Guardian by Cloudhouse™

- Expose Drift
- Validate Change
- Stay Secure

getguardian.io

Guardian
Executive Summary

The challenges to maintaining consistent systems are many, and the reality is that failures are both commonplace and costly. Guardian provides the visibility, accountability, and automation to maintain control over modern infrastructure in the data centre or the cloud. Guardian gives you an overview. See everything, everywhere.

Capabilities Overview

Misconfiguration Detection

Guardian catches misconfiguration drift across every type of device and digital asset, automatically checking them against your expectations so that discrepancies are quickly surfaced for remediation. Guardian filters signal from noise based on your priorities, so that unimportant changes don't overwhelm the ones that really matter.

Drift Management

Guardian stores the total configuration state of every node, making it easy to compare systems and environments, or see how a single system has changed over time. Discover cluster consensus with a single click, and have the differences visualised for rapid troubleshooting down to the line level of a configuration file.

Custom Policies

With Guardian policies, document your expectations and execute them against your environment to see how well it complies.

Out of the box Guardian is preloaded with policies for the Center for Internet Security's 20 critical security controls, satisfying many aspects of regulatory requirements like PCI and SOX. Create a policy from an existing system with a few clicks and apply it against similar systems in minutes.

Hardening Benchmarks

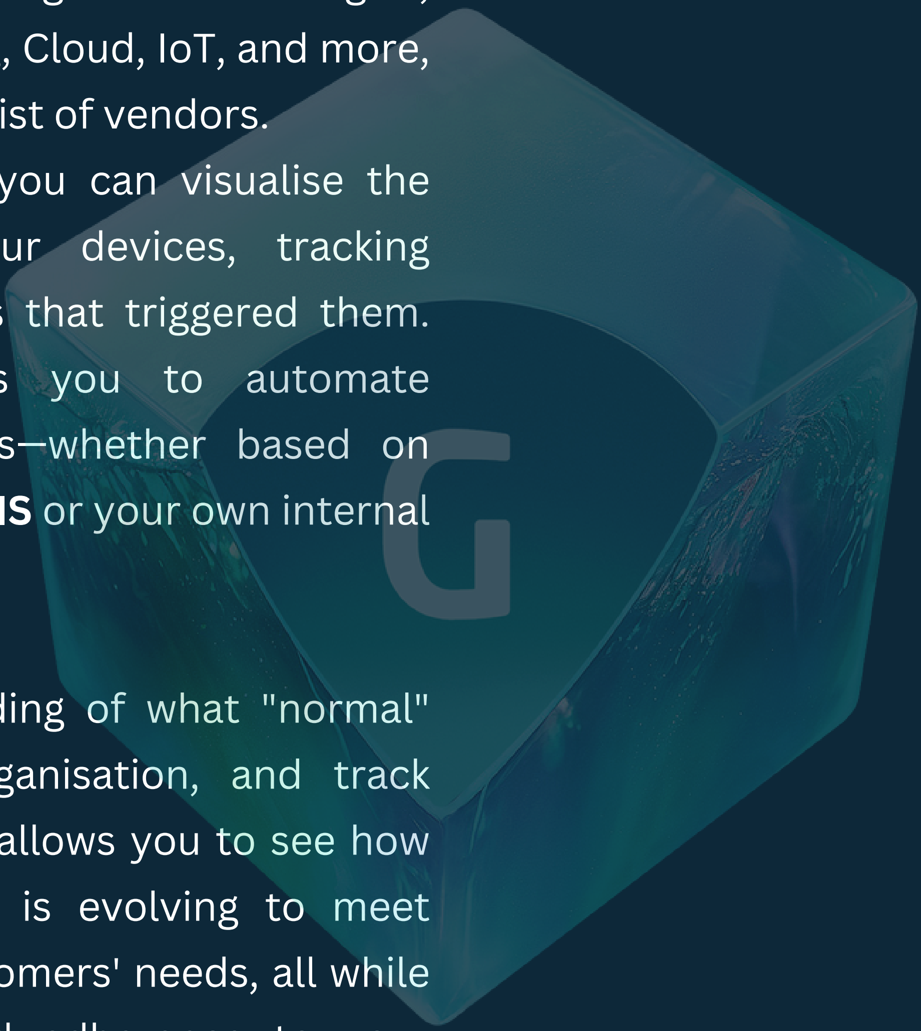
Benchmarks from the **Center for Internet Security (CIS)** offers an established standard for testing foundational security measures.

Guardian offers the capability to execute CIS policies on a user-defined schedule and includes a range of options for omitting, modifying, and supplementing the tests included in the benchmarks as published by CIS.

Guardian by Cloudhouse™

Guardian is a technology-agnostic platform that supports a wide range of technologies, including OS, Networking, Cloud, IoT, and more, from an ever-expanding list of vendors.

With our **Drift Engine**, you can visualise the entire lifecycle of your devices, tracking changes and the events that triggered them. This insight empowers you to automate compliance assessments—whether based on industry standards like **CIS** or your own internal policies.



Gain a clear understanding of what "normal" looks like for your organisation, and track changes over time. This allows you to see how your technology estate is evolving to meet both your and your customers' needs, all while maintaining control and adherence to your compliance policies.

FEATURED USE CASE

GDPR Compliance

"Due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse"

Section 1, Article 88

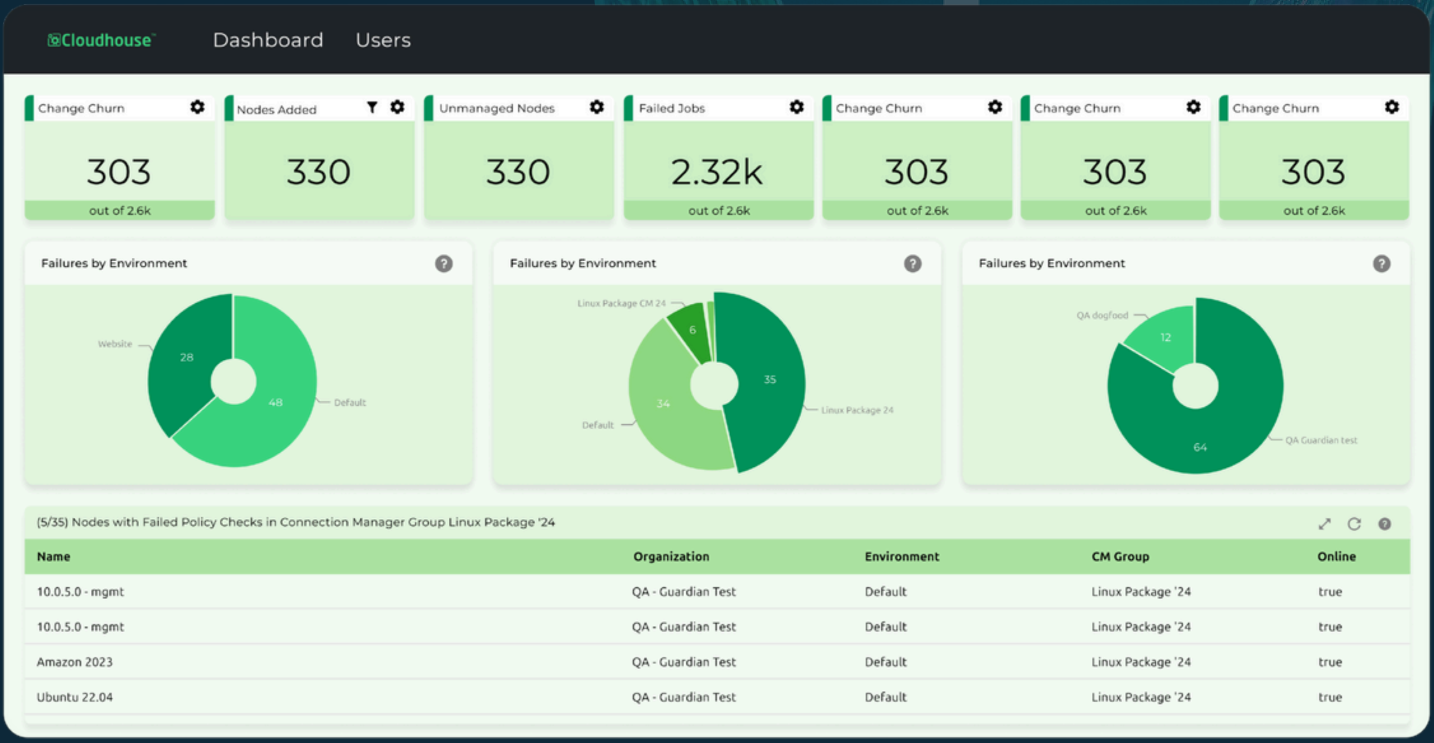
"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place"

Section 1, Article 87

Guardian helps organisations build resilience into their systems and operations, making it a natural fit for GDPR compliance.

Guardian provides the visibility and control necessary to mitigate risk in data handling and storage processes, including integrity monitoring, change management, and best practice auditing.

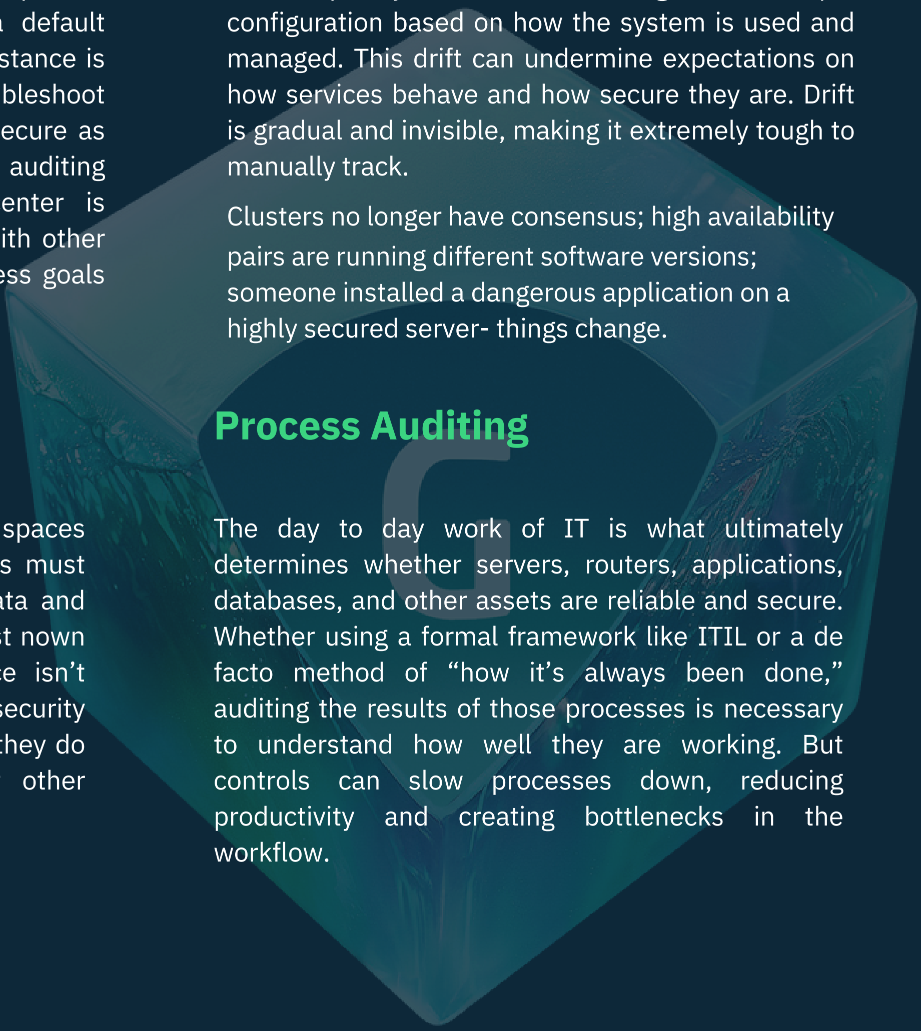
Measure your servers, network devices, applications, databases, and more against industry-standard best practices like the Center for Internet Security's critical security controls with out-of-the-box policies. With Guardian, you can understand when suspicious changes have happened that may signal a data breach.



(5/35) Nodes with Failed Policy Checks in Connection Manager Group Linux Package '24

Name	Organization	Environment	CM Group	Online
10.0.5.0 - mgmt	QA - Guardian Test	Default	Linux Package '24	true
10.0.5.0 - mgmt	QA - Guardian Test	Default	Linux Package '24	true
Amazon 2023	QA - Guardian Test	Default	Linux Package '24	true
Ubuntu 22.04	QA - Guardian Test	Default	Linux Package '24	true

Business Challenges



Misconfigurations

Most breaches are not caused by hacking, they're caused by misconfiguration. A dangerous port is accidentally left open to the internet; a default password isn't changed; a cloud storage instance is set to public because there isn't time to troubleshoot permission problems—assets are only as secure as their configurations. However, auditing misconfigurations in a complex data center is difficult and time consuming, competing with other work being driven by higher priority business goals that make security a secondary concern.

Compliance and Hardening

Many businesses operate in regulated spaces where cybersecurity and IT process audits must occur regularly to prove that customer data and services are private and secured by the best nown means. Even when regulatory compliance isn't necessary, most companies want to follow security best practices and have the evidence that they do so in the event of a data breach or other cybersecurity incident.

Configuration Drift

Things change. A system imaged from a golden master quickly drifts from that image into a unique configuration based on how the system is used and managed. This drift can undermine expectations on how services behave and how secure they are. Drift is gradual and invisible, making it extremely tough to manually track.

Clusters no longer have consensus; high availability pairs are running different software versions; someone installed a dangerous application on a highly secured server- things change.

Process Auditing

The day to day work of IT is what ultimately determines whether servers, routers, applications, databases, and other assets are reliable and secure. Whether using a formal framework like ITIL or a de facto method of "how it's always been done," auditing the results of those processes is necessary to understand how well they are working. But controls can slow processes down, reducing productivity and creating bottlenecks in the workflow.

Solution Benefits

Minimise the Risk of Misconfigurations

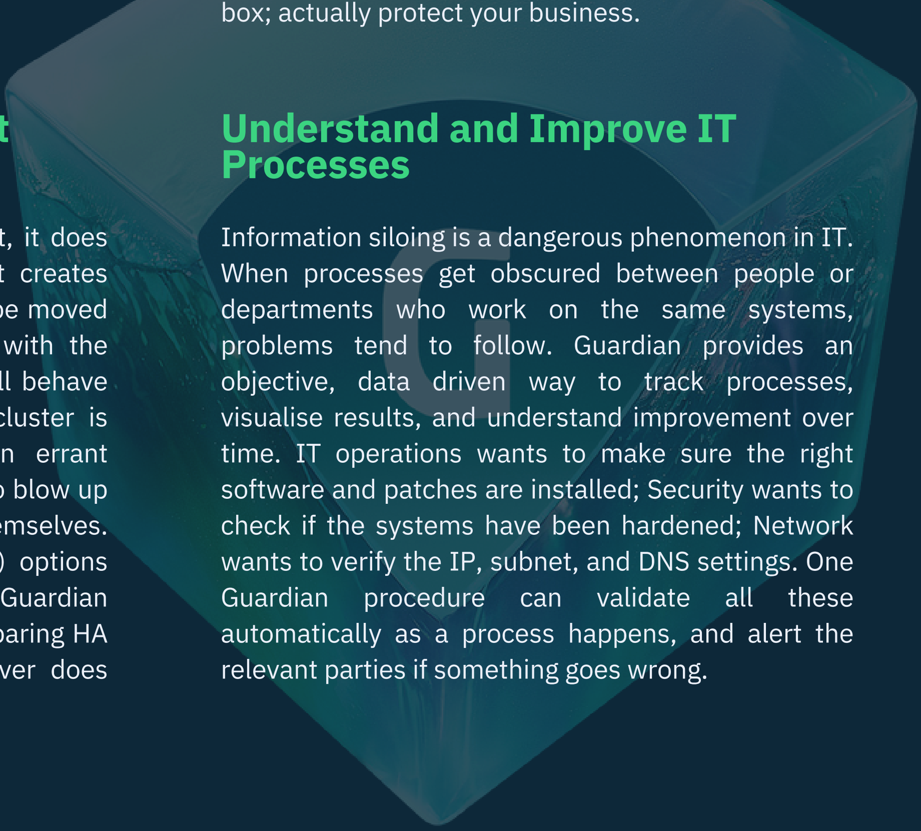
Guardian catches misconfigurations before they can be exploited, surfacing anomalies that would otherwise go unnoticed until someone else found them. Data breaches, malware, and other threats almost always rely on misconfigured systems to succeed. Guardian provides the visibility and control necessary to monitor and remediate misconfigurations proactively, a proven strategy to reduce cyber risk. Cloud storage, local servers, websites, network devices, APIs, GitHub repositories— Guardian can audit almost anything, because every risk surface matters.

Produce Reliable Systems at Scale

When Guardian prevents configuration drift, it does more than solve an abstract problem— it creates reliable infrastructure, where projects can be moved from development to test to production with the knowledge that the three environments will behave the same way. It can guarantee that a cluster is behaving as a single unit, and that an errant misconfiguration isn't a time bomb, ready to blow up when the circumstances present themselves. Businesses purchase high availability (HA) options for twice as much to reduce downtime. Guardian ensures the value of that purchase by comparing HA devices proactively, so that when a failover does occur, it occurs without incident.

Automate Compliance Assessment

The biggest problem with compliance is the overhead required to test systems and record the results in a meaningful way. Guardian automates compliance assessment and reporting, continuously auditing systems and recording the configuration state over time. Furthermore, Guardian can automatically test assets against best practices, company policy, or regulatory standards, not just one time at an audit, but all the time, so systems that fall out of compliance can be remediated as quickly as possible. Don't just check the compliance box; actually protect your business.



Understand and Improve IT Processes

Information siloing is a dangerous phenomenon in IT. When processes get obscured between people or departments who work on the same systems, problems tend to follow. Guardian provides an objective, data driven way to track processes, visualise results, and understand improvement over time. IT operations wants to make sure the right software and patches are installed; Security wants to check if the systems have been hardened; Network wants to verify the IP, subnet, and DNS settings. One Guardian procedure can validate all these automatically as a process happens, and alert the relevant parties if something goes wrong.

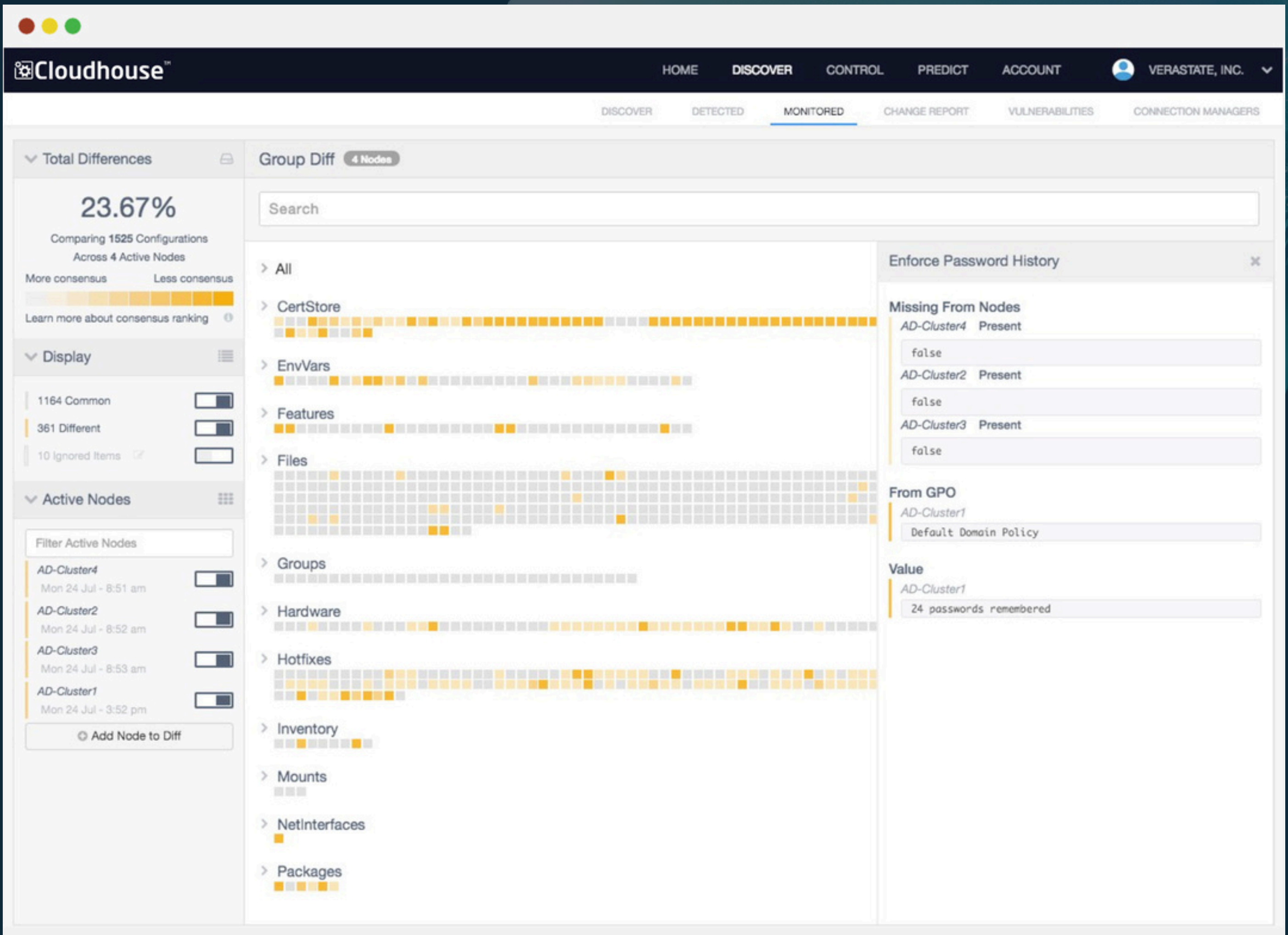
Cluster consensus

The Objective

High computing environments have systems and applications that are alike in configurations such as clusters, disaster recovery sites, or other systems performing similar roles. Over time, systems are updated and modified which can introduce variance in configurations. Keeping the variance low across these systems will ensure higher availability and reduce resources used to keep systems up and running. Organisations that achieve a low level of variance are proven to have higher availability.

The Solution

Guardian offers the ability to compare groups of like systems or environments and report on the actual variance in the configurations. Using a heatmap-like visualisation, users can immediately identify the variances across these systems and detect patterns that can guide corrective action. Guardian provides the details to pinpoint where these variances occur down to the configuration and attribute level.



Total Differences

23.67%

Comparing **1525** Configurations
Across **4** Active Nodes

More consensus Less consensus

Learn more about consensus ranking

Display

1164 Common

361 Different

10 Ignored Items

Active Nodes

AD-Cluster4 Mon 24 Jul - 8:51 am

AD-Cluster2 Mon 24 Jul - 8:52 am

AD-Cluster3 Mon 24 Jul - 8:53 am

AD-Cluster1 Mon 24 Jul - 3:52 pm

Enforce Password History

Missing From Nodes

AD-Cluster4 Present

```
false
```

AD-Cluster2 Present

```
false
```

AD-Cluster3 Present

```
false
```

From GPO

AD-Cluster1

```
Default Domain Policy
```

Value

AD-Cluster1

```
24 passwords remembered
```

Change Over Time

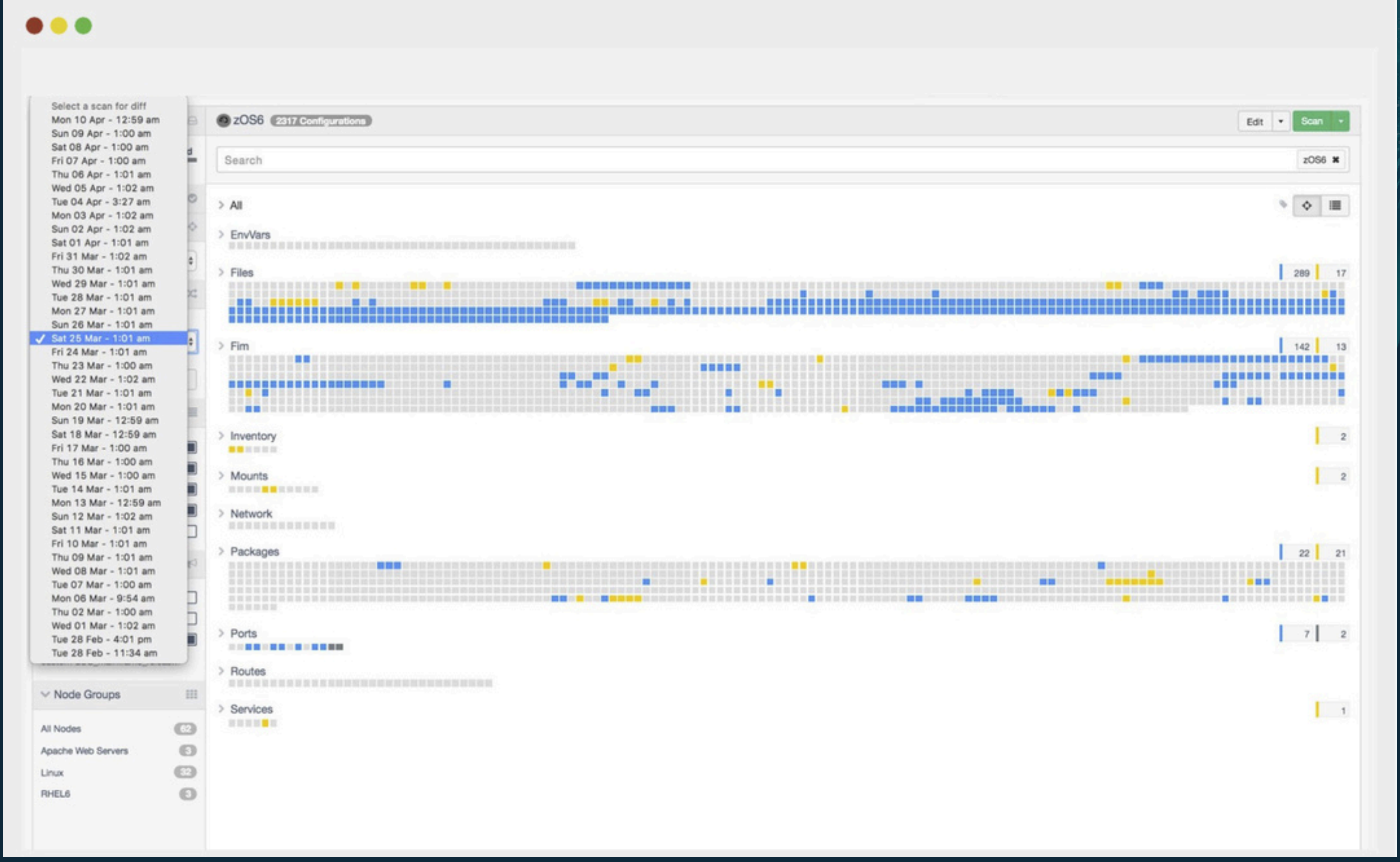
The Objective

Systems regularly change with new releases and updates. Less frequently, but more critically, users may make changes that are not captured in the change management process. These changes can introduce risk and impact the availability of systems and applications. Being able to compare the current state of a monitored system to a previous state, such as before a release, can reduce time investigating configuration state during an incident.

The Solution

Guardian continually captures system state on user defined intervals or transactional triggers, such as at the beginning and end of a deployment. Within the Guardian interface users can compare state between any two points in time to identify changes that may have prompted the current investigation, as well as to inform of those that occurred outside of other knowledge.

The findings from Guardian's total integrity monitoring can be integrated with the rest of your tool box to open incidents or trigger actions in orchestration products.



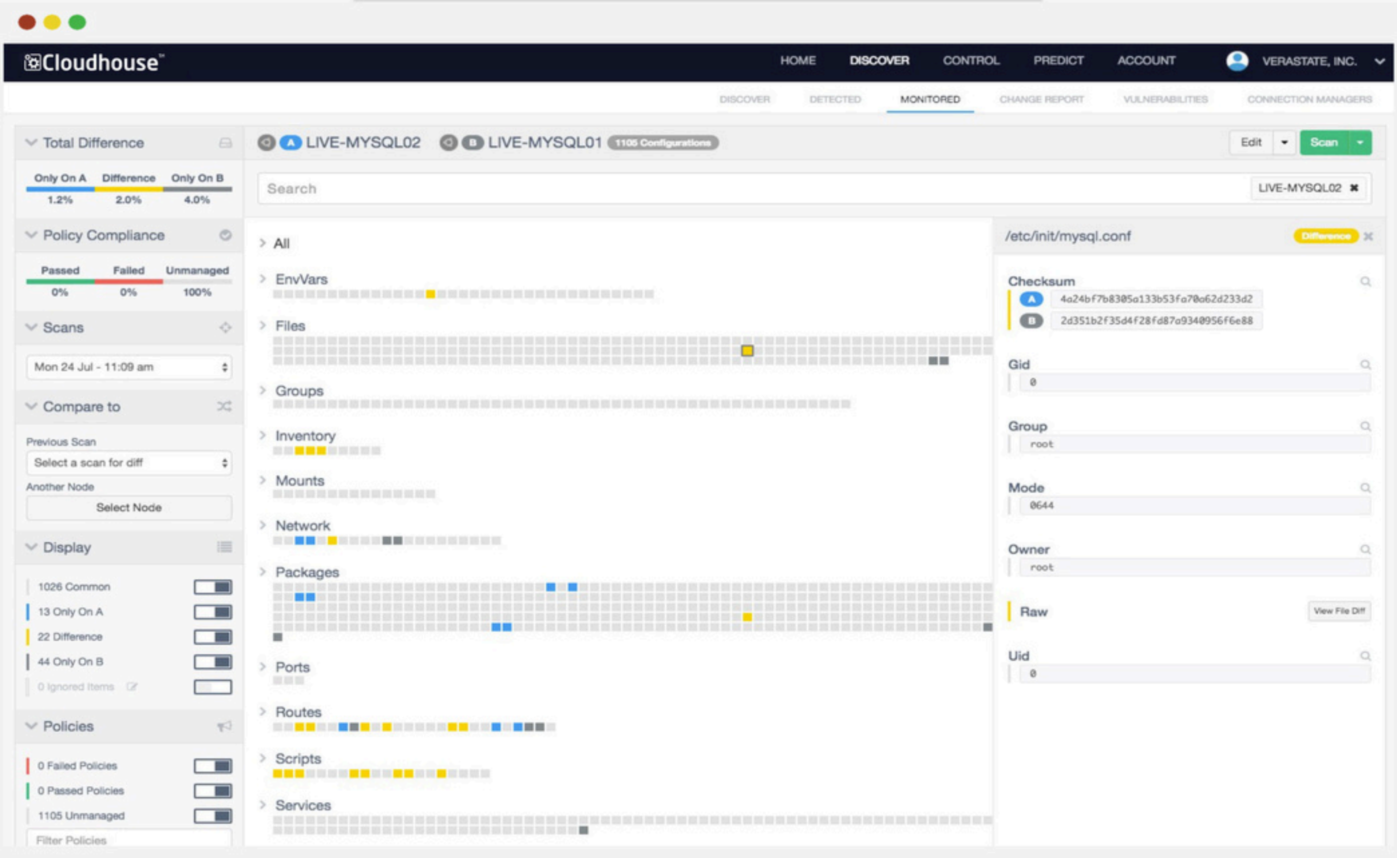
Golden Master Comparison

The Objective

Knowing that systems and applications stay in a trusted state is critical to ensuring that services remain available. Over time, inconsistent changes can cause these systems to drift from the desired state, introducing risk to availability and security. Being able to immediately identify drift from the desired state provides users the insight to address those variations before they affect availability. In cases where that analysis is not done proactively, node-to-node differencing accelerates root cause analysis to find misconfigurations in seconds.

The Solution

As updates occur, Guardian can compare the system state to the golden build or other systems of trust. The ability for on-the-fly comparisons makes it easy enough to spot variance that these checks can be part of standard operating procedures. In cases where change validation processes fail, the capability for node-to-node differencing reduces root cause analysis to minutes. With a comparison against a golden build, users can see the percentage of variance and take corrective action to ensure that any variances are known issues.



A LIVE-MYSQL02 B LIVE-MYSQL01 1105 Configurations

LIVE-MYSQL02 ✖

Total Difference

Only On A	Difference	Only On B
1.2%	2.0%	4.0%

Policy Compliance

Passed	Failed	Unmanaged
0%	0%	100%

Scans: Mon 24 Jul - 11:09 am

Compare to
Previous Scan: Select a scan for diff
Another Node: Select Node

Display
1026 Common
13 Only On A
22 Difference
44 Only On B
0 Ignored Items

Policies
0 Failed Policies
0 Passed Policies
1105 Unmanaged

/etc/init/mysql.conf Difference

Checksum
A 4a24bf7b8305a133b53fa70a62d233d2
B 2d351b2f35d4f28fd87a9340956f6e88

Gid: 0

Group: root

Mode: 0644

Owner: root

Raw

Uid: 0

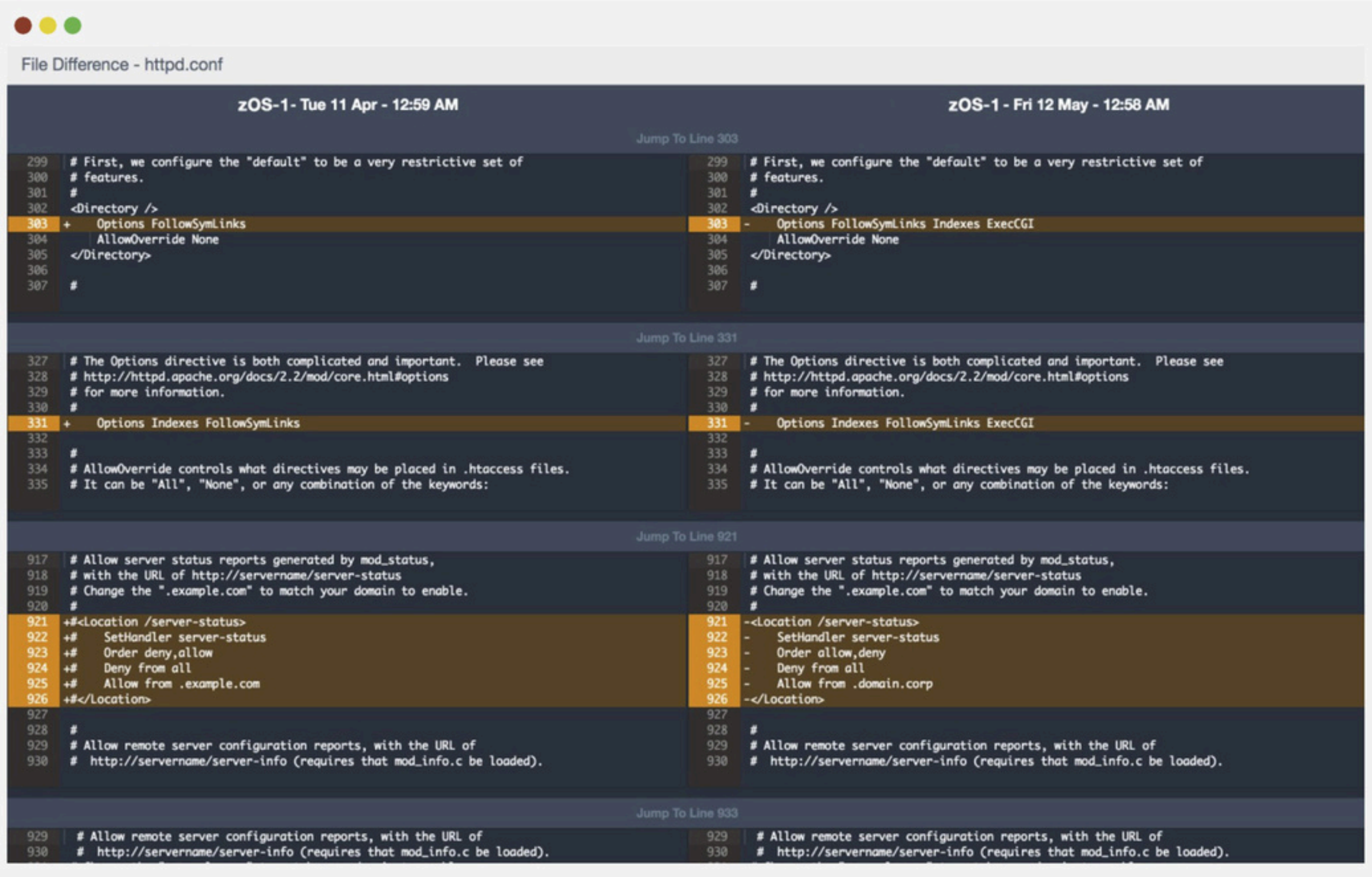
Detailed File Difference Comparison

The Objective

Visibility into file differences and configuration items is critical to being able to determine root cause and ensure changes don’t impact the availability of a system or application. When investigating large configuration files the human eye can overlook obscure modifications, missing minor differences that increase resolution time. When investigating configuration changes that don’t match a golden build or operational state, Guardian visually flags files with changes and offers the ability to view the line-by-line differences in file contents.

The Solution

This advanced comparison helps the investigating team quickly find the misconfigured items down to the exact character that is different. With configuration files such as XML where lines may not match exactly but the values within the tags are important to track, Guardian can normalise this monitoring to treat lines within a file as their own configuration items. The ability to parse configuration files into nodes or sections means that notifications can be configured to alert on changes to salient values, avoiding the need for line- by-line comparisons to understand the significance of a file change.



File Difference - httpd.conf

zOS-1- Tue 11 Apr - 12:59 AM

```
Jump To Line 303
299  # First, we configure the "default" to be a very restrictive set of
300  # features.
301  #
302  <Directory />
303 +    Options FollowSymLinks
304      AllowOverride None
305  </Directory>
306
307  #

Jump To Line 331
327  # The Options directive is both complicated and important.  Please see
328  # http://httpd.apache.org/docs/2.2/mod/core.html#options
329  # for more information.
330  #
331 +    Options Indexes FollowSymLinks
332
333  #
334  # AllowOverride controls what directives may be placed in .htaccess files.
335  # It can be "All", "None", or any combination of the keywords:

Jump To Line 921
917  # Allow server status reports generated by mod_status,
918  # with the URL of http://servername/server-status
919  # Change the ".example.com" to match your domain to enable.
920  #
921 +#<Location /server-status>
922 +#    SetHandler server-status
923 +#    Order deny,allow
924 +#    Deny from all
925 +#    Allow from .example.com
926 +#</Location>
927
928  #
929  # Allow remote server configuration reports, with the URL of
930  #  http://servername/server-info (requires that mod_info.c be loaded).

Jump To Line 933
929   # Allow remote server configuration reports, with the URL of
930   #  http://servername/server-info (requires that mod_info.c be loaded).
```

zOS-1 - Fri 12 May - 12:58 AM

```
Jump To Line 303
299  # First, we configure the "default" to be a very restrictive set of
300  # features.
301  #
302  <Directory />
303 -    Options FollowSymLinks Indexes ExecCGI
304      AllowOverride None
305  </Directory>
306
307  #

Jump To Line 331
327  # The Options directive is both complicated and important.  Please see
328  # http://httpd.apache.org/docs/2.2/mod/core.html#options
329  # for more information.
330  #
331 -    Options Indexes FollowSymLinks ExecCGI
332
333  #
334  # AllowOverride controls what directives may be placed in .htaccess files.
335  # It can be "All", "None", or any combination of the keywords:

Jump To Line 921
917  # Allow server status reports generated by mod_status,
918  # with the URL of http://servername/server-status
919  # Change the ".example.com" to match your domain to enable.
920  #
921 -<Location /server-status>
922 -    SetHandler server-status
923 -    Order allow,deny
924 -    Deny from all
925 -    Allow from .domain.corp
926 -</Location>
927
928  #
929  # Allow remote server configuration reports, with the URL of
930  #  http://servername/server-info (requires that mod_info.c be loaded).

Jump To Line 933
929   # Allow remote server configuration reports, with the URL of
930   #  http://servername/server-info (requires that mod_info.c be loaded).
```

Cloudhouse™

“Now we have an automated, scalable process that strengthens our regulatory stance and reduces risk.”

VP of Technology, Intercontinental Exchange

Supported Systems and Integrations

CI/CD Integrations	TeamCity, Bamboo, CircleCi, Jenkins, IBM UrbanCode, Team Foundation Server
Communications Integrations	ServiceNow, FreshService, Ivanti, BMC Slack, HipChat, Jira, PagerDuty, Zapier, Webhooks
Windows Servers	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Linux Servers	Solaris 10+, AIX 5+, ESXi 5.5+, HPUX, Debian, Ubuntu, Redhat, Suse, CentOS, Mac OS X, Amazon Linux
Cloud Services	AWS, Azure, GCE, Salesforce, Cloudflare, Okta, Google Apps
Databases	Microsoft SQL, MySQL, Oracle, Postgres, Sybase, DB2
Network Devices	ArubaOS, Arista DCS, EOS, Cisco IOS, Cisco NX-OS, Cisco ASA, Cisco FWSM, Cisco CATOS, Cisco ACE, Citrix NetScaler, F5 BigIP, F5 Linerate, HP Comware, HP Procurve, Juniper JunOS, Juniper ScreenOS, Palo Alto Networks Firewalls, Riverbed Steelhead, Riverbed CMC, Fortigate, and more.

Cloudhouse™

Guardian by Cloudhouse™

Contact us today to establish your single source of truth for drift and compliance.

General Enquiries

EMEA: + 44 (0) 203 515 1505
Americas toll free: +1 (833) 518
6537 sales@cloudhouse.com

getguardian.io
cloudhouse.com