

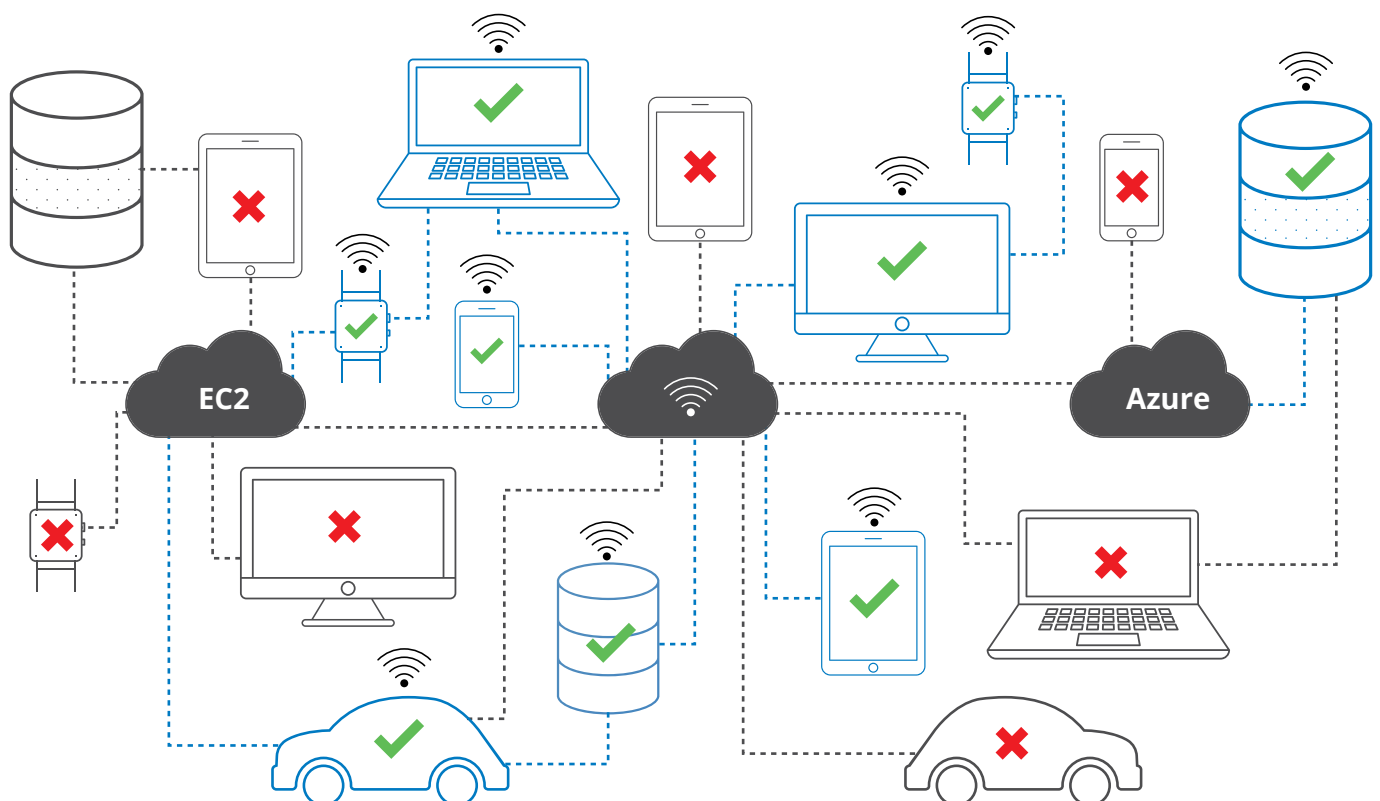
A SOLID FOUNDATION FOR INFOSEC INFRASTRUCTURE



INTRODUCTION

Complete, unobstructed visibility of your IT environment is the foundation for effective cybersecurity. Without a full, detailed inventory of all your IT assets, your InfoSec team won't be able to properly protect your organization because the things that pose the highest risk are the ones that you don't know are there.

For a long time, this basic requirement was fairly simple to fulfill. Network perimeters were well-defined and IT environments were tightly encapsulated. Accounting for and monitoring all the hardware, software and networking elements in these self-contained and sealed IT environments was straightforward.



Unfortunately, that time is gone. Network perimeters have been extended, blurred and erased, as organizations pursue the business advantages offered by digital transformation technologies and practices such as:

CLOUD COMPUTING	MOBILITY	BYOD
Cloud Computing, which has driven out of organizations' premises an ever increasing number of applications, IT infrastructure resources, and app development and delivery tools, making them instead available over the internet and hosted by vendors	Mobility, which has made roaming smartphones, tablets and laptops the preferred end user devices, displacing the static desktop PCs that live in — and never leave — corporate offices	BYOD (Bring Your Own Device), consumerization of IT, telecommuting, Shadow IT and other trends which have loosened IT departments' control over the use of computing products for work, and empowered employees to access the corporate network, applications and data from personal devices, public Wi-Fi networks and consumer web and mobile apps
THE INTERNET OF THINGS	E-BUSINESS	
<p>The Internet of Things (IoT), which is adding hordes of new — and poorly protected — endpoints to IT environments, as previously offline “things” get online, are equipped with sensors and gain the ability to transmit data and be remotely managed. Some of the categories of new IoT endpoints that IT departments suddenly have to keep tabs on and protect include:</p> <ul style="list-style-type: none"> • Vehicles • Appliances • Medical devices • Industrial machinery • Building equipment (e.g., HVAC, BACnet) 	E-business, which has exposed via the internet a wide variety of internal systems to customers, partners and employees, increasing exponentially the number of external communications and transactions handled by the average organization, along with the risk of breaches	

As a result, compiling a complete asset inventory and keeping it up to date has become much more difficult and complex. This is a big problem.

Many organizations are finding that their InfoSec infrastructures now stand on wobbly foundations because they have lost the visibility they once had over their IT assets. As these blind spots multiply within an IT environment, so does the risk of hacker intrusions, data breaches, malware infections, internal IT policy violations and regulatory non-compliance.

IT Asset Inventorying Lays the Foundation for an Organization's Security Infrastructure



TOP 5 CIS CONTROLS

CSC 1:

Inventory of Authorized and Unauthorized Devices.

CSC 2:

Inventory of Authorized and Unauthorized Software.

CSC 3:

Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

CSC 4:

Continuous Vulnerability Assessment and Remediation.

CSC 5:

Controlled Use of Administrative Privileges.

There's a reason why the Center for Internet Security (CIS) puts at the top of its 20 Critical Security Controls these two:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software



CIS estimates that organizations can slash their risk of cyber attack by a whopping 85 percent¹ if they apply these two controls, along with the next three:

- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges

In other words, getting IT asset inventory right is crucial.

After releasing the most recent version of the 20 controls in 2015, CIS published the document "Practical Guidance for Implementing the Critical Security Controls", where it explained that the purpose of the first one — Inventory of Authorized and Unauthorized Devices — is helping organizations define "a baseline of what must be defended."²

"Without an understanding of what devices and data are connected, they cannot be defended," reads the guide.

CIS recommends starting with the placement of active and passive scanners on the organization's network to detect devices.

"This inventory process should be as comprehensive as possible," the guide reads.

The next step is preventing unauthorized devices from joining the network via network level authentication, as well as "to understand what is on the network so it can be defended," reads the document.

As Joshua Platz, a senior consultant in Optiv's advisory services practice, wrote recently:

“Not everything that can go wrong on the network is done out of malice. Sometimes employees may not realize the bigger picture when they decide to bring a device and plug it into the network.”³

In an analysis of the CIS controls titled “Leading Effective Cybersecurity with the Critical Security Controls”, SANS Institute called this first one “the foundation” for the rest “because one cannot secure what one does not know about.”⁴



The constant addition and removal of systems from networks gives cyber criminals opportunities to exploit system configuration weaknesses.

“In order to manage this dynamic behavior, an organization needs to set a baseline for what assets are authorized to connect to its network. Once a ‘known good’ asset baseline is established, it can be compared to future baselines looking for unexpected deltas,” reads the study.

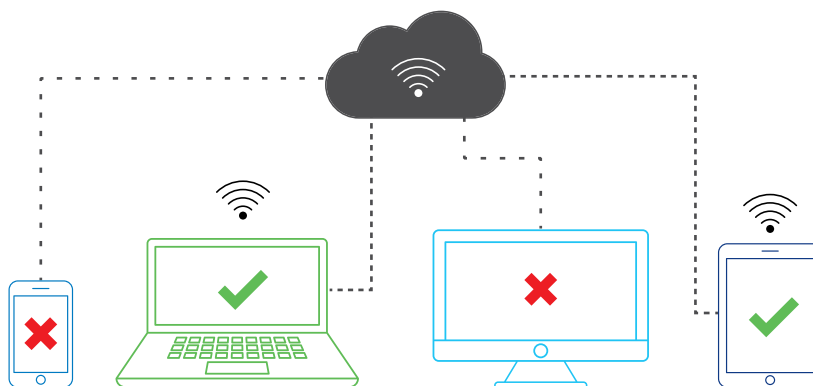
Take the case of the U.S. Department of Transportation (DOT), where a project to revamp and modernize the IT environment uncovered hundreds of consumer-grade, unauthorized networking devices⁵ that staffers had plugged into the network on an ad-hoc basis over the years.

Although the DOT didn’t find any evidence that this precarious security situation had been exploited by hackers, the IT department took concrete steps to eliminate this Shadow IT danger, which is real: Gartner predicts that by 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources.⁶

The DOT drafted specific policies regarding the introduction of new equipment into the network, re-architected the previously flat network and established centralized control and visibility.

“I think it’s really good to start to make sure you have a clear and complete understanding of your infrastructure and your network, your servers and all your connections to the internet,” former DOT CIO Richard McKinney recently told CIO Magazine. “I’m a huge proponent of you’ve got to know what you own, and you’ve got to manage what you know well.”

With regards to the second control — Inventory of Authorized and Unauthorized Software — CIS says its purpose is “to ensure that only authorized software is allowed to execute on an organization’s information systems.”



According to CIS, the most important control to implement at this stage is application whitelisting, which only allows explicitly-approved applications to run.

“While not a silver bullet for defense, this Control is often considered one of the most effective at preventing and detecting cyberattacks,” reads the CIS guide.

But, CIS cautions, successful implementation of whitelisting may require organizations to review their policies. “No longer will users be able to install software whenever and wherever they like.”

In its study, SANS Institute reiterates the whitelisting recommendation, warning that “one of the most common avenues of attack for bad actors is exploiting organizations’ lack of awareness when it comes to software running on their networks.”

The CIS controls were used as part of the U.S. National Institute of Standards and Technology (NIST) process⁷ for drafting its Framework for Improving Critical Infrastructure Cybersecurity⁸, whose methodology is grounded upon IT asset management, reinforcing its foundational importance.

An automated, continuously updated IT asset inventory system provides the foundation for many important tasks, such as:

- Eliminating the need for the time- and resource-consuming effort of inventorying manually
- Improving the efficiency of IT help desk staff by giving them accurate, complete information about assets they’re called to support and troubleshoot
- Optimizing the use of existing assets by making it easier to identify hardware and software that’s underused, completely idle, damaged, obsolete and the like
- Easing regulatory and internal compliance processes that require documenting asset information
- Prioritizing vulnerability remediation work so you patch the critical assets that need the most immediate attention

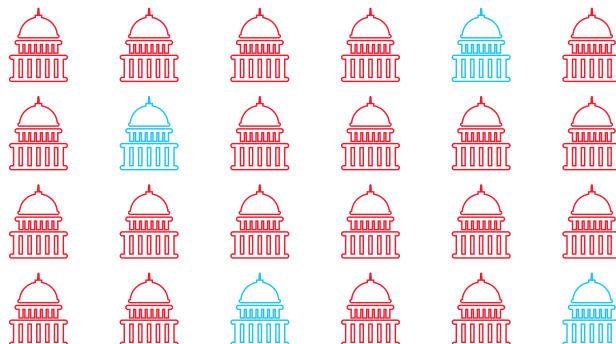
In short, an organization needs to get IT asset inventory right, or else whatever is built on top it, however fancy and sophisticated, will be ineffective.

“In terms of building a house, if the foundation is not properly structured, the integrity of everything built on top of it is compromised. Extending this concept to cybersecurity, if an advanced security solution is architected on top of a flawed security foundation, the solution has an extremely high risk of its integrity being compromised,” SANS Institute states.⁹

But organizations of all shapes, sizes and industries still fall short. Take the case of large U.S. federal agencies: Twenty out of 24 polled recently by the U.S. Government Accountability Office (GAO) had incomplete application inventories.¹⁰

20

**OUT OF 24
GOVT. AGENCIES
INCOMPLETE**



This affects their ability to streamline their software portfolios and “presents a security risk since agencies can only secure assets if they are aware of them,” GAO noted in its report.¹¹

It’s also an issue in the energy sector, as noted in a recently in a Dark Reading column by Dana Pasquali, a product management leader at GE Oil & Gas.¹²

“While energy companies are moving towards taking advantage of the digital age through more connected, digitally-enabled machines, there is still a gap in having a full view of the assets themselves,” she wrote. “Until you can perform asset management, you can’t perform risk management.”

Often, operators and managers lack a complete inventory of assets on the plant floor, even though asset management is crucial for identifying the equipment and systems in need of patches, and for understanding how machines and end points communicate across the plant, according to Pasquali.

“The asset inventory is the first critical step to improving an organization’s security posture before proactive maintenance, patching and hardening of ICS and machine software,” she wrote.

How can your organization avoid flying blind? In this whitepaper, we’ll explain five key capabilities you must have in a cloud-based IT asset inventory system, so that it will provide a rock solid foundation for your security and compliance infrastructure.

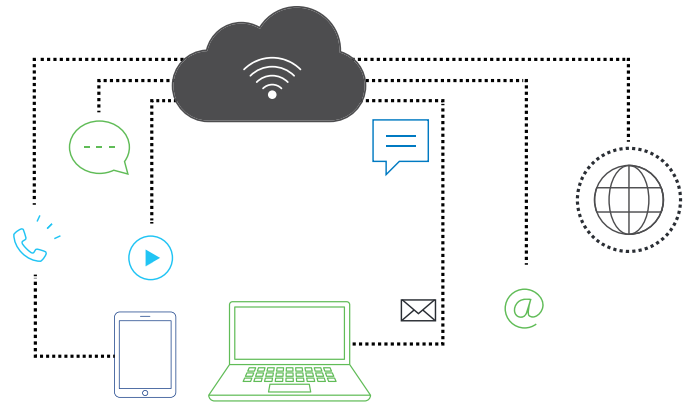
6

KEY CAPABILITIES FOR A CLOUD- BASED INVENTORY

BUT FIRST...

Before diving into the six capabilities, we'll first lay out the reasons why the system should be built upon a cloud architecture.

Aim for the Cloud



Organizations could get away with having only an on-premises IT asset inventory system when the frontier of their network perimeter was solid and unchanging. During that time, IT departments had solid grips over the IT environment and tight control over end users.

As we explained earlier, this is no longer the case. Organizations have hybrid IT environments, with IT assets on-premises, in public and private cloud instances, and on mobile endpoints. Legacy, on-premises tools for IT asset inventory lack capabilities to detect assets in these upended, heterogeneous IT environments. They may be unable to peek into cloud platforms, and their data collection tools may only work in a narrow set of devices.

For many organizations, the logical next step has been to try to complement these tools with other on-premises point solutions, and plug the functionality gaps. But attempting to manually compile a best-of-breed asset inventory system from various vendors often backfires because:

- The costs of acquiring, deploying and maintaining the new software and its companion infrastructure add up
- The complexity of integrating and managing this heterogeneous bundle may require hiring consultants and full-time specialists
- The solution may be difficult and expensive to scale
- Scans may need to be triggered manually or programmed according to arbitrary windows and schedules, instead of running continuously on “auto pilot”
- Data may be collected and stored in different repositories and formats by the various products, making hard or outright impossible to index, analyze and consolidate via a single dashboard

- The bundle may quickly fall short, requiring more point solutions to be bolted on, due to the business’ adoption of more emerging technology for digital transformation

A costly, inflexible on-premises bundle whose cobbled-together pieces don’t play well with each other will prevent you from quickly reacting to security and compliance challenges, such as:

- The daily disclosure of new vulnerabilities
- The increased danger of existing vulnerabilities included in exploit kits
- New and changing government regulations
- The adoption and revision of internal IT policies

The solution, rather, is a centralized, automated and cloud-based inventory system that’s able to collect detailed information continuously from all your IT assets, wherever they reside.

Such a system would harvest all the security, IT and compliance data you need from each asset, and store it in a single, uniform repository.

It should have a central dashboard with a report-generation function and a search engine that’s able to resolve complex queries in seconds.

Because the system is hosted and maintained by its vendor, it will be able to scale up to meet your needs easily.

Now let’s look in detail at six key elements this cloud system should have.

6 KEY CAPABILITIES FOR A CLOUD-BASED INVENTORY

**COMPLETE
VISIBILITY
OF YOUR IT
ENVIRONMENT**



The system must give you far and wide horizontal visibility across all of your organization's IT assets — both hardware and software.

Without this expansive, panoramic view, you can't properly secure your IT environment, because you can't protect -- nor defend yourself from -- what you don't know is there, whether it's unapproved personal devices from employees or hacker tools that attackers slipped into your IT environment.

"The asset inventory is the first critical step to improving an organization's security posture before proactive maintenance, patching and hardening of ICS and machine software," Dana Pasquali, a product management leader at GE Oil & Gas, wrote in her Dark Reading article "3 Steps Towards Building Cyber Resilience Into Critical Infrastructure" about the cybersecurity of industrial control systems (ICS).¹³

Tony Sager, Senior Vice President & Chief Evangelist at the Center for Internet Security, told CSO Magazine recently that one of the most frequent questions he gets from organizations interested in implementing the controls is: Where do we start?¹⁴

"For me, the answer was always about 'visibility' — what devices are in your enterprise, what software is running, how is it being operated (patched and configured)? If you don't know what you have, it is hard to defend it," he said.

"These kinds of things provide the basic operational foundation for understanding your environment and where it is vulnerable, spotting the Bad Guys, deploying defenses, and even recovering from the inevitable problems," Sager added.

QUALYS SENSORS:	ON PREMISES		CLOUDS Amazon, Azure, Google, etc.	
	Perimeter	Internal	Perimeter	Internal
Internet Scanners	✓	✗	✓	✗
Scanner Appliances	✗	✓	✗	✗
Virtual Scanner Appliances	✗	✓	✗	✓
Cloud Agents	✓	✓	✓	✓

To deliver this broad scope of discovery over on-premises, cloud and mobile assets, the system needs to rely on a variety of data collection sensors, such as:

- **Physical appliances** that scan IT assets located on your premises
- **Virtual appliances** that remotely scan your private cloud and virtualized environments
- **Cloud appliances** that remotely scan your internet-as-a-service (IaaS) and platform-as-a-service (PaaS) instances in commercial cloud computing platforms
- **Lightweight, all-purpose agents** installed on IT assets that continuously monitor them

This set of sensors should continuously and proactively collect system, compliance, and security data from the IT assets, and feed it to a common, extensible, and central cloud platform, where this information is aggregated, indexed, correlated, and analyzed.

Even with multiple sensors, there may be times where a single asset inventory system is unable to discover all asset data on its own. This could be due to legacy or proprietary discovery engines, for example, a vendor-specific configuration management system. This is why synchronization of discovered assets to and from systems such as a federated CMDB is essential to having complete visibility.

In addition to this far-reaching view of all IT assets, the system must have a powerful search engine that can resolve simple and complex queries in a matter of seconds.

That way, you will be able to get instant answers to questions like:

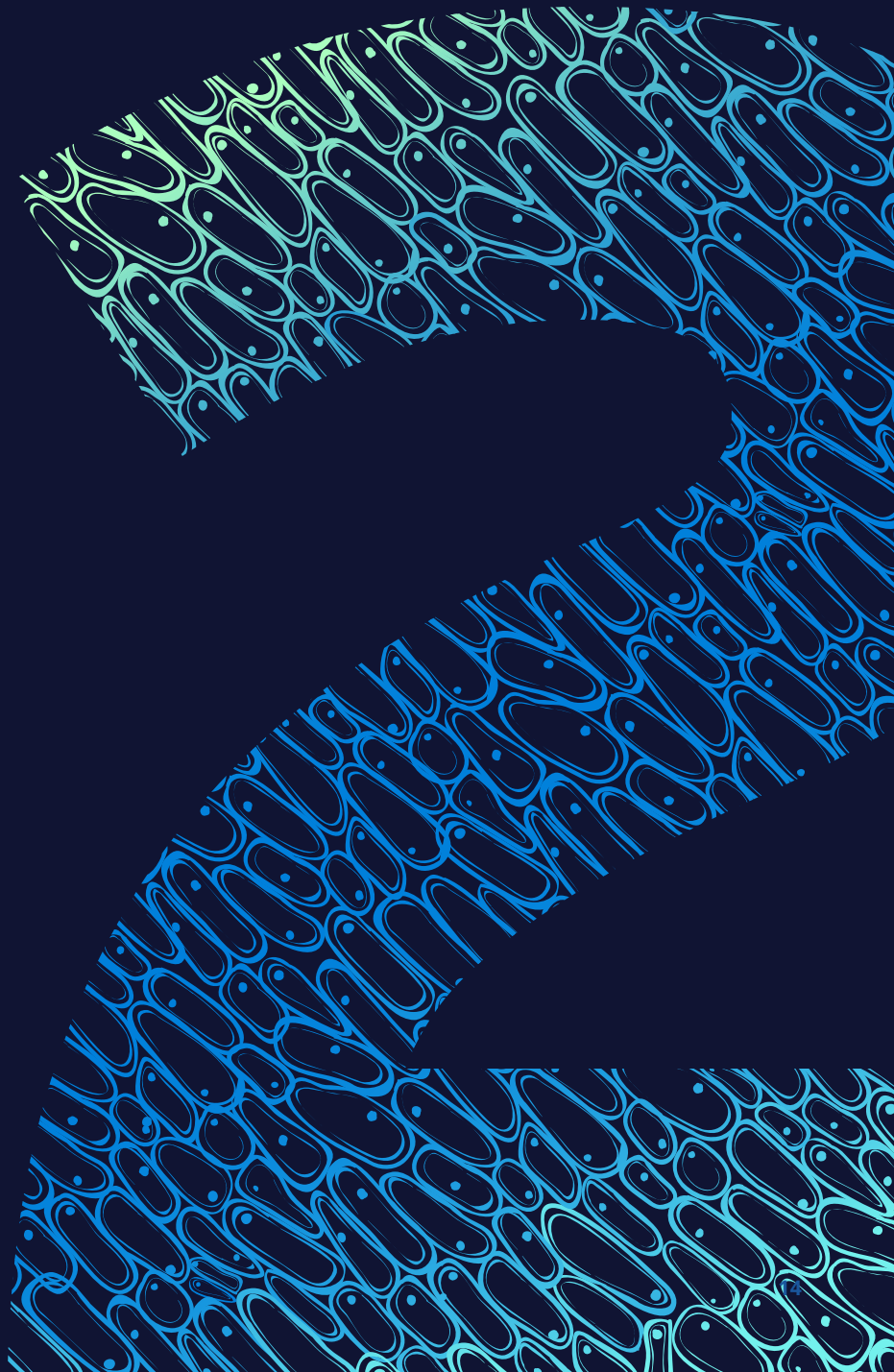
- How many PCs from a particular manufacturer do we have in our environment?
- Which of our IT assets are impacted by a specific vulnerability?
- Which servers are running an operating system that its vendor recently stopped supporting?
- Which IT assets have a particular piece of software installed?

You should also be able to run a query with a combination of multiple criteria to zero in more narrowly on a search, and find out, for example: How many Lenovo laptops running the latest version of Windows 10 and located in my India office have a particular vulnerability?

This continuous process of data collection and discovery is the first step towards having an automated process for IT asset inventory that yields a full, always-updated view of your IT environment.

6 KEY CAPABILITIES FOR A CLOUD-BASED INVENTORY

**DEEP
VISIBILITY
INTO
ASSETS**



Of course, it's not enough to have a complete list of IT assets if the data collected for each one is shallow.

An InfoSec team needs deep visibility into IT assets, including their hardware specs, installed software, network connections, approved users, installed patches and open vulnerabilities.

This profound discovery gives organizations a multi-dimensional view of each asset, encompassing both its IT and security data.

To compile such detailed profiles, automated inventory solutions must aggregate and consolidate data collected using various methods and processes, such as authenticated scans and asset-based agents.

Here's a sampling of IT asset data an InfoSec team should have access to in seconds after querying their inventory system:

Types of IT Asset Data Your Inventory System Should Provide	
<ul style="list-style-type: none">• Hardware type, such as a laptop, server or printer• Hardware manufacturer and model name/number• Total RAM, disk space and CPU count• Operating system and specific version• All installed software, including applications, drivers, utilities and plug-ins, and their respective versions• Virtualized environment details, including images inside and outside of the environment• Asset name, IP address• Geographic location and time zone	<ul style="list-style-type: none">• Services, file systems, running processes and registry keys• Last time the system was booted up• Approved user accounts, and record of their log-ins• Network adapters• Open ports• Installed patches• Existing vulnerabilities• IT policy compliance settings

The system should index all these data points so that you can craft queries that combine any of them, allowing you to get answers for very specific questions related to your asset inventory.

6 KEY CAPABILITIES FOR A CLOUD-BASED INVENTORY

**CONTINUOUS
AND AUTOMATIC
UPDATES**



Having a list of assets that's comprehensive both horizontally and vertically is of limited value if the data isn't continuously updated.

New vulnerabilities are disclosed every day, and old ones can become more dangerous from one moment to the next if, for example, they're included in automated exploit kits.

Meanwhile, an employee's laptop can quickly go from secure to compromised if the user falls victim to a phishing email attack, gets infected with malware or installs unapproved software.

You need to flag these instances as soon as possible, so you can take whatever action is necessary to protect your organization from a potential breach or compliance violation.

For example, in a recent study on the practice of continuous monitoring, SANS Institute stated that critical vulnerabilities should ideally get remedied in one day or less.¹⁵

The reason? The risk of a breach reaches moderate levels at the one-week mark and becomes high when a vulnerability remains in a critical system for a month or longer, according to the study.

Here again an integrated cloud-based platform for automated inventory management edges out a heterogeneous smorgasbord of point products, each focused narrowly on a specific type of IT asset.

The cloud option collects a complete set of IT and security data, providing a holistic view of each asset. It keeps these detailed snapshots in its central repository, and updates them around-the-clock via scanners and agents.

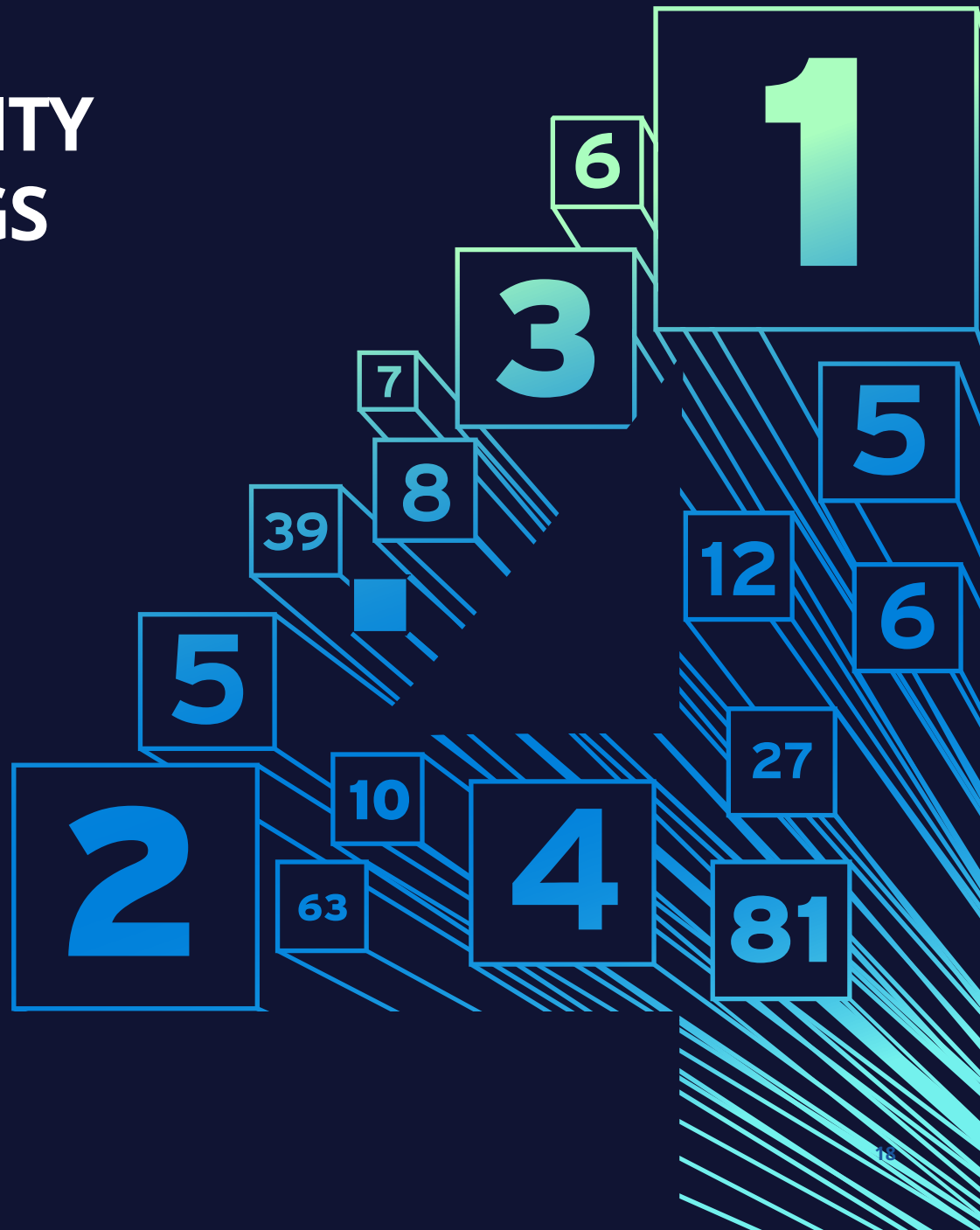


Because the asset inventory system is hosted and maintained by the vendor, customers can scale their usage as much as required without worrying about provisioning hardware and deploying software on-premises.

Organizations can query this scalable, global and extensive inventory and obtain answers and a clear picture of their security and compliance posture in seconds.

6 KEY CAPABILITIES FOR A CLOUD-BASED INVENTORY

ASSET CRITICALITY RANKINGS



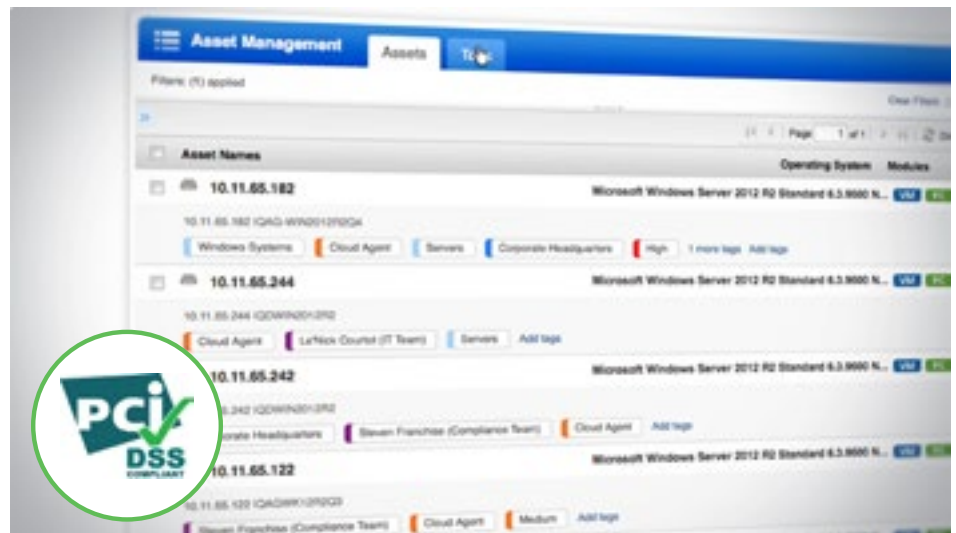
With a complete and continuously updated list of IT assets that includes IT and security details for each, now you need the system to help you highlight and rank the criticality of assets.

Just like not every vulnerability is created equal, not all assets carry the same weight.

Criteria for establishing the criticality of an asset includes:

- Who are its users, and what are their roles and importance in the organization?
- What type of data does the asset handle, transmit and store, and how sensitive is that information -- confidential intellectual property, private consumer data, etc ...?
- To what regulatory and internal compliance requirements is the asset subject to?
- How essential is the asset to the successful operation of the business?
- How attractive is the asset to hackers, how vulnerable is it and how exposed is it to the Internet?

The system should support tagging of assets, so you can slap labels on them and, for example, identify those that fall within the scope of PCI DSS (Payment Card Industry Data Security Standard) compliance.



You should be able to apply tags manually or configure rules and parameters so the system can also automatically stamp labels on assets.

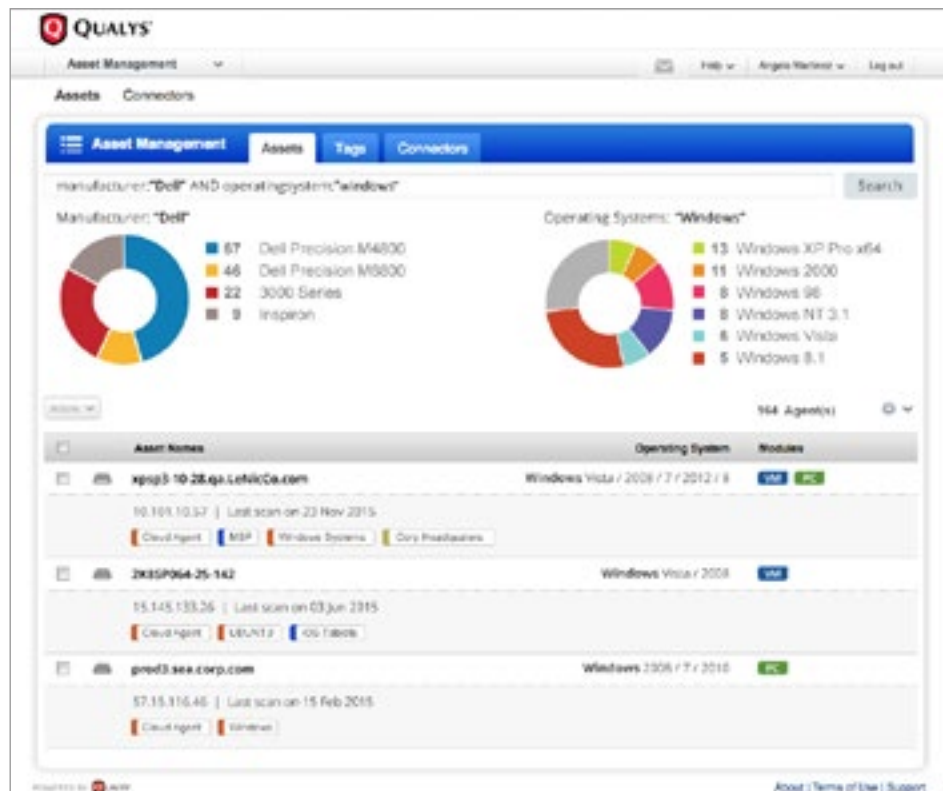
With this categorization data added to the inventory, an asset's criticality can then be calculated based on all the system, security and compliance information collected about it, and on the established hierarchies and priorities, all aggregated and consolidated in the system's cloud-based repository.

6 KEY CAPABILITIES FOR A CLOUD-BASED INVENTORY

DASHBOARDING AND REPORTING



An interactive, customizable dashboard is essential for visualizing the security, configuration and compliance status of IT assets.



We previously discussed the importance of having an inventory system with a powerful search engine that lets you fire off complex ad-hoc search queries against the asset database.

The system should build upon this search functionality and allow you to turn queries that you run frequently into dashboard widgets.

That way, you'll have a constantly updated answer to that query displayed permanently on your dashboard, without having to manually run the same search over and over.


To help you further monitor the status of these assets, the system should display the queried data in various visual ways using graphs, tables and charts.

You also should be able to set certain thresholds, and have the system alert you when they've been crossed by, say, changing the widget's background color from green to red.

The system should also let you create different dashboards tailored for various purposes and users, such as InfoSec pros, compliance/risk managers, and CSOs.

6 KEY CAPABILITIES FOR A CLOUD-BASED INVENTORY

INTEGRATION WITH YOUR CMDB



Another key capability for a cloud-based, automated IT asset inventory system is its ability to link up with your CMDB (configuration management database) and continuously feed it fresh, detailed data.

Although many CMDBs act as their enterprises' de facto IT asset inventories, the truth is that often their information is outdated.

This can be because it's exhausting and time-consuming for staffers to update it, or because the CMDB's native discovery tools are designed for compiling initial inventories, not for capturing subsequent changes.

The solution is to integrate the CMDB with an automated IT asset inventory system that continually detects granular system, security and compliance data on new and changed assets across an IT environment.

When its information is always current and comprehensive, a CMDB is better able to illustrate and map the relationships, connections, hierarchies and dependencies among IT assets.

This allows IT departments to be more effective at a variety of critical tasks, such as change management, service requests, incident response, system repair and impact analysis.

In fact, it's advisable to establish a federated model with automated ways of discovering and exchanging this data among multiple sources, using the CMDB as the main information repository.

A Case Study: Qualys and ServiceNow

A great example of this key element is the integration between Qualys and ServiceNow via a certified application that synchronizes Qualys asset discovery and classification data with ServiceNow's CMDB.

Specifically, the app automatically synchronizes data from Qualys AssetView with the ServiceNow Configuration Management system.

Leveraging Qualys' highly distributed and cloud-oriented architecture, as well as a variety of data collection methods and technologies, including Qualys' groundbreaking Cloud Agents, AssetView compiles and continually updates a full inventory of an organization's IT assets, whether they're on-premises, in the cloud, or on mobile endpoints.

The information can include hardware data such as manufacturer, model, CPU, memory, and disk space, as well as software inventory data such as software name, version, and vendor.

Changes made on a device are immediately transmitted to the Qualys Cloud Platform and then synchronized with ServiceNow.

For joint customers, this means an end to unidentified and misclassified assets, and data update delays, all of which increase the chances of security breaches. Instead, they get real-time, comprehensive visibility into their IT asset inventory so they can flag security and compliance risks immediately.

Conclusion

As we have explained in this whitepaper, many organizations have lost control over their IT asset inventory as they rush to adopt digital transformation technologies that have blurred the boundaries of their network perimeters.

If you find yourself in this predicament, you need to fix it. This lack of visibility into your IT environment undermines the foundations of your enterprise security and compliance infrastructure and puts you at serious risk of a breach: You can't protect what you don't know exists in your network.

To regain a complete, detailed and continuously updated inventory of all your IT assets, wherever they reside (on premises, in cloud instances or mobile endpoints) you need an automated, cloud-based system that gives you the following capabilities:

6 KEY ELEMENTS OF AN IDEAL CLOUD-BASED IT ASSET INVENTORY SYSTEM



Provides complete visibility of your IT environment

- Gives you far and wide horizontal visibility across all IT assets, including hardware and software
- Continuously collects and feeds system, compliance, and security data from IT assets into a central cloud platform for aggregation, indexing, correlation, and analysis
- Offers powerful search and complex query functions with the ability to combine multiple criteria



Gives deep visibility into assets

- Lets you see hardware specs, installed software, network connections, approved users, installed patches, and open vulnerabilities
- Aggregates and consolidates data collected from authenticated scans, asset-based agents, and more
- Indexes data points, giving you the ability to craft queries combining any of them and get answers to very specific questions



Performs continuous and automatic updates

- Collects, keeps snapshots of, and continuously updates a complete set of IT and security data
- Is hosted and maintained by the vendor, allowing you to scale your usage without needing to provision hardware or deploy software on-premises
- Allows you to perform queries and get a clear picture of security and compliance posture



Helps highlight and rank criticality of assets

- Supports tagging of assets for easy labeling and identification
- Gives you the ability to apply tags manually or configure rules and parameters for automatic tagging
- Calculates criticality based on asset's aggregated and consolidated system, security, and compliance data, as well as established hierarchies and priorities



Includes interactive, customizable dashboarding and reporting

- Allows you to turn frequently run queries into dashboard widgets, so you can easily see a constantly updated answer
- Visually displays the queried data in various charts, tables, and graphs
- Lets you create different dashboards tailored for various purposes and users



Integrates with your CMDB

- Enables CMDB to better illustrate and map the relationships, connections, hierarchies, and dependencies among IT assets
- Helps IT departments to be more effective at a variety of critical tasks, including change management, service requests, incident response, system repair, and impact analysis
- Allows the IT asset inventory system to leverage data from the CMDB for vulnerability and compliance management

References

- ¹ <https://www.cisecurity.org/critical-controls.cfm>
- ² <https://www.cisecurity.org/critical-controls/documents/Controls Practical Guidance for Web v4.pdf>
- ³ <https://www.optiv.com/blog/top-20-cis-critical-security-controls-csc-through-the-eyes-of-a-hacker-csc-1>
- ⁴ <https://www.sans.org/reading-room/whitepapers/critical/leading-effective-cybersecurity-critical-security-controls-36797>
- ⁵ <http://www.cio.com/article/3172927/security/how-dot-cio-discovered-a-network-compromised-by-shadow-it.html>
- ⁶ <http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/>
- ⁷ <http://www.prnewswire.com/news-releases/center-for-internet-securitys-response-to-the-national-institute-of-standards-and-technologys-request-for-information-300218699.html>
- ⁸ <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- ⁹ <https://www.sans.org/reading-room/whitepapers/critical/leading-effective-cybersecurity-critical-security-controls-36797>
- ¹⁰ <http://fedscoop.com/agencies-have-incomplete-software-application-inventories-audit>
- ¹¹ <http://www.gao.gov/assets/690/680120.pdf>
- ¹² <http://www.darkreading.com/vulnerabilities---threats/3-steps-towards-building-cyber-resilience-into-critical-infrastructure/a/d-id/1326464>
- ¹³ <http://www.darkreading.com/vulnerabilities---threats/3-steps-towards-building-cyber-resilience-into-critical-infrastructure/a/d-id/1326464>
- ¹⁴ <http://www.csoonline.com/article/3089414/leadership-management/how-to-use-critical-security-controls-to-prioritize-action.html>
- ¹⁵ <https://blog.qualys.com/news/2016/12/05/sans-survey-report-organizations-continuous-monitoring-programs-must-keep-maturing-to-yield-full-benefits>

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 8,800 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. For more information, please visit www.qualys.com. Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.



Qualys, Inc. - Headquarters
1600 Bridge Parkway
Redwood Shores, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys is a global company with offices around the world. To find an office near you, visit <http://www.qualys.com>