidence in results • May be partially measured by reviewing time spent by security and IT professionals investigating, tracking and verifying assets
Information aggregation and reporting	• Report on the enterprise network vulnerability and risk status continuously • Utilize numeric scoring of risk and vulnerabilities, applying the same tolerance across the enterprise • Utilize customer-determined asset values to provide business context to security risk	• In a recent survey, 72% of security professionals reported they did not have an effective way to measure and report on network security risk, and cannot track if their risk is increasing or decreasing over time • Network security remains a top concern of CIOs (per Gartner survey) • Fortra customers use VM reports throughout their reporting processes, including inclusion in Board of Director packages	• Substantial professional and administrative time can be saved with automated reporting • Security effectiveness can be increased with trending over time and improved focus on vulnerabilities and risk • While not quantified, better decisions can be made about where to apply budget dollars based on a risk-based approach to security
Integrated view of security risk and compliance	• A single, integrated view of the entire network's IT security and compliance posture • Reporting for all audiences: executives, security, IT operating and audit teams • A unified scan engine to gather security and compliance data	• Mature, best practice organizations use Fortra's risk scores to drive quarterly bonuses	• An integrated suite of tools that eliminates multiple point solutions is the most efficient and cost effective method to improve security and compliance
Incident handling	• Reduce reactive incident handling with risk based approach to vulnerability remediation	• Over 11,000 vulnerabilities have been reported annually on average for the last three years, coupled with internal incidents reported by staff and security teams identify other issues to be investigated	• Time savings can be measured in the amount of ad-hoc time spent on investigations of new vulnerabilities and their possible enterprise impact • Risk reduction resulting from speed of handling and the ability to determine the true security risk to the enterprise
Remediation	• Provide extensive details about vulnerabilities and remediation or mitigation options with references to 3rd-party advisories • Bi-directional, closed loop ticketing	• Remediation research is a significant time investment for IT teams after a vulnerability is identified for remediation • Most vulnerabilities requires multiple steps to ensure and verify closure	• Significant remediation time can be saved with ticketing process automation in the communication time alone, allowing remediation to begin more rapidly • More importantly, verification of remediation can be automated ensuring the risk is removed and IT teams are effective in remediation actions

COMPLIANCE IMPACTS

Issue	Fortra Provides the Capability to:	Supporting Facts	Financial Impact
Uniform foundation for internal policy and regulatory compliance	• Quantitative risk scoring for each device aggregates to a baseline score for the entire enterprise. With a baseline score established and policy and compliance defined, continuous monitoring for compliance enables both precise and timely compliance management	• With the advent of Sarbanes-Oxley, in many cases reported audit fees have more than doubled and in addition many organizations have incurred significant consulting fees to implement and verify internal control processes • If these processes do not become standard and automated, organizations will continue to pay significant fees for audit time of disparate and manual process • One customer stated they now use 20 percent of the effort in supporting audits than they did prior to using Fortra solutions	• Impact can be measured in time spent preparing for audits, supporting audits with manual or ad-hoc reports, and other audit support on a quarterly and annual basis • Many companies are receiving Management Letter comments from auditors about network security controls, as the pervasiveness and importance of the network continues to expand • Fines are issued for non-compliance with the Payment Card Industry Data Security Standard (PCI DSS)
Automating compliance control objectives	• Many organizations are subject to multiple regulatory requirements with some overlapping requirements—internal policy and control objectives can be set, measured and monitored for reporting to internal and multiple external auditors and regulators	• Organizations have hundreds or thousands of control objectives and if manual process are used or managerial attestation is needed to support audit requirements, this is a significant manpower initiative	• Internal Impact can be measured by the number of control objectives that can be automated multiplied by the time spent manually verifying a control • Audit costs can be reduced by providing auditors with documentation of the control, process and reporting for their verification

OPERATIONAL IMPACTS

Issue	Fortra Provides the Capability to:	Supporting Facts	Financial Impact
Complete view of what is running on the enterprise network	• Maintain a continuous, up-to-date profile of all networked assets on the network	• Fortra customers are able to identify opportunities for application consolidation • Organizations may not know if they are operating within licensed volumes or seats of software	• Man hours saved in not having to patch and maintain multiple versions • Cost avoidance of system downtime • System repair and productivity loss • Organizations may be able to negotiate savings in maintenance if they have not deployed all copies licensed • Organizations can ensure they are only running licensed copies of software, avoiding public announcement and fines
Comparative reporting and trending by ownership of network and IT assets	• Report on vulnerability and risk status by network, asset class, geography or business unit owner	• Fortra customers have seen dramatic improvement in network maintenance by publishing reports on performance by network owner[2] • Organizations utilized Fortra reporting to include security performance in bonus and compensation criteria	• Reduced risk and increased IT efficiency with the information to focus first on the areas of highest risk to the organization for remediation
Standard configuration of new equipment	• Verify pre-production hardening of new servers to standard configurations and not introduce additional risk	• Fortra customers have found some of the key benefits of proper hardening include better performance by disabling unnecessary services, reduced management overhead and downtime as fewer services require fewer patches, and a reduced attack surface • The certification process is now seen as a value added part of the process rather than a burden that may cause provisioning delays[3]	• Reduction in ongoing maintenance costs and a positive culture change regarding security

References

1. Tripwire survey of over 1000 security professionals and management
2. Tripwire USAID Case Study
3. Tripwire Fujitsu Case Study

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

Copyright © Fortra, LLC and its group of companies. Fortra™, the Fortra™ logos, and other identified marks are proprietary trademarks of Fortra, LLC.
(tw-gd-0424-r1-hm)