Deloitte.

Addressing routine technology processes and cyber risks through simplified managed services

enterprise Intelligent Secure Configuration Management as a Service (eISCMS)

Organizations spend enormous amounts of resources annually managing the security configurations of tens of thousands of devices. It is not rocket science—it is a slow, constant, manual, repetitive process. With the best of intentions, few do it effectively.

Although repetitive, the exacting nature of the work results in human error. It also distracts skilled people from focusing on other critical projects.

By the time one set of devices has been reconfigured, it is likely out of date. Why? Because the scope and requirements change—and grow more complex—as fast as the infrastructure itself changes. And worse, the threat landscape changes even faster, rendering yesterday's configuration continually exposed to risk.

Part of the problem is that secure configuration management as a function—straddles the line between information technology (IT) operations and IT security, requiring collaboration between typically siloed groups. The continuous stream of changes driven by the security side cause downtime concerns on the operations side and the IT team is usually responsible for execution of designs they do not fully understand.

It is an extensive and difficult technical problem that imposes huge uncertainty on whether your environment is properly configured. The uncertainty can lead to paralysis as organizations don't know how to patch a hole of which they don't understand.

Organizations try to manage the problem with an array of point solutions—but central visibility is lacking. Is the infrastructure more secure today than it was yesterday? Few can answer the question.

Paradigm shift is required—adding resources or improving processes will not keep up with the rate of increase in cyber threats. As cyber threats automate, organizations should also equip themselves with automation.

In 60% of cases, attackers are able to compromise an organization within minutes

99.9% of the exploited vulnerabilities were compromised more than a year after the common vulnerabilities and exposure was published

60% of incidents were attributed to errors made by system administrators

Breaches*

*Source: Verizon 2015 Data Breach Investigation

Creating an automated managed service to achieve efficient operations

As an organization expands or teams with others, their responsibilities grow, requiring the protection of new capabilities and, most importantly, data. Deloitte Advisory offers continuous system and device configuration, including advanced, threat-aware secure configuration design and automated configuration execution using market-leading technologies.

Deloitte Advisory's service offerings provide end-to-end automation and a growing set of capabilities:

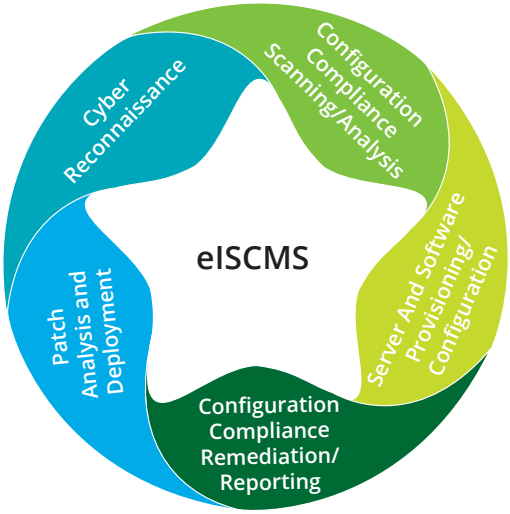
Server And Software Provisioning/ Configuration—eISCMS reduces manual intervention via automated provisioning of new servers and rolls out new configurations in minutes versus hours. Required for organizations that need resources to grow as fast as them.

Configuration Compliance Scanning/ Analysis—eISCMS provides visibility and on-demand analysis of your IT or security environment by integrating our contentious scanning capability.

Configuration Compliance Remediation/Reporting—The ability to scan your environment only provides a point solution that may be inadequate to handle enterprise resource management needs. eISMCS provides the automated security remediation capability that turns scanning results into action.

Patch Analysis and Deployment—It requires significant patching/updates from their vendors. Integrated with compliance reporting, eISCMS provides the ability to automate patch roll-outs during scheduled downtime.

Cyber Reconnaissance—Nobody can see into the future, but eISCMS integrates with collectors to gather and analyze data to provide IT resource owners threat awareness. eISCMS takes continous monitoring further to provide near real-time sweeps against the threat landscape for an active awareness of everything happening in your environment.



Our Experience

Demonstrated history of effective innovations
Our use-case-driven innovation environment leverages emerging technologies to continuously enhance our eISCMS offering. Built on our demonstrated delivery methodology, eISCMS leverages our deep technical experience, regulatory knowledge, IT vendor relationships, and access to our global network of skilled professionals.

Rely on our industry experience and knowledge
We have deep experience across every major sector and industry and bring broad context for understanding your particular set of cyber risk and business challenges.

Solution benefits

Unifying Your Organization.

IT security and operations have different organizational performance metrics.

The former has an ever-growing number of requirements that need to be implemented immediately, while the latter cannot afford the downtime required to support that effort. **Deloitte Advisory's approach allows for tailored deployment packages that decrease downtime and limit the clash between these departments, helping your organization remain focused on its mission.**

Improve Your Organization's Velocity.

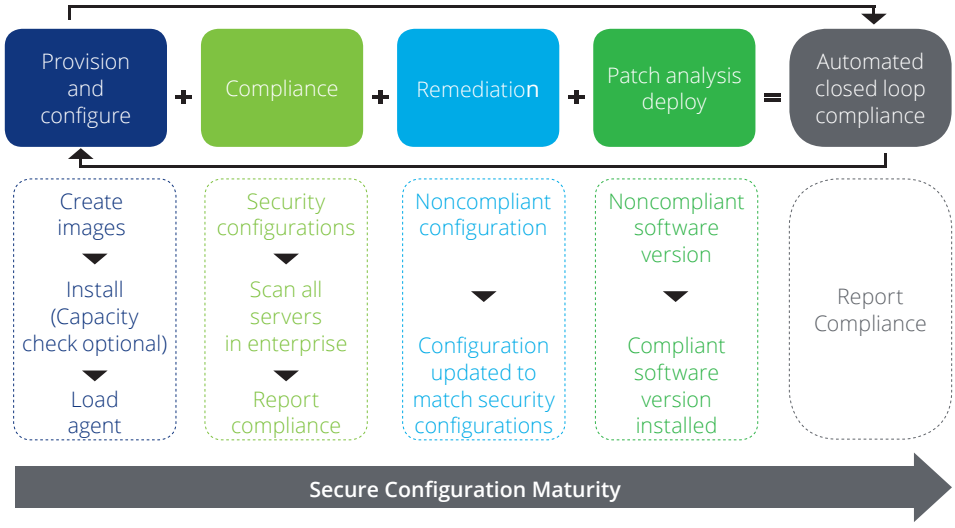
The ability to promptly deploy a critical patch, respond to an intrusion, or enact preventive measures are capabilities inherent to Deloitte Advisory's offerings. It is no longer sufficient to only scan and discover vulnerabilities. Our approach leverages that information to automatically remediate noncompliant findings and **keep IT environments continuously hardened.** Deloitte Advisory can also help deploy preventive measures that **promote consistent security postures** and promote mission continuity.

Free Up Resources to Concentrate on your Business Objectives.

Organizations tend to increase the number of resources to handle cyber threats. Deloitte Advisory's approach can help **alleviate the need for large amounts of resources and automate tasks performed by individuals.**

The eISCMS Approach

- Know your starting point and your future objectives
- Create a set of standardized configurations to achieve high-quality efficiency
- Manage and provision IT assets effectively
- Mature and integrate resources
- Create visibility for executive-level risk decisions
- Choose from services that span the full life cycle



Helping you become Secure.Vigilant.Resilient.™

To grow, streamline, and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what is most important to your organization, you must invest in cost-justified security controls to protect your most important assets, focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A Secure.Vigilant.Resilient. cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

- **BEING SECURE** means having risk-focused defenses around what matters most to your mission.
- **BEING VIGILANT** means having threat awareness to know when a compromise has occurred, or may be imminent.
- **BEING RESILIENT** means having the ability to regain ground when an incident does occur.

Server and software provisioning/ configuration

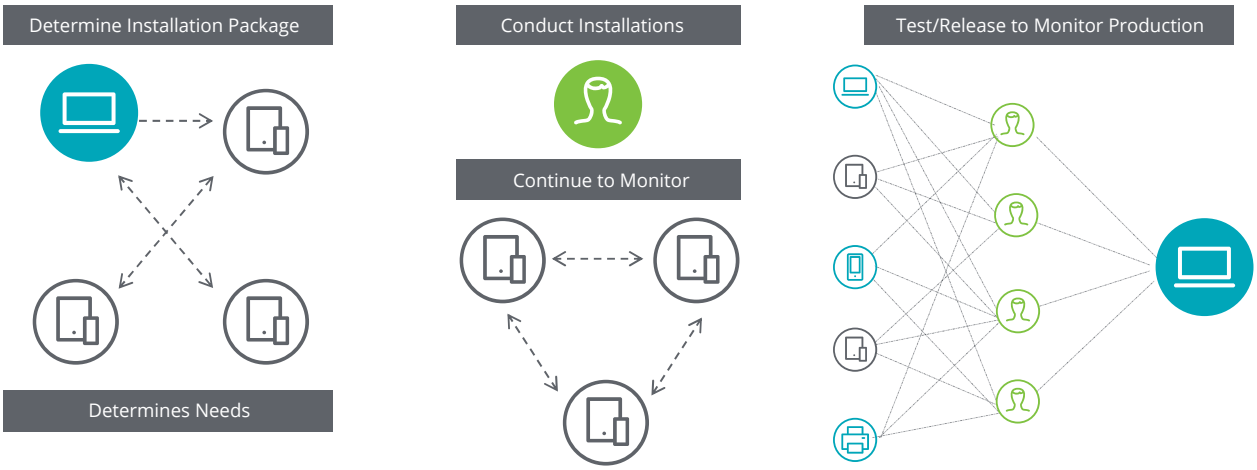
eISCMS reduces manual intervention via automated provisioning of new servers and rolls out new configurations in minutes versus hours. Required for organizations that need resources to grow as fast as them.

Manual method

Challenges:

- Installation/upgrade inconsistencies can create security vulnerabilities.
- Manual installation/upgrade process can take one week per server.
- Uploads/downloads consume significant bandwidth.
- Baseline changes may not be properly tracked or communicated, creating vulnerabilities.

Traditional manual approach:

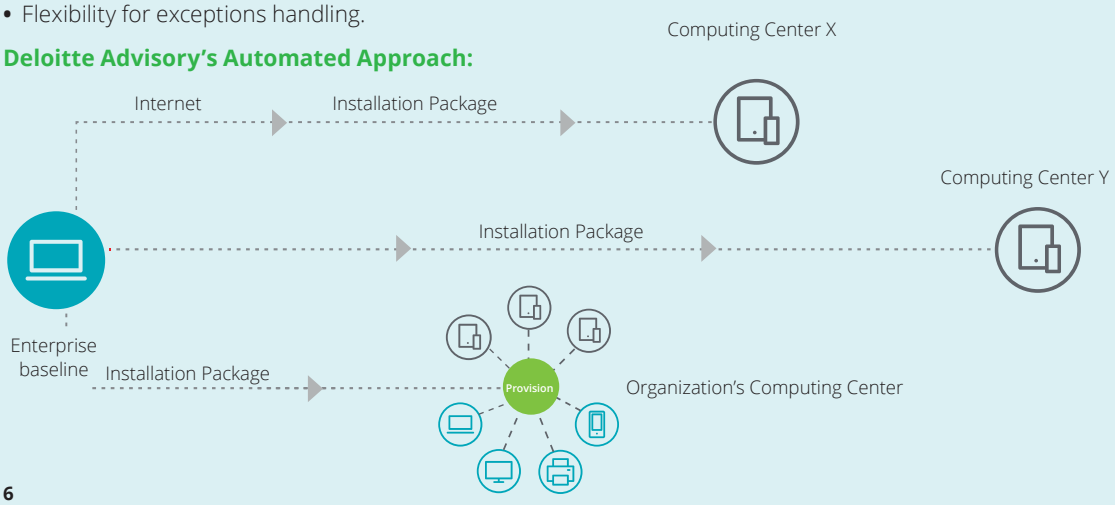


Deloitte Advisory's Managed Service

Value delivered:

- Uniform, high-quality installation, configuration, and upgrade.
- Average process reduced from one week to less than two hours per server or group of servers in parallel.
- Significantly lower bandwidth usage due to simultaneous uploads/downloads.
- Automated tracking and communication.
- Flexibility for exceptions handling.

Deloitte Advisory's Automated Approach:



Configuration compliance scanning/ analysis

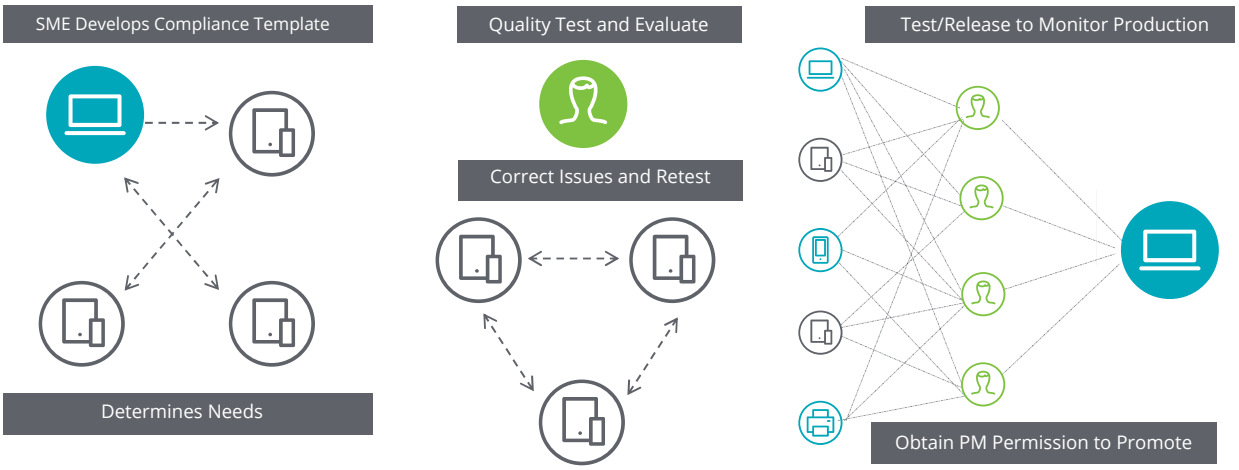
eISCMS provides visibility and on-demand analysis of your IT or security environment by integrating our continuous scanning capability.

Manual method

Challenges:

- Manual line-by-line code analysis of server software—tens of thousands per system administrator.
- Average eight hours of analysis time per server.
- Hundreds of security configuration guidelines—e.g., CIS, DISA, HIPAA, NIST.
- System vulnerabilities due to the length of time between security scans.
- System vulnerabilities due to errors and inconsistencies in manual scans.

Traditional manual approach:



Deloitte Advisory's Managed Service

Value delivered:

- Ad-hoc scanning of one or many servers to evaluate progress toward security compliance goals.
- Flexible automated scanning schedule, from daily to weekly, based on client preference.
- Continuous visibility into status of security compliance and hardening status.
- Automated compliance tracking and reporting.

Deloitte Advisory's Automated Approach:

Configuration compliance remediation/ reporting

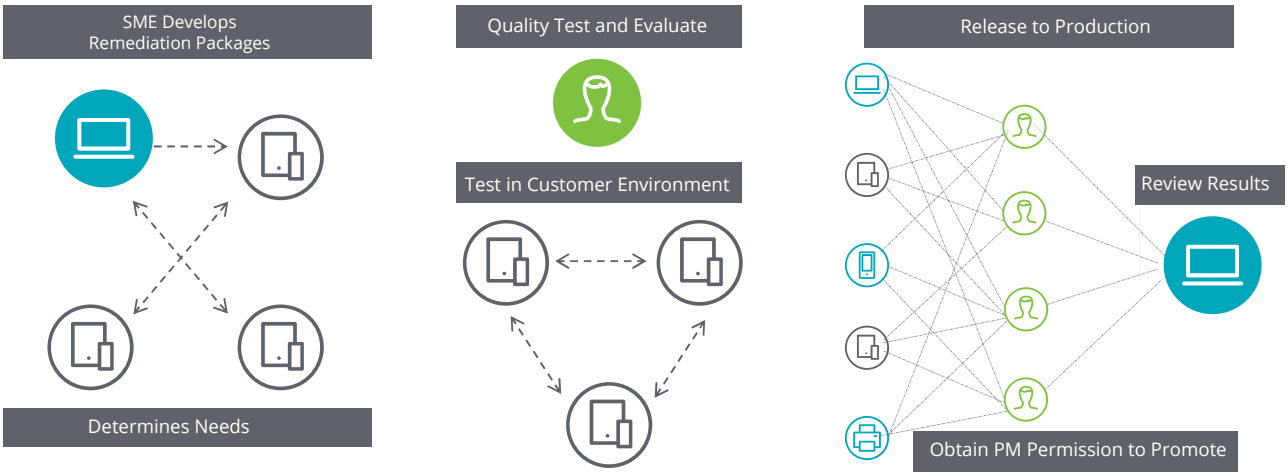
The ability to scan your environment only provides a point solution that may be inadequate to handle enterprise resource management needs. eISMCS provides the automated security remediation capability that turns scanning results into action.

Manual method

Challenges:

- Separate patch analysis and remediation processes and tools.
- Time-consuming analysis and installation scheduling process.
- No prestaging capabilities.
- Manual log-on, installation of patches, and rebooting of each server—several hours per server.
- Inconsistent and error-prone change tracking and reporting.

Traditional manual approach:

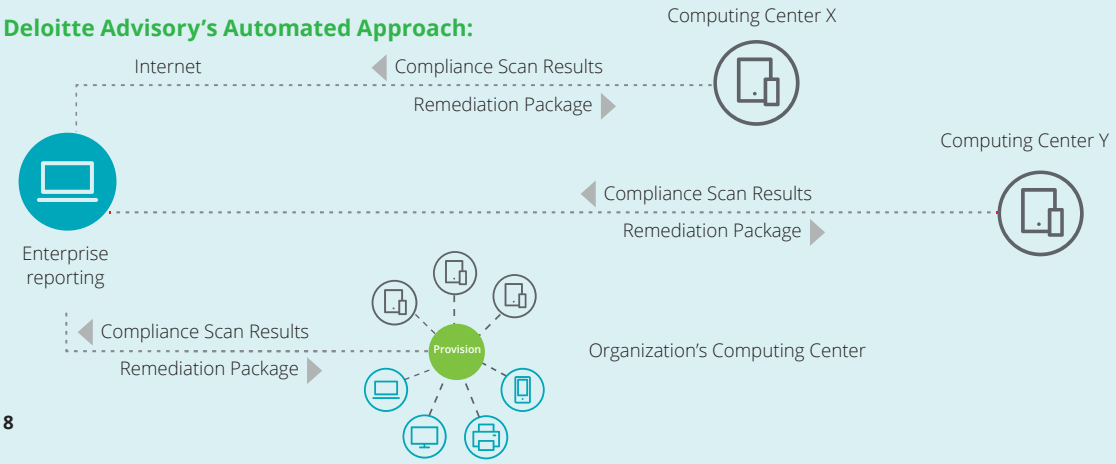


Deloitte Advisory's Managed Service

Value delivered:

- Automated correction of noncompliant configurations as part of secure configuration scanning process.
- Parallel automated configuration of hundreds of settings across thousands of servers.
- Automated rollback capability to reduce server downtime.
- Efficient use of system administrator resources.
- Automated tracking and reporting of remediation.

Deloitte Advisory's Automated Approach:



Patch analysis and deployment

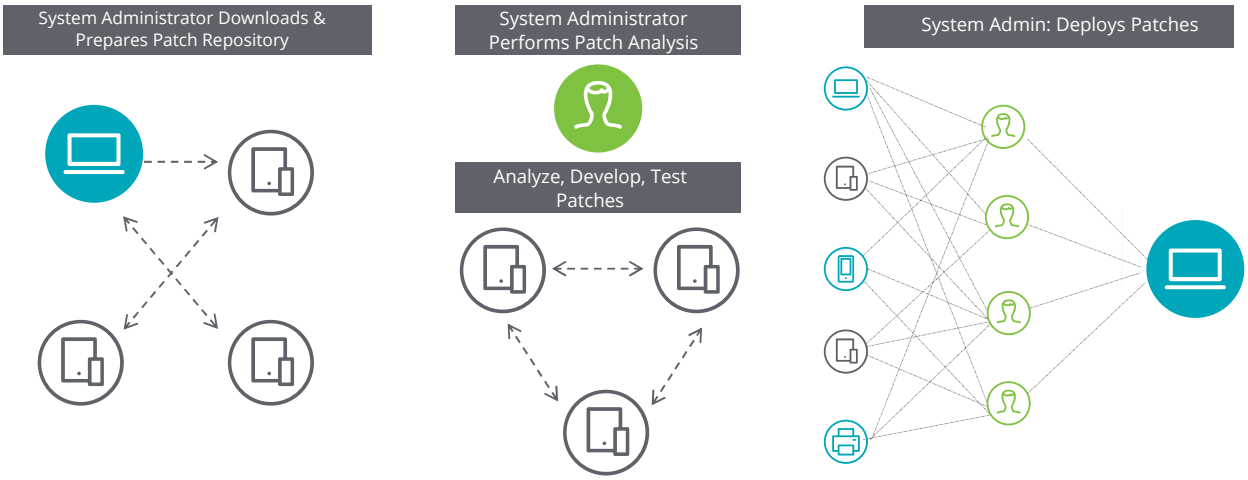
Information technology requires significant patching/updates from their vendors. Integrated with compliance reporting, eISCMS provides the ability to automate patch roll-outs during scheduled downtime.

Manual method

Challenges:

- No centralized patch analysis, pre-staging and committal.
- Manual patch dependency mapping and pre-staging.
- Fixed installation scheduling.
- Manual, in series patch installation—hours per server | no repeater servers in global deployments.
- Manual change tracking and reporting.

Traditional manual approach:

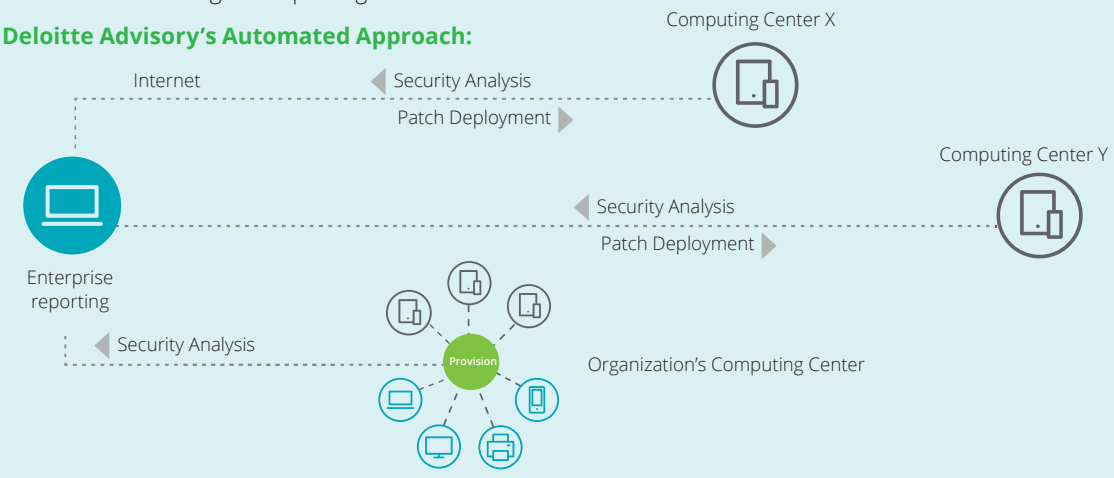


Deloitte Advisory's Managed Service

Value delivered:

- Automated correction of noncompliant configurations as part of secure configuration scanning process.
- Parallel automated configuration of hundreds of settings across thousands of servers.
- Automated rollback capability to reduce server downtime.
- Highly-efficient use of System Administrator resources.
- Automated tracking and reporting of remediation.

Deloitte Advisory's Automated Approach:



Cyber reconnaissance

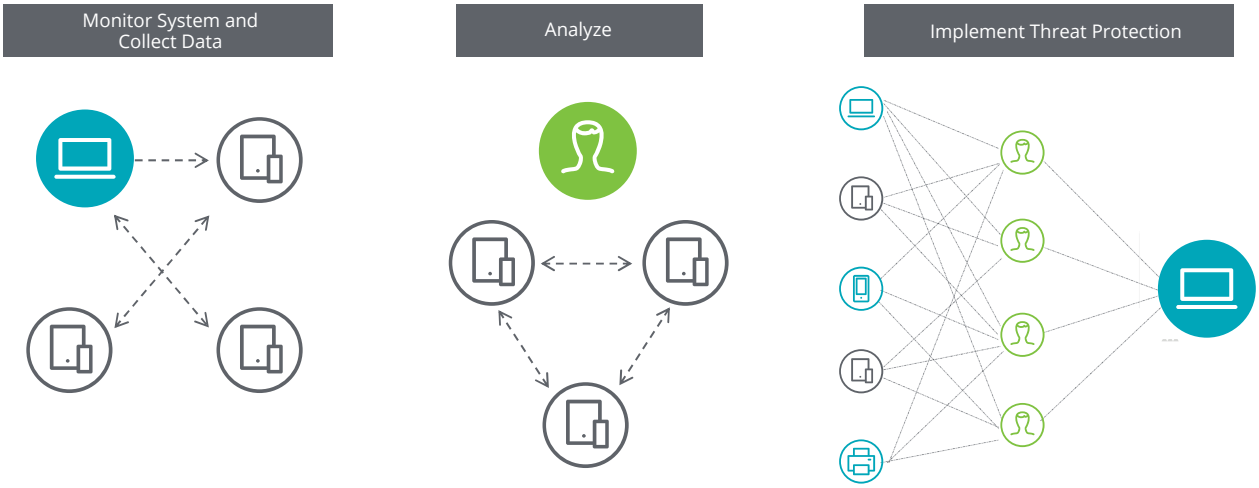
Nobody can see into the future, but eISCMS integrates with collectors to gather and analyze data to provide IT resource owners with threat awareness. eISCMS takes continous monitoring further to provide near real-time sweeps against the threat landscape for an active awareness of everything happening in your environment.

Manual method

Challenges:

- Out-of-date and incomplete information creating vulnerabilities.
- Separate systems for data-gathering and analysis, creating delays and the potential to miss critical threats.

Traditional manual approach:

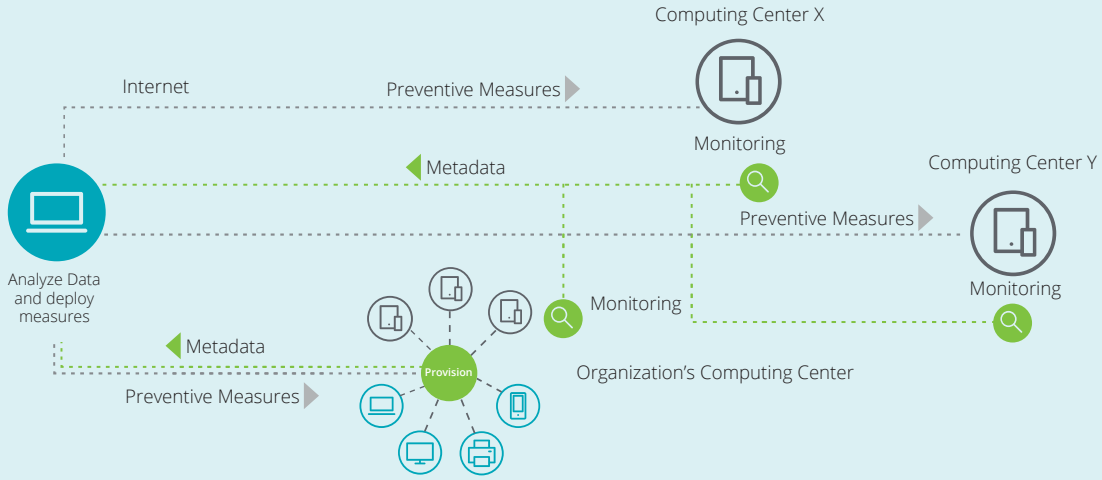


Deloitte Advisory's Managed Service

Value delivered:

- Comprehensive data collection across the enterprise.
- Centralized execution of data gathering and analysis.
- Simultaneous monitoring of multiple systems globally.

Deloitte Advisory's Automated Approach:



Client case study—Value delivered

Client profile

- Global operations, providing IT processing capability, systems management, communications and storage in support of services, agencies, and combatant commands
- Secure facilities strategically located around the world
- Supports millions of users with petabytes of storage
- Transitioning from a traditional software implementation and sustainment model to a service provider delivered enterprise software-as-a-service operating model

Security challenges

- >10,000 networked servers globally
- Server security configuration transparency
- Auditing against stringent security controls—more than 11,000 security technical implementation guides (STIG) compliance rules for servers alone
- Enterprise-wide visibility of security posture
- Inventory life cycle control of tens of thousands of servers
- Long discovery, incident response, and compliance reporting times

Deloitte Advisory's solution

- Enterprise services—security compliance/remediation, automated secure provisioning, patch analysis/deployment
- Operations—content development, sustainment, and project management office

Exponential return on investment achieved

Task	Before	After
Scan server for STIG Audit	20 minutes	3 minutes
STIG Analysis using Gold Disk (STIG versus Actual and Remediate back to compliance) per server	3 days (without rollback and audit trail)	10 minutes (with rollback and audit trail)
STIG Analysis using Gold Disk for 100 Servers	300 days	2 days
Server Inventory/ Configuration/ Remediate	15 days	15 minutes
Install, Configuration, Patch new servers	3.5 hours per server	7 minutes per server
Change Tracking/Server Drift Tracking	N/A	Continuous/Automated
Documentation (exceptions/changes)	Limited if done	Automatic real-time reporting

Contact us:

Deborah Golden

Principal l Federal Cyber Risk Services Leader

Deloitte & Touche LLP

debgolden@deloitte.com

+1 571 882 5106

Mark Masone

Principal | Deloitte Advisory

Deloitte & Touche LLP

mmasone@deloitte.com

+1 571 882 5071

Learn more:

Federal Practice

http://www.deloitte.com/federal

Cyber Risk Services

http://www2.deloitte.com/us/en/pages/risk/solutions/cyber-risk-services.html