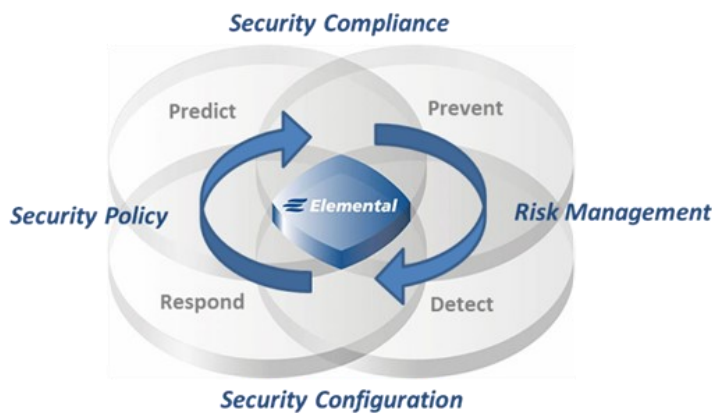


# ELEMENTAL SECURITY PLATFORM

## Cybersecurity Compliance Enforcement Automation System providing protection against internal and external threats

The Elemental Security Platform (ESP) is an advanced enterprise level security compliance enforcement automation system that is suited for any size organization—in the cloud, data-center or on premise. ESP is the game changing policy enforcement driven cybersecurity solution that ensures critical digital assets are continuously in compliance hence always protected. As a highly integrated, fully automated, scalable system the Elemental solution is the answer to effective information security assurance, auditable compliance and risk management. It achieves this through automatic deployment, continuous monitoring and enforcement of cybersecurity policies and controls.



*ESP is the most functionally integrated enterprise solution that combines the four capabilities essential for effective security, policy compliance and risk management*

The Elemental solution is a multifunctional software as a service (SaaS) platform that unifies the key technologies required to effectively govern cybersecurity risk, assess compliance and protect information systems. This comprehensive approach enables organizations to realize their internal cybersecurity and compliance goals by combining:

- ◆ An extensive library of security controls and policy templates
- ◆ Tightly integrated technical security controls governing system configuration, utilization and network access
- ◆ Automated implementation, monitoring, and enforcement of security policies
- ◆ Automatic adaptation to system and network security posture changes
- ◆ Continuous monitoring of system integrity and compliance
- ◆ Measuring and reporting of security posture, compliance, risk, and value of digital assets

### Manage risk with a holistic approach to cybersecurity, compliance and system trust relationships

By automating the many actions required for efficiently managing security policies, the Elemental Security Platform improves effectiveness, reduces costs, and enhances productivity of IT security administration.

The ESP system implements security policies consistently across heterogeneous operating systems and throughout the multiple operational layers of networked computers, easily transposing them from premise or datacenter to the Cloud. It monitors the configuration, usage, network activity, and inventory of all managed machines running the ESP agent, therefore continuously assessing, implementing and adjusting the security posture of these systems by deploying new policies in order to dynamically adapt to changes.



## Key Features

### Security Policy Management

**Automation of security policies** is a key component of the Elemental solution. ESP admin's express and deploy policies simply by selecting from an extensive library of security controls and policy templates. Elemental also makes it simple to define target groups or security zones and automatically apply policies to all hosts in the group. As the activity of hosts and their security posture changes, group membership also changes automatically and the correct policies are applied accordingly, which makes the ESP system dynamically adapt to a changing security context.

**Unified Policy Infrastructure** – ESP offers a unified framework for cross-platform security and regulatory policies spanning network traffic, operating system, users, hardware devices, environments, locations, applications and data.

**Automated Targeting and Deployment** – Dynamic grouping of computers based on ESP admin defined criteria describing the configuration, activity, and inventory of individual machines enable policies to be precisely targeted and automatically updated.

### Security & Regulatory Compliance

Elemental provides the framework to achieve compliance with industry and government regulations, this includes an extensive policy library. ESP ships with several thousand individual controls (rules), plus an extensive array of editable, pre-defined policy templates for:

- ◆ OS and application security baselines: NSA, CIS, NIST, DISA, and Microsoft
- ◆ Regulatory requirements: NIST 800-171&172, SOX, PCI-DSS, HIPAA/HITECH, FISMA (NIST 800-53), GLBA, etc.
- ◆ Security zones—micro segmentation: access controls to regulate network traffic among users, systems, workloads, groups, etc.
- ◆ Security configuration management and activity controls

### Unparalleled Visibility

**Auto-Discovery** – the Elemental agents passively monitor the network for new computers. Unauthorized machines are quickly discovered and classified to identify their operating system, hardware details, and networking activity.

**Network Communications** – detailed traffic information for both managed and unmanaged computers enables administrators to monitor and regulate traffic for systems, applications, users, and network segments.

**Security Configuration** – get an in-depth profile of the operating system, network properties, application settings, and system configuration parameters.

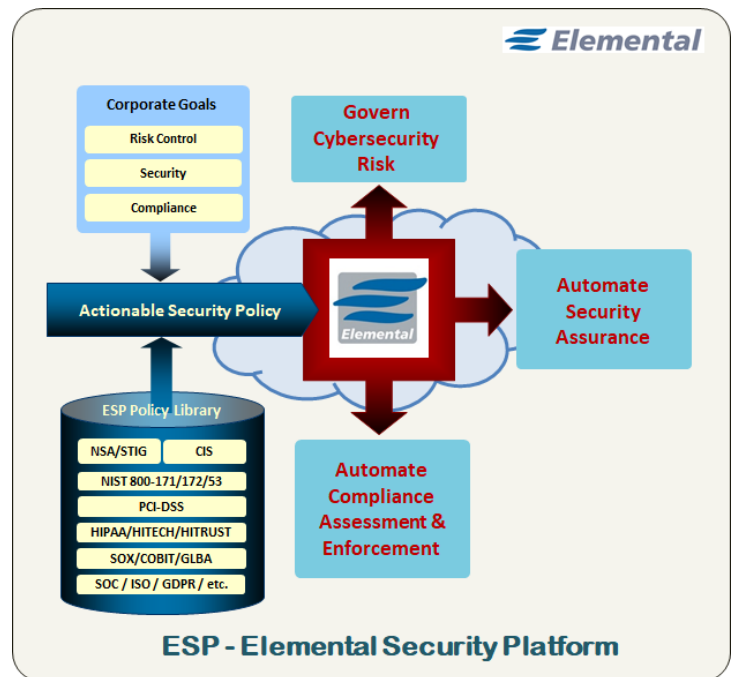
**Users and Accounts** – accounts and user logon activity are tracked by ESP enabling implementation of policies based on user roles and entitlements.

**Hardware and Software Inventory** – the Elemental agent gathers a detailed summary of devices, installed applications, running processes and services.

### Protect Critical Resources

**Identify and Contain Unauthorized Systems** – Integrated host-level access controls ensure access is denied—whether these unauthorized systems are unknown systems discovered on the network, or known ones that have fallen out of compliance with required policies.

**Layered Protection** – ESP provides highly targeted, granular, and always-on host level access controls that ensures only secure and authorized systems are granted access to critical resources.



### Elemental Security Operations Center

The Elemental Web based Console is the central control point for security policy management, dynamic policy target group definition, compliance and risk monitoring, as well as reporting. Policy deployments are precisely targeted, automatically deployed, and continuously updated. The ESP enables administrators to import groups from directory services (Active Directory) or to specify groups of computers based on their common characteristics, network behavior, security and risk posture, or user activity.

The Elemental system provides extensive reporting capabilities, including a suite of executive dashboards, detailed views and histories of compliance, risk and value, network traffic activity, and trouble ticket administration. The ESP reporting makes it easy for administrators to document the state of their networked systems and to identify changes that occur on individual systems or in the communications among systems.

### Risk Management

The ESP programmatically determines the value and risk of machines based on a myriad of observed characteristics, roles, behavior, and usage information. The ESP quantifies the value and risk of all machines on the network, both managed and unmanaged, through the analysis of multiple factors including compliance, trust, system properties, the type and volume of networking activity, stored information, as well as the roles of machines and users. This capability identifies high value and at-risk systems enabling organizations to identify, mitigate, and manage IT risks.

### The Bottom Line

ESP is a multifunctional, affordable SaaS solution leveraging next-generation technologies to provide tremendous value to security professionals:

- Improves the efficiency of security and IT staff
- Unifies visibility across IT security controls
- Supports the shift from end-point and disparate tools to a holistic and adaptive integrated solution
- Reduces network attack surface through 'always-on' adaptive network access control and micro-segmentation
- Provides automatic security posture assessment and adjustment
- Provides business aligned metrics to demonstrate and enforce cybersecurity compliance