



Elemental Cyber Security

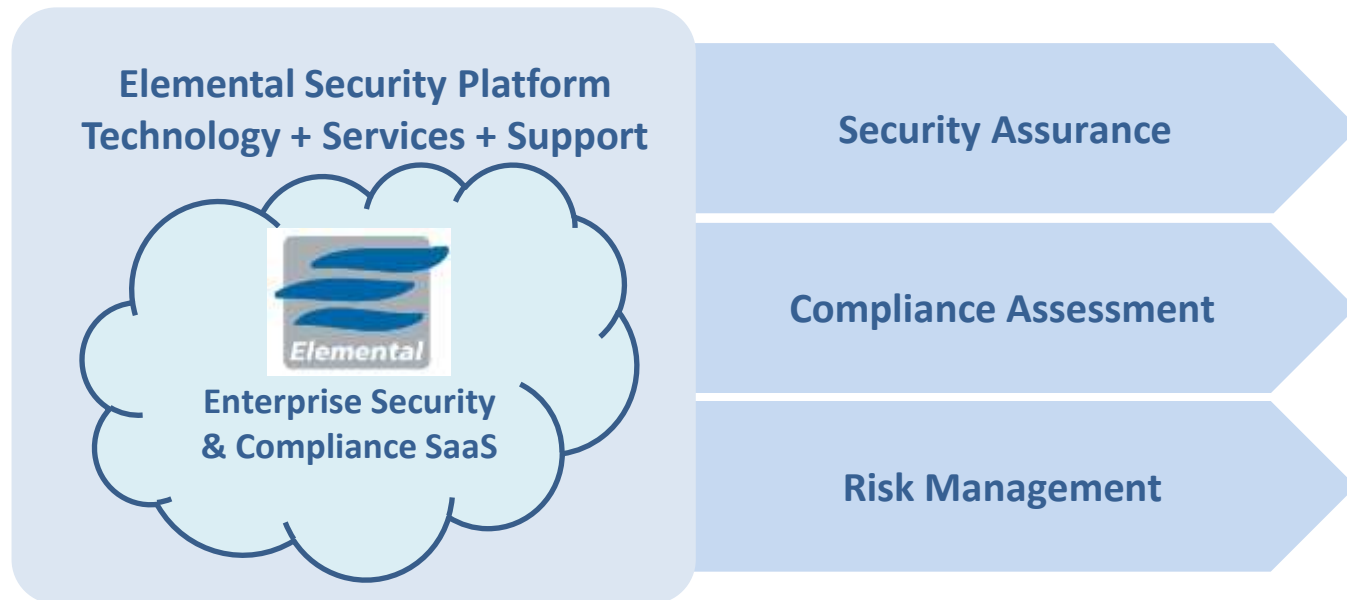
**Brings Cyber Security Assurance & Automation
to any cyber Risk and Compliance initiative!**

ESP Solution Technical Features

by Marius O. Bratan

Marius.Bratan@elementalsecurity.com

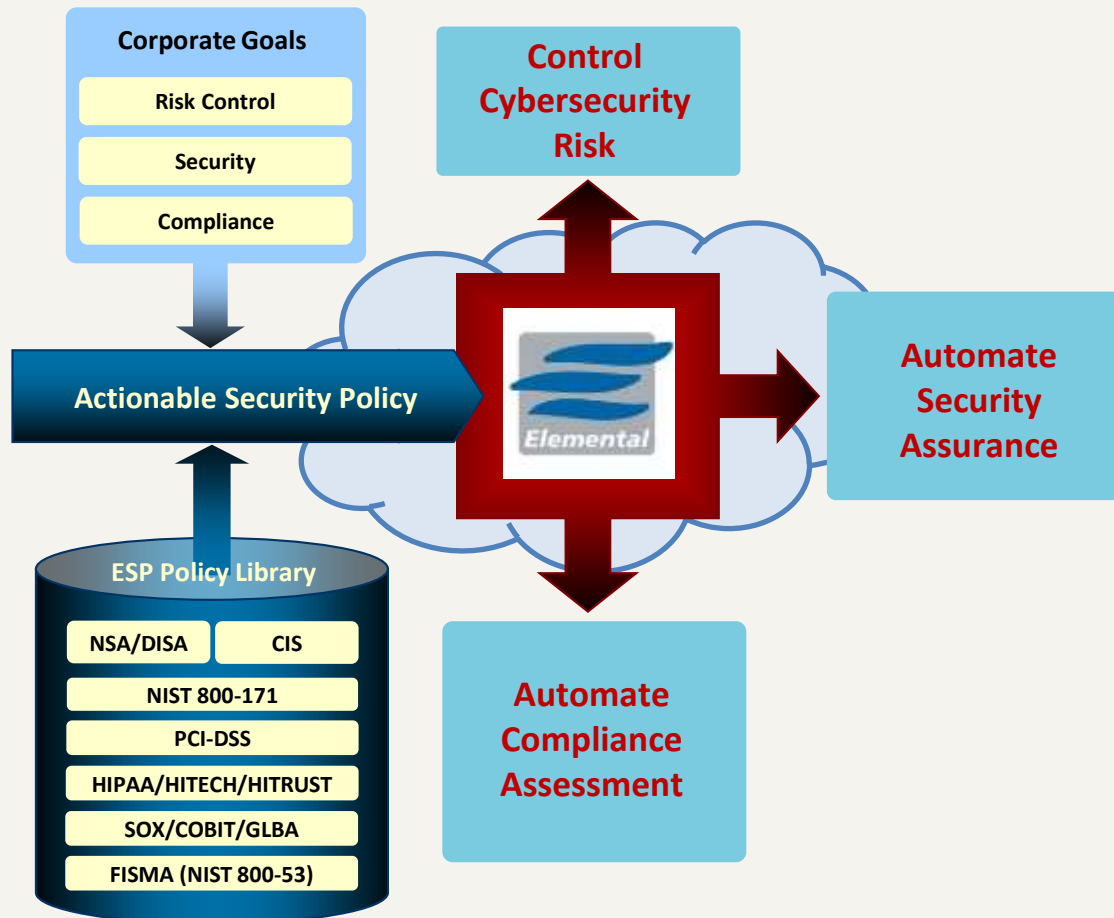
Elemental Cyber Security Platform



Bring Automation & Security to any cyber Risk and Compliance initiative!

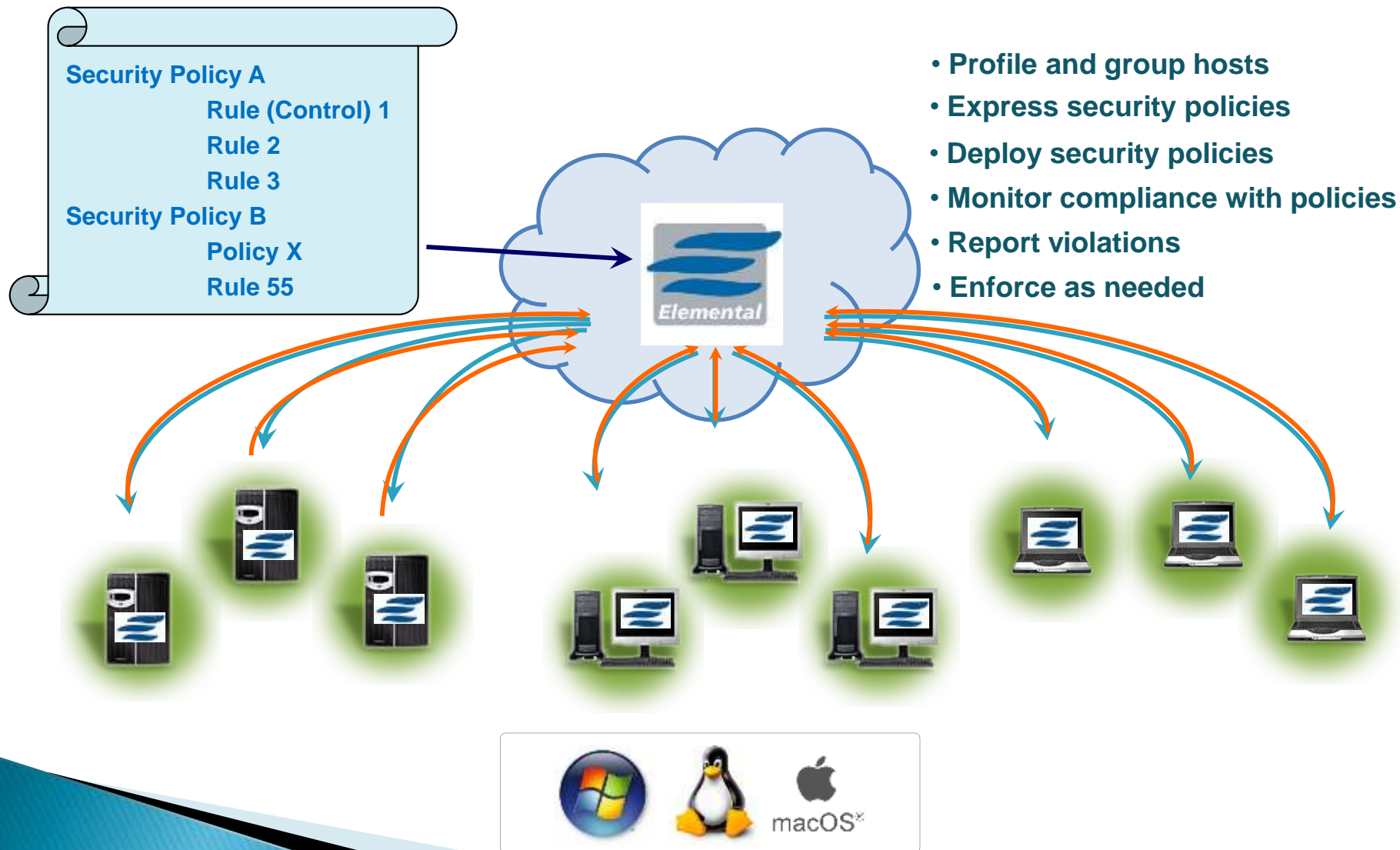
Elemental Customer Applications

- ▶ DoD contractors protecting CUI following NIST 800-171 & 172 recommendations and working towards the next CMMC maturity level certification
- ▶ Financial services provider protecting server and client-machines from Cyber Attacks and Malware/Ransomware
- ▶ E-Commerce provider protecting their Payment Processes and enforcing PCI-DSS Compliance
- ▶ IT Services Provider performing a security and compliance assessment following best industry standards CIS, NSA, STIG
- ▶ Construction company auditing and enforcing their industry specific Security Policies
- ▶ University Hospital ensuring their 24x7 HIPPA / HITRUST Compliance Automation
- ▶ Managed Services Provider demonstrating their infrastructure is SOC 2 compliant

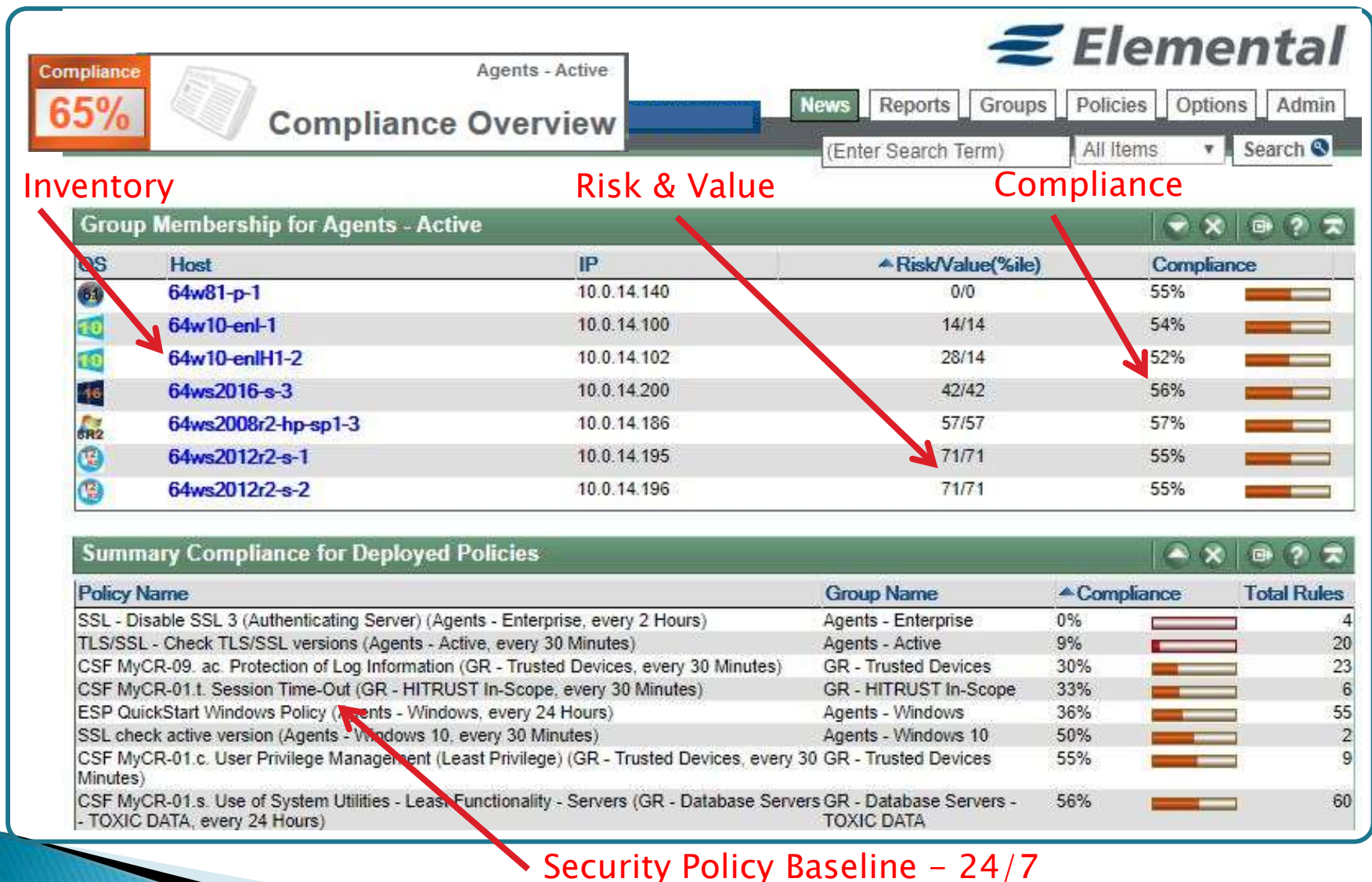


ESP - Elemental Security Platform

ESP Deployment Architecture



ESP brings it all together: Security Compliance Risk



ESP: Elemental Policy Library

Policies

Log Out espadmin ⓘ
Create Policy ⓘ

Views

- Deployed Policies
- Global Rule Exceptions
- Audit Trail - Global Rule Exceptions
- Summary Views

Policies

- Elemental Security Platform (ESP)
- Regulatory Compliance & Industry Standards
 - CIS - Center for Internet Security
 - CIS AIX
 - CIS HP-UX
 - CIS LINUX Red Hat
 - CIS Mac OS X
 - CIS Windows 10 Enterprise
 - CIS Windows 7
 - CIS Windows 8.1
 - CIS Windows Server 2008
 - CIS Windows Server 2012
 - CIS Windows Server 2016
 - HIPAA/HITECH Security Policies
 - HITRUST CSF Security Policy
 - NIST 800-171 Security Policy**
 - NIST 800-53 (FISMA) Security Policy
 - PCI DSS Security Policy
 - SOX Security Policy

Compliance
69%

NIST 800-171 Security Policy

Contained Policies and Rules for NIST 800-171 Security Policy

The following policies and rules are contained within NIST 800-171 Security Policy.

- 3.1 - Access Control
 - 3.1.3 - Control the flow of CUI
 - 3.1.8 - Limit unsuccessful logon attempts
 - 3.1.10 - Use Session Lock
 - 3.1.11 - Terminate User Session
- 3.2 - Awareness and Training
- 3.3 - Audit and Accountability
 - 3.3 - Audit Policy - IBM-AIX
 - 3.3 - Audit Policy - Oracle Solaris
 - 3.3 - Audit Policy - Red Hat Enterprise
 - 3.3 - Audit Policy - Windows
- 3.4 - Configuration Management
 - 3.4.1-2 - Baseline Configuration Settings

Contained Policies and Rules for 3.3 - Audit and Accountability

The following policies and rules are contained within 3.3 - Audit and Accountability.

- 3.3 - Audit Policy - IBM-AIX
- 3.3 - Audit Policy - Oracle Solaris
- 3.3 - Audit Policy - Red Hat Enterprise
- 3.3 - Audit Policy - Windows
 - Auditing account logon events using domain credentials set to success and failure
 - Auditing logon events using local credentials set to success and failure
 - Auditing of Active Directory object access disabled
 - Auditing of process tracking disabled
 - Auditing set to audit account management success and failure
 - Auditing set to audit object access failure
 - Auditing set to log all privilege use failure
 - Auditing set to log all security policy changes success and failure
 - Auditing set to log all system events success and failure
 - Generate security audits right set
 - Manage auditing and security log right assigned to Administrators

Policy Rules

ESP Security Compliance Metrics

Compliance

83%



Agents - Active

Compliance Overview

Deployed Policies

ESP Agent information and status	100%	<div><div></div></div>
Agents - Installed (Read Only)	100%	<div><div></div></div>
ESP Command Output Gather	100%	<div><div></div></div>
Agents - Installed (Edit) (Undeploy)	100%	<div><div></div></div>
ESP Document Value Policy	100%	<div><div></div></div>
Agents - Installed (Read Only)	100%	<div><div></div></div>
ESP Initial Policy	42%	<div><div></div></div>
Agents - Installed (Edit) (Undeploy)	42%	<div><div></div></div>
ESP Network Traffic Monitoring	100%	<div><div></div></div>
Agents - Installed (Edit) (Undeploy)	100%	<div><div></div></div>
ESP Packet filter default rules	100%	<div><div></div></div>
Agents - Installed (Read Only)	100%	<div><div></div></div>

Format and eject of removable media allowed by Administrator
 Retention method for system log set to "Manually"
 Retention method for security log set to "Manually"
 Disable password caching
 Always prompt when downloading
 Disable adding channels

Deployed Policies

	Group Name	Compliance	Total Rules
Installed, every 2 Hours)	Agents - Installed	100%	32
d, every 24 Hours)	Agents - Installed	100%	32
, every 8 Hours)	Agents - Installed	100%	6
ours)	Agents - Installed	42%	40
lled, every 30 Minutes)	Agents - Installed	100%	1
			3

Compliant Hosts

Risk/Value (%ile)	Compliance
16/0	31%
16/0	31%
50/0	31%
0/0	32%
83/66	38%
66/83	41%

Compliant Policy Rules

# Hosts Applied To	# Exemptions	# Not Applicable	Compliance
6	0	0	0%
6	0	0	0%
6	0	0	0%
6	0	0	0%
6	1	0	0%
6	0	0	0%
6	0	0	0%
6	0	0	0%
6	0	0	0%
6	0	0	0%

ESP Report Scheduling & Exporting

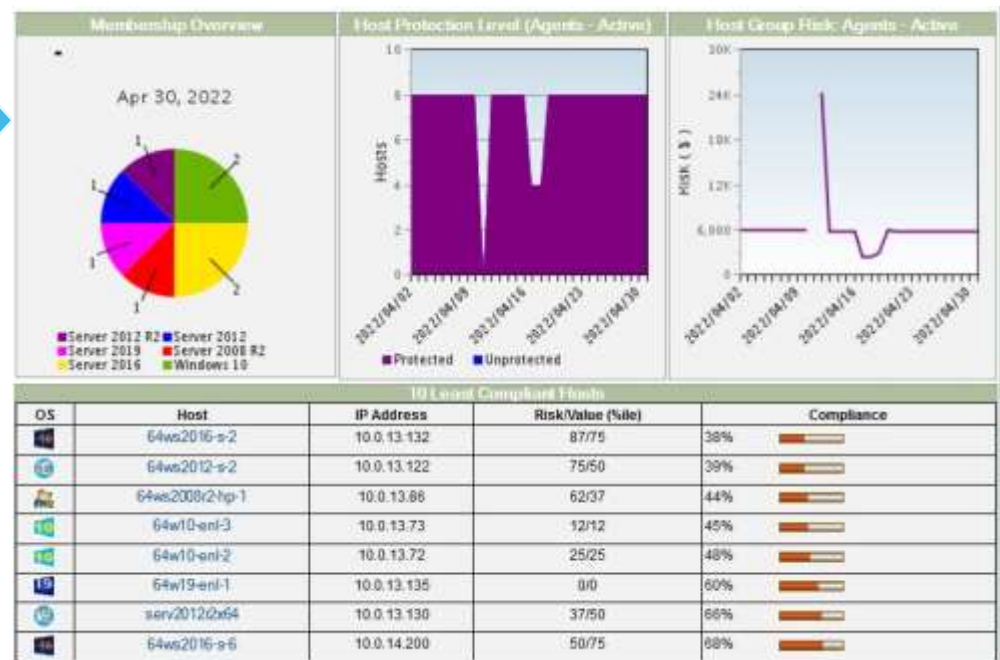
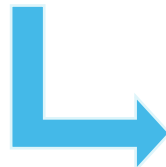
Reports

[Log Out ecslab](#)
[View Scheduled Reports](#)

Available Reports

- Management Reports
 - Compliance
 - Policy
 - By Host Group
 - By Host Value
 - Overview
 - Host Group
 - Risk
 - Operational Overview
 - Agent
 - AWDL Agent Statistics
 - Agent Population for Host Group
 - Agent Status for Host Group
 - Agents Targeted for Deployed Policy
 - Alarms for Agent
 - New Agents
 - Compliance
 - Agent
 - Host Group
 - Policy
 - Enforcement
 - Rules Enforced - Deployed Policy
 - Rules Enforced - Host Group
 - Host Group
 - All Host Group Membership Statistics
 - Host Group Comparative Membership
 - Membership Changes
 - Membership Count
 - Protected Hosts
 - Rule Remediation
 - Risk
 - Traffic
 - Trouble Ticket
 - Value

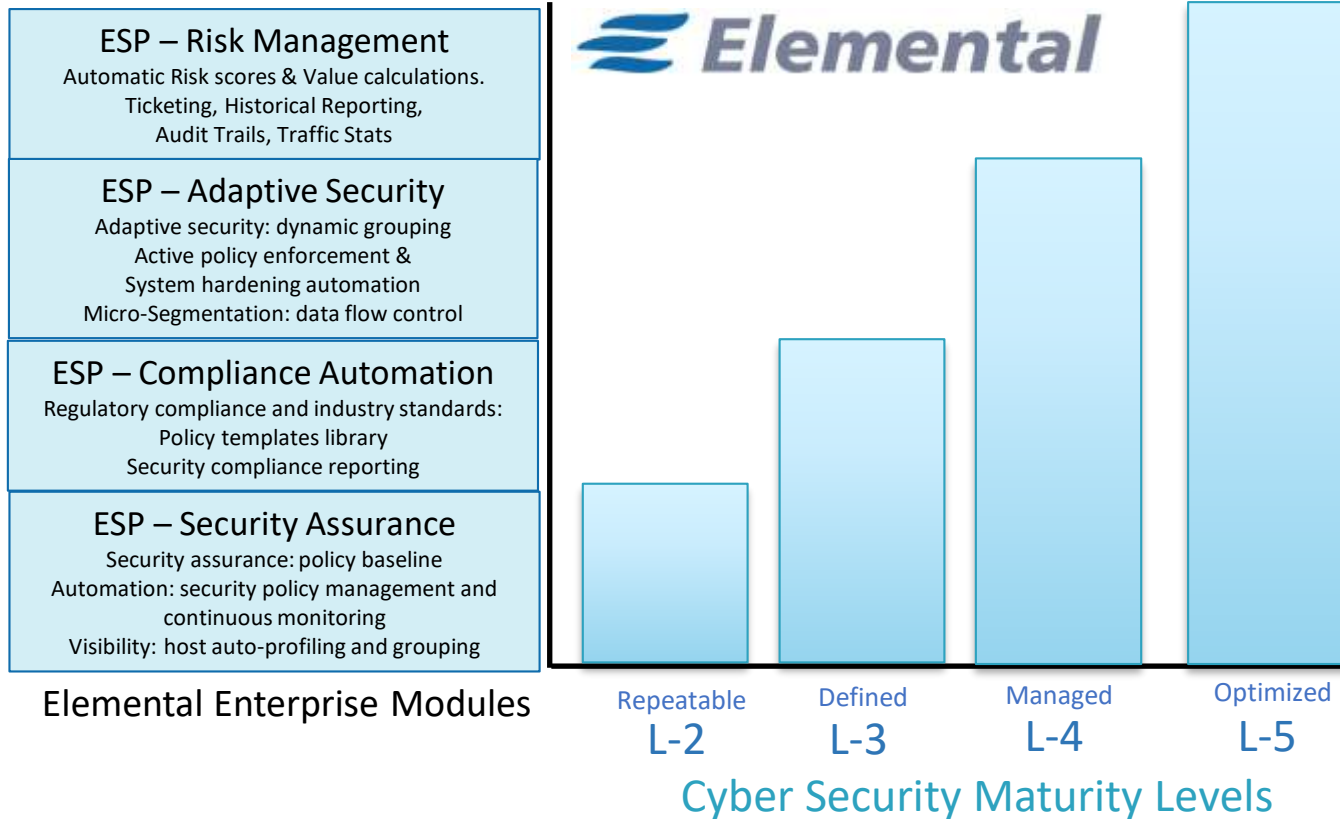
Scheduled Reports				
Report Name	Description	Period	Last Run Email	
Host Group Compliance Overview for Agents - Installed	Compliance by h...	Daily at 12am.	Success	
Policy Operational Overview for ESP Initial Policy	Operational ove...	Monthly at 12am on the 1st.	Success	



Elemental technology is unique

- ▶ ESP highly integrated platform: Security + Compliance + Risk
- ▶ ESP Policy Engine: *manage policy lifecycle*
automate policy deployment, monitor and enforce
- ▶ ESP Dynamic Grouping: *adaptive to change*
 - Security posture change detection
 - Automatic policy adjustment
- ▶ ESP System Hardening: *host config enforcement*
- ▶ ESP Policy based *micro-segmentation*
- ▶ ESP Policy Library:
thousands of ready to use security controls (rules)
- ▶ ESP PolicyFUEL: *extensible policy library*
- ▶ ESP FuelPacks: *policy templates library*
- ▶ ESP Reporting: *real-time* metrics and *historical* reporting
- ▶ ESP Audit Trails

Cybersecurity Maturity Model



Any size: Start-up to Enterprise

- ▶ ESP scales easily:
 - from very small start-up (a few PCs) deployments
 - to large Enterprises (thousands of endpoints) deployments
 - for On-Premise/Datacenter and Cloud environments

*Start small and grow within
a single platform to automate your
Security Assurance & Compliance
Assessment, Enforcement*

The Elemental Cyber Security Platform

- ▶ A unique approach to Security & Compliance & Risk



Cloud Hosted Cyber
Security Platform
Host where you need it



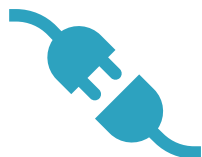
Affordable
subscription based
per-use pricing



Real-Time Policy
Execution at the
Endpoint



Zero-Trust Security
Concept



Fully automated
Set-Up process



Zero Carbon Foot-
print for unmatched
Sustainability