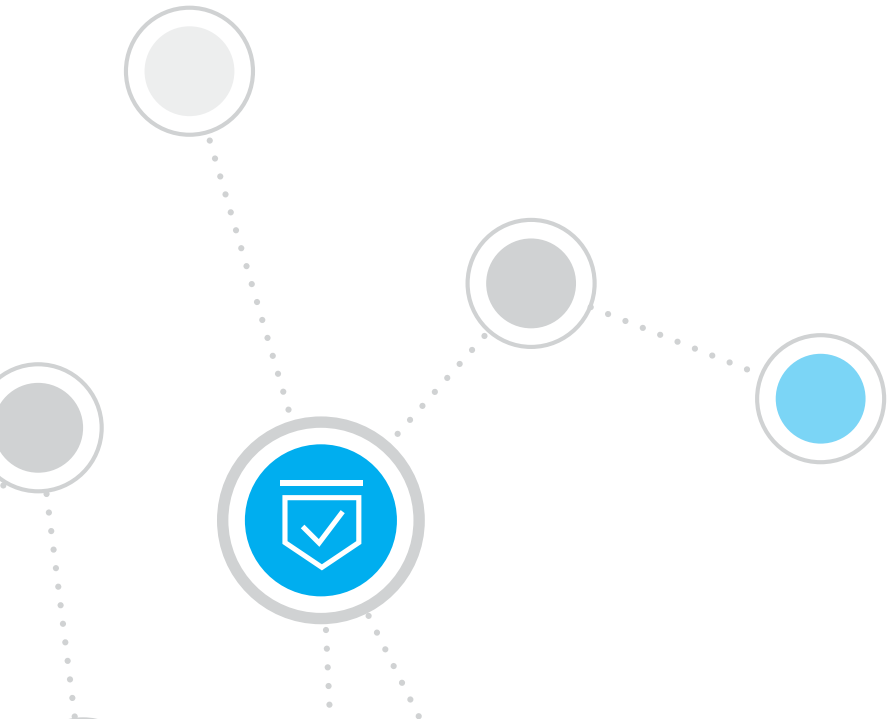
FORESCOUT

Implementing the FAIR Model with Forescout



Why Talk Risk Versus Compliance?

In 2013, Gartner made a bold statement that "compliance with regulations should no longer be the primary consideration of CIOs when planning IT risk and security measures."[1] Gartner further recommended that organizations "change their reactive, check-the-box mindset and start viewing compliance as a risk."[2]

Five years and multiple new regulations later, companies are still struggling with making the transition. As regulatory pressures mount and fines increase, some are questioning whether focusing on risk as opposed to compliance is really worth the effort? The short answer is "yes," with the help of the right technology. And, compliance will also be made easier in the process.

A Risk-Based Versus a Compliance-Based Approach

Traditionally, organizations subject to regulations such as Sarbanes-Oxley, PCI-DSS, NERC-CIP or other federally mandated requirements structured their security assessments to align with those regulations. For example, to avoid PCI-DSS fines, retail and other companies that store cardholder data typically hired a third-party assessment consultancy to create policies that prepared them for a PCI audit or assessment. They then created technical controls or selected existing controls to satisfy the policies. From there, the organization engaged in a "check-box" exercise of comparing the controls periodically to changes in the environment, always trying to stay one step ahead of the audit.

By contrast, a risk-based approach attempts to identify and quantify specific risk targets, thus measuring exposure of those targets. The Factor Analysis of Information Risk (FAIR) Institute defines risk management as "the combination of personnel, policies, processes and technologies that enable an organization to cost-effectively achieve and maintain an acceptable level of loss exposure."[3] This methodology provides a model for quantifying information risk in financial terms. It also complements accepted cybersecurity guidelines, such as the NIST Cyber Security Framework, by providing a financial dimension to the existing technical framework. Does the presence of a risk management framework eliminate the need to focus on compliance? Not at all. The two can work hand in hand.

In this paper, you'll learn how compliance transitions to becoming a critical element in a strong risk management program with the help of the Forescout platform.

What Is FAIR, and Why Should We Care?

The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing information risk. It provides standards and best practices for gauging and reporting on information risk from the business perspective.[4]

The biggest value that FAIR offers businesses is access to a consistent approach to quantifying information risk, thus reducing ambiguity. With a solid foundation on which to build a risk management program, organizations can use the meaningful measures that FAIR helps them to develop to make well-informed decisions.

The FAIR methodology establishes the basics of an effective risk management system as comprising the following elements:

1. Risk – Threats, assets, controls and impact factors that result in loss exposure
2. Risk management – The resulting decisions related to risk governance and how the organization chooses to execute on those decisions
3. Feedback loop – The measures and metrics related to asset-level controls and their efficacy, threat intelligence and losses and overall root-cause analysis data

By utilizing the FAIR methodology, organizations can potentially minimize breaches because threats become more obvious and can be diffused earlier in the kill chain.

Reducing the Risk of Business Interruption from Security Incidents and Breaches

In a nutshell, risk is based on the analytical proposition that loss occurs at a probable frequency and magnitude. In the digital age, a data breach, where tens of millions of consumer records are exfiltrated by an attacker, is a typical example of a catastrophic loss event. Does knowing your risk rating mean that you will never suffer a breach? It won't completely eliminate breaches, but it can lower the frequency of such events and reduce the impact when they do occur. A risk-based approach can help you identify your vulnerabilities and initiate stronger preventative strategies.

Let's explore a few of the most well-publicized breaches this decade:

- **Equifax** - Criminals gained access to certain files in the company's system from mid-May to July 2017 by exploiting a weak point in website software, according to an investigation by Equifax and security consultants.[5]
- **British Airways** - Threat actors likely had access to the British Airways site before the reported start date of the attack on August 21, 2018 – possibly long before. Without visibility into its Internet-facing web assets, British Airways was not able to detect this compromise before it was too late.[6]
- **Anthem -** The large-scale cybersecurity attack on Anthem in 2015 led to potential exposure of 78.8 million consumer records in a data breach. It was caused by a foreign-nation attacker, according to the California Department of Insurance.[7]

In the case of the Equifax breach, where the accounts of 145.5 million Americans were hacked, the threat agents had access to the company's assets, namely the website software, for a period of two-and-a-half months. Hackers exploited a known vulnerability in the Apache Struts web application software, a widely used enterprise platform. A patch for this vulnerability was available, yet the company's controls did not catch the need to apply this patch, nor did they monitor and detect the presence of the threat agents.

Device Compliance and Risk Reduction

Achieving true device compliance can go a long way toward helping you reduce risk.

The maxim, "you cannot manage what you cannot measure" is essential to reducing risk in your enterprise. At Forescout, we believe in taking that maxim a step further and saying, "you can't secure what you can't see."™ Devices that are not visible and are not being actively managed can create blind spots, increasing the potential for a threat agent to exploit vulnerable assets.

Organizations need comprehensive visibility across the extended enterprise – from campus and data center to cloud and operational technology (OT) networks. Without visibility to all your connected devices – from laptops to mobile devices to Internet of Things (IoT) devices – how can you truly protect the enterprise and implement important security measures? In other words, how can you effectively control access to your network, perform network segmentation, ensure device compliance, manage assets and respond to incidents?

Let's take a look at a decision tree that demonstrates how the visibility afforded by the Forescout platform can reduce risk, decreasing both the frequency of loss events and the impact when a loss event does occur.

Forescout Decision Tree

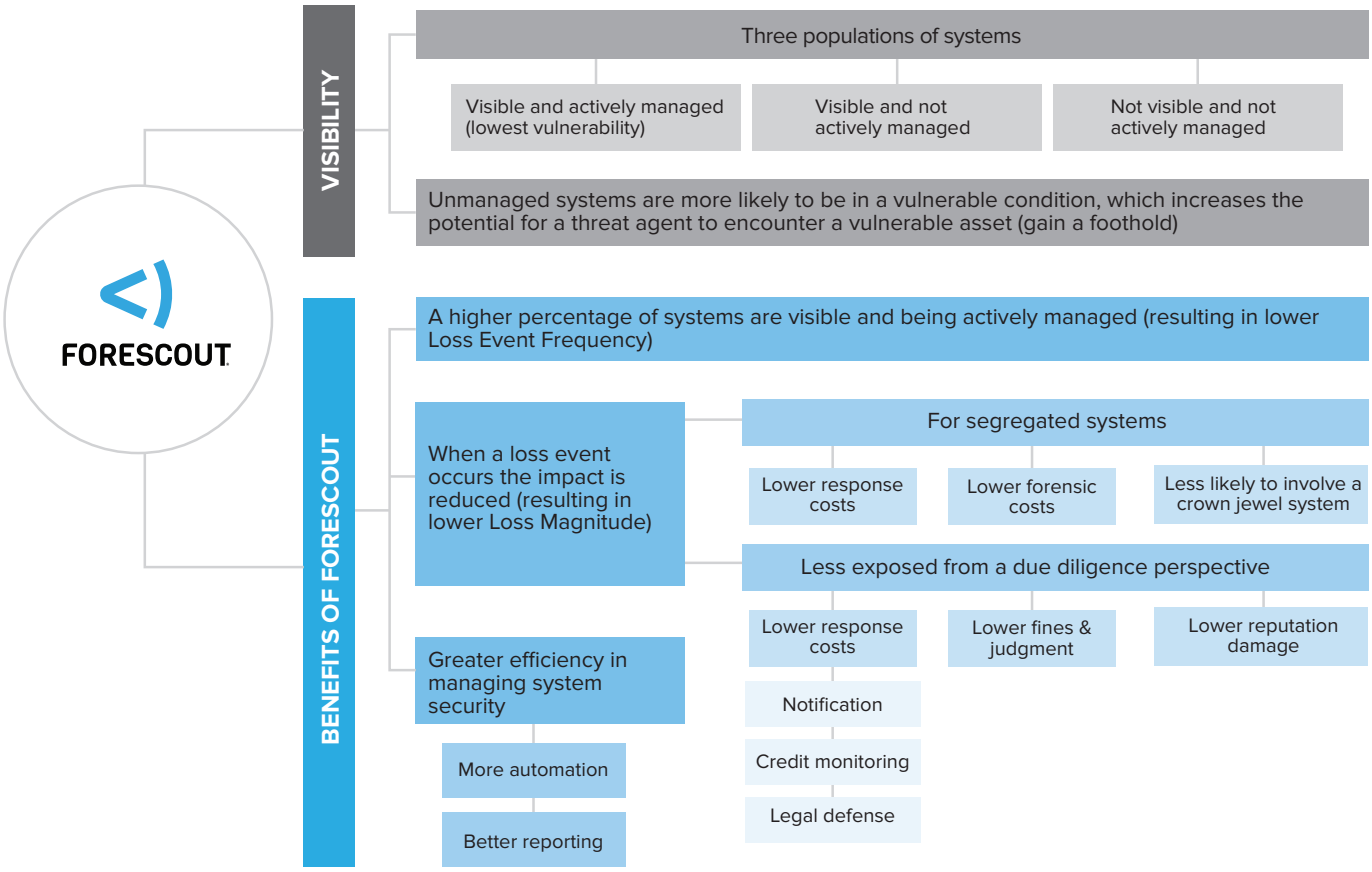


Figure 1. Reducing loss event frequency through complete asset visibility.

IoT Ushers in Greater Cybersecurity Risk

According to Statista, the installed base of Internet of Things (IoT) devices is forecast to grow to almost 31 billion worldwide by 2020.[8] In a related prediction, Gartner estimates that, by 2020, IoT attacks will account for more than 25 percent of the identified attacks on an enterprise.[9]

How Forescout Can Help

When it comes to visibility, there are three classes of devices:

- Devices that have been identified, are visible and are actively managed (least vulnerable)
- Devices that are visible and are not actively managed
- Devices that are not visible and not actively managed

Unmanaged devices are more vulnerable and are more likely to be exploited by threat agents, who leverage them to gain a foothold in your network.

The Forescout platform minimizes this risk through pervasive device visibility. When you have increased visibility to the devices on the network and are able to manage them, loss events like breaches occur less frequently.

Device Visibility: Forescout continuously discovers, classifies and assesses every IP-connected device that touches the extended enterprise network – managed and unmanaged. Our platform enables you to:

- Discover all IP-addressable physical, virtual, IoT and OT devices as soon as they connect – without requiring agents
- Classify, profile and categorize devices, users, applications and operating systems
- Assess device posture and continuously evaluate device state to policy

Minimizing Loss Magnitude Through Effective Network Segmentation

Noncompliant or unauthorized devices on the network pose a huge risk. With our network segmentation capabilities, you can logically separate your network into secure zones. Each zone is compartmentalized and isolated from all others. For example, the server where data is stored can be placed in one segment, and the part of the network where your security cameras are connected can be another segment. There's a wall between the two. When a device like a security camera is hacked, what goes on in that segment stays in that segment. Containing the malware or cybercriminal within just one localized portion of the network minimizes potential damage. Your data stays safe. Not incidentally, segmentation also guards against insider threats because sensitive data and systems can be isolated from "curious" employees attempting to venture where they don't belong.

From a financial perspective, segregating systems through network segmentation has multiple benefits:

- Lower incident response costs
- Lower forensic costs
- Lower likelihood of exposing high-value assets and data

Network Access Control (NAC): Forescout applies unified NAC policies across heterogeneous campus, data center, cloud and OT environments – with or without the 802.1X wireless LAN standard, which provides centralized authentication of users. With our NAC capabilities, you can:

- Automate policy-driven network access based on user privileges, asset compliance and security posture
- Continuously monitor devices and alert IT staff/users or apply remediation actions according to policy
- Restrict, block or quarantine noncompliant or compromised devices

Network Segmentation: Forescout simplifies segmentation planning and automates ACL/VLAN assignment to reduce your attack surface. Network segmentation enables you to:

- Monitor traffic to understand device dependencies and map, plan and deploy network segments
- Assess devices quickly and when needed to automate segmentation assignment
- Integrate with your wired/wireless switches, VPNs, cloud-based management systems and next-generation firewalls to boost ROI

Containing Incidents and Diffusing Threats Through Automation

Lack of sufficient device visibility and intelligence prevents organizations from being able to effectively predict, identify or respond to threats. Most security tools are great at sending alerts but incapable of triggering or initiating actions. The high volume of alerts – including many false positives – requires manual validation and remediation by resource-constrained security operations staff. The ideal solution reduces the attack surface and allows you to automate remediation and incident response.

Incident Response: Forescout automates threat detection, prioritization and containment to accelerate incident response and mitigate risks. This helps you:

- Execute predefined remediation of noncompliant devices at time of connection to reduce mean time to respond (MTTR) and downtime
- Continuously monitor device security posture, incident severity and overall threat exposure to accelerate response
- Gain out-of-the-box workflow interoperability with leading SOAR vendors using Forescout Extended Modules

Ensuring Device Compliance with Appropriate Controls

One of the primary goals of a strong risk management program is to reduce the frequency or probability of a threat agent coming into contact with an asset. In the case of information risk management, hardware tools – including firewalls, switches and routers and technical controls such as network segmentation – can be used effectively to keep the good guys in and the bad guys out. The combination of hardware and software controls increases the level of effort required by threat agents, deterring attacks and reducing risk. Strict security policy enforcement is also a critical element of a comprehensive risk management program. Both proper controls and strong policies are foundational to true device compliance.

In the case of Equifax, one or more devices may have been out of compliance with corporate security policies. The inability to verify that current endpoint security tools are installed, configured and operating properly or that the appropriate patches on the device have been applied signifies that the proper controls are not in place or have not been enforced.

Regulatory compliance often drives an organization's implementation of technical controls. While most regulations are not prescriptive in defining granular controls, some are very specific. For example, PCI-DSS's requirement 1 is: Install and maintain a firewall and router configuration to protect cardholder data. Most companies will adhere to a technical framework as the basis for complying with a specific regulation. One example is healthcare organizations that utilize the HITRUST Cyber Security Framework as a way of ensuring technical controls for HIPAA are met. Other regulations prescribe adherence to a specific technical framework. For example, Defense Acquisition Regulation System (DFARS) mandates adherence to the NIST 800-171 framework of technical controls.[10]

Whether utilizing software, hardware or soft/policy controls, effective technical controls will decrease frequency of adversarial contact and, therefore, reduced risk.

Device Compliance: The Forescout platform continuously assesses devices, monitors them and enforces compliance policies to reduce risk. It helps you:

- Assess the who, what, where, operating systems versions and more of networked devices in seconds
- Detect missing/broken agents without waiting weeks for point-in-time vulnerability scans
- Control system configurations and update weak or default passwords – even on IoT/OT devices

The Role of Asset Management in Reducing Risk

As enterprises grow and evolve, identifying, managing and securing digital and IT business assets become more challenging than ever before. Storing asset information in multiple, disconnected repositories makes it difficult to establish a unified data set and could put assets at risk. Inconsistent data, lack of visibility to mission-critical assets and ineffective security controls can impact compliance.

Digital asset management is the practice of providing an accurate accounting and inventory of technology assets. The problem some organizations face is that they may not be able to see all their assets – for very good reasons. Assets are both inside and outside the corporate perimeter.

They may not be detected by existing monitoring tools. They may be cloud or virtualized workloads. And organizations often don't have a good way to track them. As more and more data is being generated by nontraditional devices and transmitted beyond the network perimeter and back again, valuable digital business assets become vulnerable to attack, which increases risk.

As we have mentioned, managing security risk relative to digital business assets starts by knowing who and what is on your corporate network and beyond the network perimeter. Without comprehensive visibility to connected devices, you will never have a complete and true asset inventory, and you will certainly not be able to track the movement of devices or virtualized/cloud workloads. If your IT department uses manual processes to manage digital assets and data sets, inaccuracy is almost guaranteed, making it impossible to establish a baseline of assets.

Incomplete asset information has consequences:

- It reduces the effectiveness of IT governance operations that depend on CMDB solutions
- It drives inaccurate or incomplete reporting and weakens integration points into technologies and solutions that rely on that data
- It creates headaches for finance and support organizations – they cannot reconcile or report properly with incomplete or inaccurate endpoint data
- It can impact compliance. Preparing for financial and security audits and license compliance requires a trusted, error-free asset inventory

Asset Management: The Forescout platform automates inventorying and maintains accurate asset details across IT and OT networks. Asset management enables you to:

- Maintain an accurate configuration management database (CMDB) with real-time updates to improve operational consistency and reduce manual errors
- Inventory and track agentless devices, including IoT devices, virtual machines and critical infrastructure
- Instantly pinpoint the exact location of all IT and OT devices

Six Steps to Effective Information Risk Management

1. **Select a risk analysis method that will work for your unique business environment.**
   The method you choose must be practical and the results defensible. The FAIR methodology is an open methodology, which was selected by The Open Group as its standard model for risk management. The Open Group is a consortium of over 625 organizations that enables the achievement of business objectives through technology standards. Members include large corporations such as Oracle and IBM.[11]

2. **Establish governance and accountability.**
   NIST Special Publication 800-39 defines governance as "the set of responsibilities and practices exercised by those responsible for an organization"[12] (your board of directors and executive management). This group is in charge of strategically aligning risk management decisions with business objectives, executing the process of risk management, allocating the appropriate resources and measuring and monitoring risk management metrics to ensure goals and objectives are met.

3. **Start with clean data.**
   Quantitative risk analysis is only as good as the data used as input. We've all heard the old adage "garbage in, garbage out." Risk managers who spend the time to improve the quality of the data reap the rewards of a quantitative risk analysis that is more defensible, making it more legitimate. As an example, Forescout customers have discovered 60 percent more devices than previously known.* The Forescout platform continuously discovers all

IP-connected devices – without requiring agents – the instant they enter your network. It provides in-depth visibility into those devices using a combination of active and passive discovery, profiling and classification techniques.

4. **Visualize the big picture.**
   Identify the risks that your organization faces based on the potential frequency of a loss event and the magnitude of the loss. See the risk use cases above for real-world examples of loss magnitude based on a single metric of customer churn.

5. **Focus on reducing the frequency of loss events.**
   You can accomplish this by identifying vulnerabilities – that is, by defining the probability that a threat agent will compromise a system resulting in a loss and by implementing controls to reduce the frequency of a threat event. A camera with a default password poses very little risk if it's still in a box and not powered on. When functioning, that camera could be viewed as a high-risk asset if it is accessed and exploited by a threat actor.

6. **Make continuous improvements.**
   Establish a feedback loop for reviewing incidents and assessing the efficacy of the controls. Forescout uses an agentless approach to detecting devices as they connect to the network, automating simple and repeatable tasks and infusing those elements into existing IT security and management services. With improved process workflow automation, Forescout elevates your information security strategy above traditional point-in-time security models (visibility through snapshots) to a continuous compliance management program, providing ongoing assessment and remediation for the endpoint's connection lifecycle. Continuous visibility can help you satisfy regulatory requirements and strengthen your compliance risk posture.

About Forescout

orescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environment and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, 100-percent real-time discovery and classification, as well as continuous posture assessment.
As of December 31, 2018, 3,300 customers in over 80 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity. **Learn how at www.Forescout.com.**

---

* Based on actual Forescout customer experience.

[1] NewsBytes PH, August 2013. http://newsbytes.ph/2013/08/12/gartner-compliance-no-longer-main-driver-of-it-risk-security-measures/

[2] Gartner Says Risk-Based Approach will Solve the Compliance vs Security Issue: https://www.infosecurity-magazine.com/news/gartner-says-risk-based-approach-will-solve-the/

[3] FAIR Institute, Risk Management: https://www.fairinstitute.org/fair-risk-management

[4] https://www.fairinstitute.org/fair-risk-management

[5] Equifax breach: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[6] British Airways breach: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[7] Anthem breach: https://healthitsecurity.com/news/anthem-data-breach-reportedly-caused-by-foreign-nation-attack

[8] Statista IP devices, 2020: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[9] Network Computing article: https://www.networkcomputing.com/network-security/5-tips-harden-network-security-connected-enterprise

[10] DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting text: https://www.acq.osd.mil/DPAP/dars/dfarspgi/current/index.html

[11] OpenGroup Members: https://www.opengroup.org/elected-member-representatives

[12] NIST Publication: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

Learn more at
www.Forescout.com

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

© 2019. Forescout Technologies, Inc. is a Delaware corporation. Forescout, the Forescout logo, ActiveResponse, ControlFabric, CounterACT, CounterACT Edge and SecureConnector are trademarks or registered trademarks of Forescout. Other names mentioned may be trademarks of their respective owners. **Version 02_19**