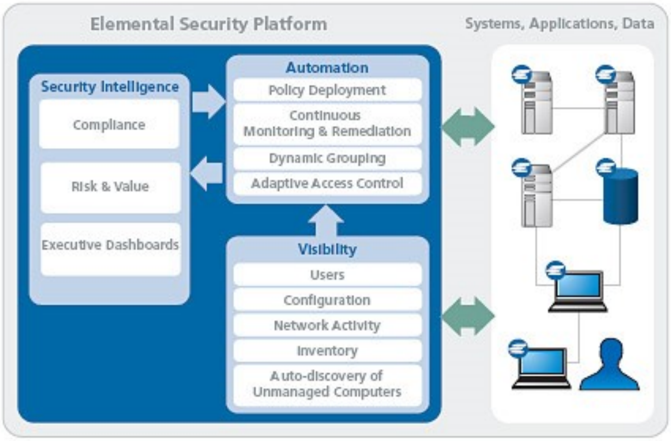
Elemental

ELEMENTAL SECURITY PLATFORM

ENTERPRISE RISK MANAGEMENT

As pressure is mounting to justify spending on IT security, enterprises are confronting persistent and evolving threats as well as increasing internal security breaches. In this environment, assessing cyber risk can present an important capability to help administrators manage security and compliance initiatives in a way that most effectively protects the key interests of the organization. The Elemental Security Platform (ESP) is an innovative highly integrated self-adaptive cyber risk and security policy management solution that fits into any size organization in the cloud or on premise.



ESP is the most functionally integrated enterprise solution that combines security policy and configuration management, security compliance enforcement, as well as risk management capabilities.

The **Risk Metrics Framework** provided by ESP enables security professionals, managers and auditors to make informed decisions about defining and targeting security policies throughout their computing environment to protect critical assets, information and business operations.

At Elemental Cyber Security, we believe that Cyber Risk Management consists of three core components :

- **Value**: understanding the value of assets that comprise the enterprise's computing infrastructure and the associated loss potential of these assets resulting from inadequate or ineffective security control;
- **Metrics**: communicating the security and risk posture of the network environment through business-aligned metrics;
- **Enforcement**: taking measures to mitigate the level of cyber risk.

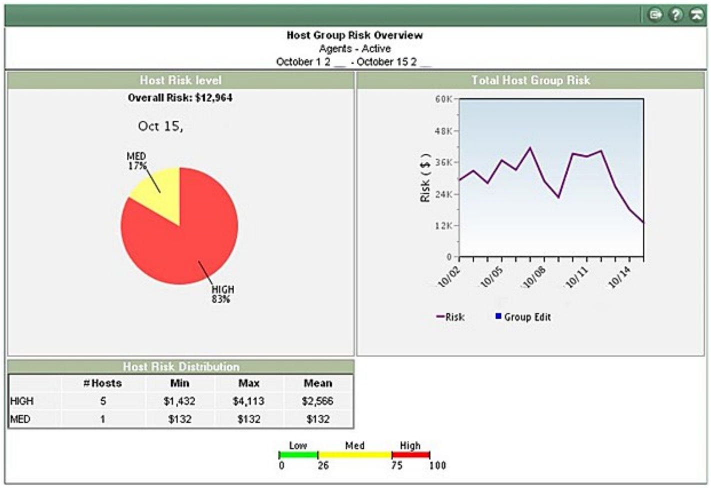
The quantitative risk management capability offered by the **Elemental Security Platform (ESP)** leverages the extensive visibility it provides into the state, security posture, activity, and roles of systems to programmatically assess the value and associated risk of all machines on the network. This includes machines not running the ESP agent. In this way, the ESP enables a fundamental shift in the processes of managing cyber security compliance and adaptive network access controls from a posture of being ***reactive*** to external and internal threats to one that is ***proactive***, internally directed, and aligned with business interests. Elemental's Cyber Risk Management solution represents a maturation within the security marketplace, providing the much-needed context to more fully leverage investments in IT security.

The Cyber Risk Management capabilities provided by the Elemental Security Platform are enhanced through a suite of dashboards and reports that facilitate cross functional organizational communications while creating awareness for business leaders and stakeholders. These tools effectively bridge the communication gaps created through the separation of duties by providing clear, actionable information. Once empowered with an understanding of the level and sources of risk, security professionals and business leaders can make informed decisions on how to best allocate limited resources to mitigate and manage Cyber Risk.

Cyber Risk Management applied in an enterprise

Cyber Risk Management is a key enabling technology that directly supports the processes of managing security compliance and policy-based network segmentation as well as access controls. Some key solution features provided by the ESP include:

- **Identifying critical high-value assets**: Most corporations face the challenge of not even knowing what is on their network, let alone understanding the value individual systems represent to the business. The ESP cuts through this opaqueness, enabling the identification of machines that—based on their properties, activity, or roles—represent significant value. The continuous monitoring provided by ESP further enables this assessment to reflect context variations, exposing the impact of known changes as well as those not expected or not immediately evident.
- **Determining exposure to loss of network assets**: Once the value of assets has been determined, the next step involves gaining a quantitative understanding of their associated loss potential due to security exposures. Ongoing monitoring of the risk of systems identifies those assets that pose the greatest business exposure for an organization.
- **Prioritization & planning of security initiatives**: Security and Compliance management becomes much easier when the fundamentals are known and understood. Rather than addressing each set of compliance requirements—such as SOX, PCI, NIST or HIPAA—as a discreet project, risk awareness coupled with pervasive and enterprise-wide automated security policy management enables enterprise IT management to be strategic in how they implement required security controls. The scope and dynamic nature of enterprise networks has stretched available resources beyond the brink. By using risk and value metrics, available resources and budgets can be directed to those issues that improve security compliance while also having the greatest impact on protecting the assets and infrastructure that are critical to the business



Host Group Risk Overview
Agents - Active
October 1 2 __ - October 15 2 __

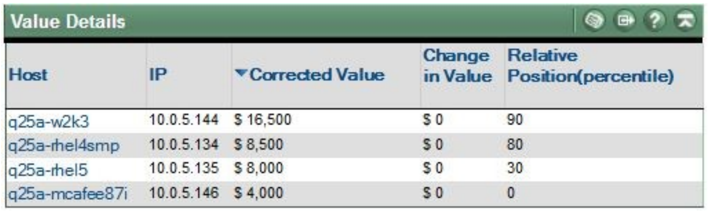
Host Risk level

Overall Risk: $12,964

Oct 15,

Host Risk Distribution

	#Hosts	Min	Max	Mean
HIGH	5	$1,432	$4,113	$2,566
MED	1	$132	$132	$132

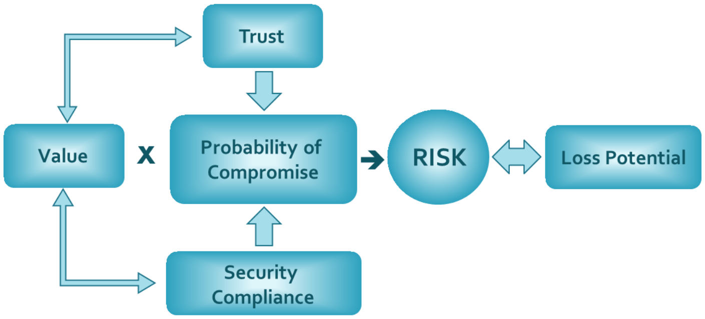


Value Details

Host	IP	▼Corrected Value	Change in Value	Relative Position(percentile)
q25a-w2k3	10.0.5.144	$ 16,500	$ 0	90
q25a-rhel4smp	10.0.5.134	$ 8,500	$ 0	80
q25a-rhel5	10.0.5.135	$ 8,000	$ 0	30
q25a-mcafee87i	10.0.5.146	$ 4,000	$ 0	0

An innovative approach to Cyber Risk Management

The Elemental Security Platform provides automated Risk Assessment correlating value, security compliance and trust relationships of systems. Risk becomes an integral part of the ESP, providing unified oversight and control for security and compliance management. In simplest terms, Cyber Risk can be viewed as a measure of the associated loss potential for a computing system:



The visibility enabled by the ESP provides a rich set of multi-faceted value, trust and security compliance indicators. During its Risk assessment, the ESP is combining for each observed system the following factors:

Value Indicators: System Value is determined by a number of factors—including the type and characteristics of systems, observed networking activity, and the value of the information stored or transacted by and through it. More than simply the intrinsic value of the machine, the indicators of value are closely aligned with a measure of the value an asset represents to the business, and are rooted in the context of the business environment. This means the value indicators are 'tunable' through weighting that best reflects the most relevant factors within specific operational environments. These include:

- Hardware / Software / Devices / Applications
- Documents: context- and age-dependent
- Network Activity – a comprehensive view of the volume and type of both inbound and outbound communications
- Roles – weightings based on the business purpose, location, and importance of systems

Compliance & Trust Indicators: The unified policy framework delivered by the ESP encompasses a wide array of native policy-based controls that traverse the many operational layers of computing devices. In quantifying a measure of the degree of risk to which a system is exposed, the ESP takes into account the system's compliance with its assigned security policies, as well as the compliance of systems it trusts. Collectively, a system's adherence to and conformance with a set of well-written security policies provides a robust and comprehensive methodology for assessing the potential for systems to be compromised or disrupted.

The Bottom Line

The ability to account for the value of systems and the level of risk to which they are exposed enables ESP users to plan and manage their security compliance initiatives from a position informed by security intelligence. Whether implementing policies to protect key information and assets, demonstrating compliance with regulatory requirements, or implementing measures to ensure business continuity, the ESP provides the business-aligned security metrics that serve both the operational efficiency and effectiveness. It also gives business leaders a meaningful assessment of the security and risk posture of their investments in information systems.

www.ElementalSecurity.com