Whitepaper

Balancing Security Operations and Compliance

The Security Compliance Trap

Many IT organizations have security compliance requirements that they must achieve in order to meet regulatory guidelines, standards, or regulations to achieve authorization to operate. There is often a challenge for Security Teams in achieving the security compliance goals and ensuring it helps their security operations and can be effectively maintained.

February 2020

Table of contents

Product Notes by:
Dan Carroll, Dell U.S. Federal
Jerry Breaud, VMware

Summary:

The cost of an imbalance between compliance and operational security can lead to costly fines or expensive data breaches that can be difficult if not impossible to recover. Organization have to study and define clear requirements that support both categories and provide joint beneficial outcomes when developing IT transformational goals that will help them with their operational and core business goals.

As data availability continues to expand from the edge/IOT, through the Data Center, and into cloud solutions, the capability to effectively protect data and meet compliance will have to be supported by automation, assessment solutions, and compliance reporting that can drive effective incident response.

Executive Summary

IT organizations continuously work to balance focus, funding and resources to protect business critical data from the ever-emerging cybersecurity threats against their IT infrastructures. Implementing and maintaining an effective cybersecurity framework that accounts for data that is continuously expanding at the edge/IOT to the data center and into the cloud has never been more important. Adding to this complexity is the need to meet more stringent regulatory mandated, guidelines, standards and laws that are being enacted to protect sensitive customer data. Non-compliance can have severe penalties that could include fines, legal implications, or loss of authority to operate.

IT organizations also face the challenge of ensuring that funding requirements can support the work of meeting and maintaining compliance against their daily operational cybersecurity operations to monitor, assess, and respond to real-time threats.

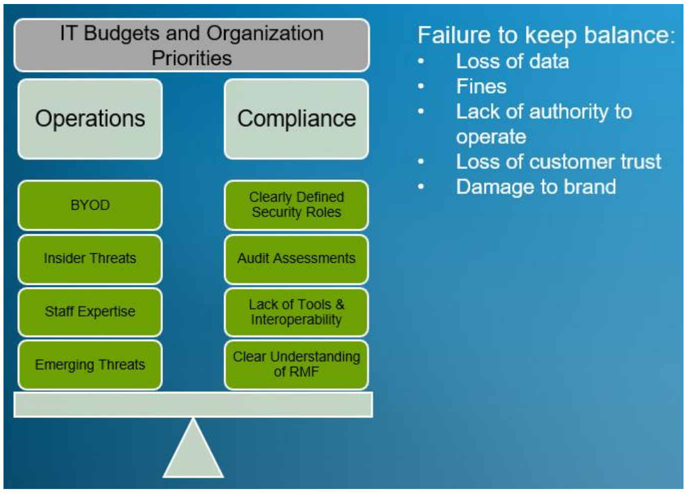

Figure 1: Balancing Priorities

DELL TECHNOLOGIES TRUSTED HYBRID CLOUD

Dell Technologies has developed a cloud-based architecture that can be deployed both in Public, Private, and Hybrid scenarios that utilizes the same core architecture and components that can meet both compliance and operational cybersecurity requirements. The solution utilizes best of breed hardware and software from the Dell Technologies family allowing customers to run on-demand configurable pool of shared computing resources within their own architecture.

1. Introduction

This whitepaper provides an overview of the how the Dell Technologies Trusted Hybrid Cloud solution can help IT Organizations overcome the challenges of implementing a Hybrid Cloud solution that can meet both operational and compliancy cybersecurity requirements.

2. Terminology

- Cybersecurity Framework - A policy framework of computer security guidance that organization implement to assess and improve their ability to prevent, detect, and respond to cyber-attacks.
- NIST – National Institute of Standards and Technology is a non-regulatory agency under the U.S. Department of commerce charged with the mission of fostering innovation and competitiveness in technology development.
- NIST SP 800-53 – NIST Special Publication 800-53 is a catalog of security controls that leverages people, processes, and technology to protect information and information systems. It is used as the security control building blocks of an effective cybersecurity or risk management framework. It is also used or reference to define the requirements for various industry and government regulatory requirements. It is published and maintained by NIST
- HIPAA - The Health Insurance Portability and Accountability Act was created primarily to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft.
- PCI DSS - PCI-DSS are multi-faceted security standards that include requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The standards are intended to assist organizations in protecting customer account data.
- SIEM – Security Information and Event Management provides centralized security event management, correlation and normalization for context and alerting and reporting.
- HIPAA - Health Insurance Portability and Accountability Act was enacted to define flow of patient healthcare data and how it should be protected from fraud and theft.
- NERC CIP - North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system.
- PCI - Payment card industry (PCI) compliance standards require merchants and other businesses to handle credit card information in a secure manner.
- FISMA - Federal Information Security Management Act of 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for their information and information systems.

3. The True Cost of Compliancy VS Operational Risk

Organizations spend large sums of money and resources in the pursuit of regulatory compliance. As an example, the American Hospital Association estimated that the healthcare industry spends around $39 billion annually to pursue regulatory compliance requirements. For an average size community hospital that equates to $7.6 Million a year. [i]

The spending on compliance has not decreased the increase in ransomware attacks against hospitals which has seen an 89 percent increase in Q3 of 2019. [ii]

Even with the amount of money spent on regulatory compliance the healthcare industry still incurs a cost of $3.92 million per data breach globally with the U.S. average being $8.19 million per breach. [iii]

This data shows that an increase in compliancy spending does not decrease the risks of attacks and does not necessarily improve risk response.

3.1 GOVERNMENT RISKS

Governmental risks of non-compliance or lack of operational effectiveness goes beyond the financial. National security, country infrastructure, and free elections are all cyber-targets of bad actors. Attacks on these and other critical services provided by the government could destabilize the economy, the populace, or the nation.

A 2017 audit of the U.S. government's Office of Personnel Management (OPM) suggested that many agencies, including the OPM, still have a long way to go to get their security programs off the ground, government organizations must build trust with the private sector and tap companies in the security industry to guide their efforts.

The OPM audit found that while the agency had improved its overall data protection program, a moratorium implemented during fiscal year 2015 on all security assessment and authorization activities effectively weakened its security posture. The following year, the OPM authorized a sprint that was designed to bring all systems into compliance.

The results of the most recent audit showed that after the sprint Two-thirds of the wide area network (WAN) and local area network (LAN) security controls the inspection team tested were found to be either not satisfied or only partially satisfied. The auditors opined that in this state, the likelihood of being able to identify vulnerabilities is significantly reduced.

Even more critical is the absence of a standard LAN/WAN system security plan (SSP). In the auditor's view, the SSP completeness is foundational. Without it, security teams lack inventory controls and knowledge of what is present within the network.

Even with the mixed results of cybersecurity improvement efforts providing mixed results the U.S. Government continues to increase its spending. For the FY 2020, the Department of Homeland Security (DHS) requested a total of $1.92 billion for its entire cyber security budget, making it the second-largest budget among the government agencies. The Department of Defense (DoD) had the biggest proposed cyber security budget with a request of $9.6 billion. Overall cyber security spending in the United States is projected to increase by approximately 5 percent in FY 2020. Total proposed agency cyber security funding in 2020 is $17.44 billion. [iv]

The challenge that faces government procurement agencies is, even with the increased budgeting how do IT organizations ensure that their cybersecurity investments yield both operational improvements as well as compliance requirements.

3.2 REDUCING THE COST AND RISK

Analysis from the "Cost of a Data Breach Report 2019", conducted by the Ponemon Institute[v] found that key factors from the make-up of the security team an organization has in place, to the complexity of the IT environment, tended to influence the cost of a data breach. Elements that drove down costs included:

- Formation of an incident response team and regular testing of the incident response plans
- Automation technologies including AI and automation in the incident response orchestration
- A comprehensive security operations approach that instills security testing and design into the development process of IT solutions

Cloud transformation increased the total cost of a data breach. Key recommendations to reduce the risk and cost associated with data breaches and cloud transformation include:

- Discover, classify and encrypt sensitive data
- Identify database misconfigurations
- Minimize complexity of implementation and maintenance of IT and security environments from the edge through the data center and into the cloud
- Investment in governance, compliance and risk management programs

4. They Key to understanding Cybersecurity Compliance

The National Institute of Standards and Technology published Special Publication 800-53. NIST SP 800-53 provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). These controls are used as reference control requirements for many U.S. based regulatory requirements to include HIPAA, CIP, NERC, PCI, FISMA, FedRAMP, and many others.

When an IT organization is assessing their IT solutions for compliance they are assessing the solution features and capabilities to the NIST SP 800-53 security controls, either directly or through the regulation or directives translation of the control. IT organizations often face the challenge of ensuring they have the capability to interpret the regulatory requirements and security controls effectively to ensure the solution can meet compliance.

5. The Key to Effective Cybersecurity Operations

IT Organizations are tasked with ensuring that their services fulfill a primary obligation of supporting the core business requirements of the company, or institution. This means ensuring that their IT systems and practices meet the necessary compliance checks in order to pass the necessary security audits and evaluations to achieve authority to operate. The problem arises when this compliance work is viewed as a milestone to be achieved VS standard operational procedure.

The reason many IT organizations view the pursuit of regulatory compliance as a milestone to be achieved is that it is a key requirement when bringing new systems or solutions online prior to integrating them into normal operations to support the core business. The primary challenges of pursuing cybersecurity compliance for systems and solutions are:

- Defining the cybersecurity compliance requirements for the solution as part of the purchasing process
- Ensuring the solution has the necessary features to support cybersecurity operational practices
- Gathering the documentation of proof from the vendor to support the compliancy assessment and reporting
- Obtaining proof beyond the vendor claims that the solution can meet an organizations cybersecurity operational goals

In order to effectively move away from a milestone approach to a standard operational model that integrates cybersecurity compliance, organizations should implement a cybersecurity framework. The framework should be developed to provide guidance and practices on how to assess, protect, detect, and respond to cybersecurity threats as part of normal IT business operations that utilize cybersecurity compliance requirements as keys to ensuring IT solutions have the feature to support the framework operation.

The NIST has published a reference cybersecurity framework that was developed through private and public partnership with the goal of improving cybersecurity practices in the global community. [vi]

The Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks.

Customers can leverage this framework to help them improve their current operational and compliance approach to cybersecurity.

6. Dell Technologies and NIST Collaboration

NIST established their Cybersecurity Center of Excellence (NCCoE) in 2012. The NCCoE is a US government organization that builds and publicly shares solutions to cybersecurity problems faced by the global IT organizations.

Dell Technologies established a Cooperative Research and Development Agreement (CRADA) with the NIST NCCoE focused on establishing a reference architecture that would address security and privacy challenges for the use of shared cloud services in hybrid cloud architectures. [vii]

The architecture that was designed and published through this collaboration provides:

- Implementation of and documentation of the applicable technology based NIST SP 800-53 security controls.

- Continuous compliance enforcement for regulated workloads between the on-premises private and hybrid/public clouds
- Single pane of glass for management, monitoring, and alerts for cybersecurity operations and incident response

Dell Technologies has leveraged this collaboration to develop a commercially available solution that can help customers solve the challenge of leveraging cybersecurity compliance capabilities and operations into a customer's cybersecurity framework implementation.

7. Dell Technologies Trusted Hybrid Cloud

When developing a commercial solution using the NIST NCCoE Trusted Cloud Architecture Dell Technologies defined the following requirements to ensure the technology provided customers with industry leading support for both cybersecurity compliance and operational requirements.

The Dell Technologies Trusted Hybrid Cloud provides the following layered approach to cybersecurity.

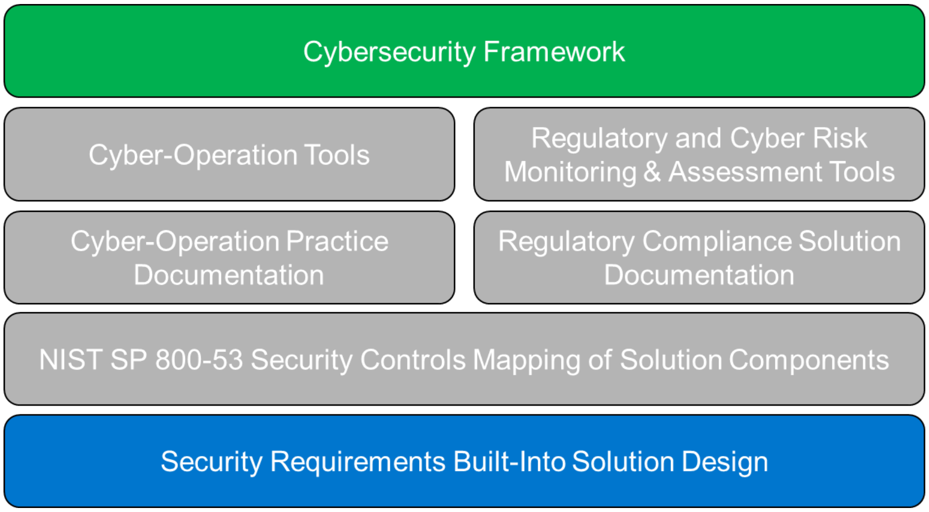
Cybersecurity Framework
Cyber-Operation Tools
Regulatory and Cyber Risk Monitoring & Assessment Tools
Cyber-Operation Practice Documentation
Regulatory Compliance Solution Documentation
NIST SP 800-53 Security Controls Mapping of Solution Components
Security Requirements Built-Into Solution Design

Figure 2: Layered Solution Approach

Dell Technologies approached the Trusted Hybrid Cloud Solution by establishing the NIST SP 800-53 security controls as part of the architecture design requirements. Many products and solutions don't consider security control application until after the core function of the solution is designed and approach the security as a fence to put around the solution. By implementing security control requirements as a design requirement, they become a feature deliverable of the solution and ensure accountability and documentation is achieved across the design process and is built-in VS being bolted on. A built-in security approach provides security features and functions that are easier to enable and manage.

VMware has established a practice of mapping the controls of their solutions into a common control hub database tool. The tool uses the mapped controls to generate documentation sets for various operational and compliancy requirements. This capability was extended across all Dell Technology elements of the solution.

The control mapping is also integrated into the Regulatory and Cyber Risk Monitoring and Assessment Tools. This will allow the customer to understand how changes will affect their compliance and operational cyber-posture before a change is made and to report on the current state of compliance and operations to simplify routine audits and assessments.

Dell Technologies has the necessary tools and components in its portfolio to develop the core structure of the Trusted Hybrid Cloud.

7.1 CONTROL MAPPING

The Dell Technologies Trusted Hybrid Cloud utilizes solutions across the Dell Technologies portfolio including Dell EMC VxRail, Unity XT, and Dell Networking plus solutions from VMware and RSA.

VxRail is built on top of the latest Dell PowerEdge servers with embedded hardware and system-level security features to protect the infrastructure with layers of defense. Breaches are quickly detected, allowing the system to recover to a trusted baseline.

Dell Networking SmartFabric OS10 is a transformational software platform that provides networking hardware abstraction through a common set of APIs.

Dell EMC Unity XT storage provides critical security features, including Integrated Data Protection, encryption, file storage, and replication.

VMware Validate Design VMware Validated Design is a family of solutions for data center designs that span compute, storage, networking, and management, serving as a blueprint for your Software-Defined Data Center (SDDC) implementation. The documentation of VMware Validated Design consists of succeeding deliverables for all stages of the SDDC life cycle.

Dell Data Protection is delivered through the Data Domain Operating System (DD OS) with Avamar is the intelligence that powers Dell EMC Data Domain. It provides the agility, security and reliability that enables the Data Domain platform to deliver scalable, high-speed, and cloud enabled protection storage for backup, archive and disaster recovery.

RSA SecurID uses identity insights, threat intelligence and business context to provide secure access to all of your users, across all of your applications, from the ground to the cloud.

RSA NetWitness Platform provides cyber operation tools that apply advanced technology to enable security teams to work more efficiently and effectively. It uses behavioral analysis, data science techniques and threat intelligence to help analysts detect and resolve both known and unknown attacks. It also uses machine learning to automate and orchestrate the entire incident response lifecycle.

RSA Archer provides the capability to better manage data protection requirements associated with industry standards and global regulations. Improve the classification and assess relationships between risks and controls that pertain to managing data.

Fornetix VaultCore is an encryption key management system that automates the full encryption key lifecycle. It enables secure management of up to hundreds of millions of keys across the entire enterprise from infrastructure to end point with little impact to performance. VaultCore is equipped to employ FIPS 140-2 level 2 validated root of trust.

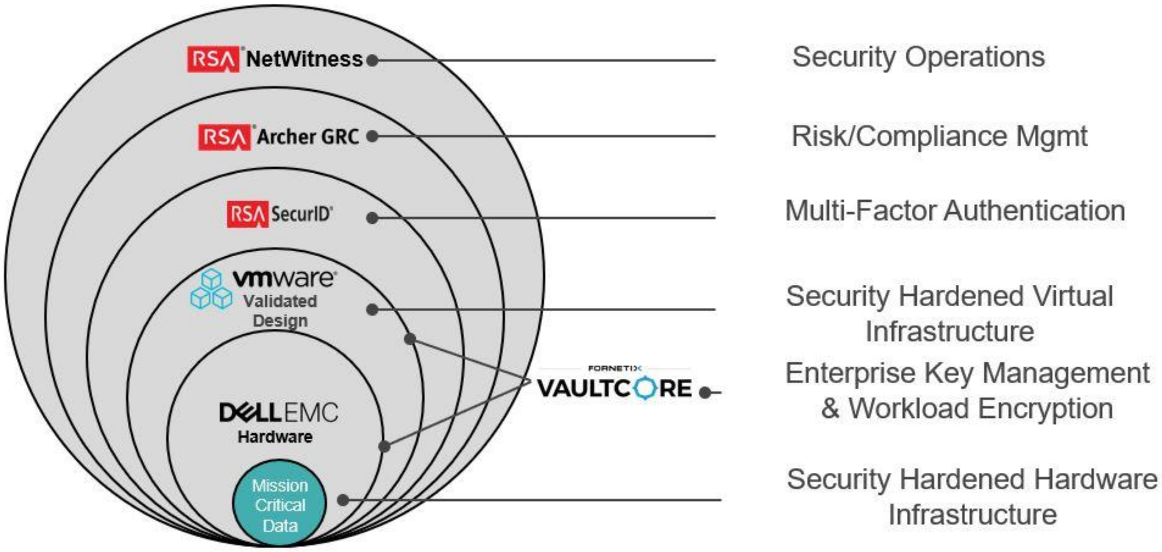

Figure 3 Security from the Center Out

All the components have security control mapping to ensure full support of a comprehensive security design and compliance documentation.

7.2 THIRD PARTY VALIDATION

The Dell Technologies Trusted Hybrid Cloud solution has gone through multiple phases of validation to help a customer understand what they can expect from the cybersecurity posture to assist with their procurement decisions.

The architecture was validated by the NIST NCCoE to meet their defined security goals for a Trusted Hybrid Cloud Architecture.

Dell Technologies employed 3rd party companies to assess the NIST SP 800-53 technical security controls application and attest through their own documentation to the validity of the security control achievements.

Dell Technologies employed a 3rd party company to perform cybersecurity penetration scanning and testing to validate the security posture of the architecture and its capability to protect data as defined in the specification of the solution deployment.

These practices and the produced materials provide reporting and details on the capability of the solution to meet both cybersecurity operational and compliancy requirements.

8. Achieving and Maintaining Cyber Operational and Compliance Balance

IT Organizations need to assess, develop, refine their cyber-security frameworks to ensure they understand what requirements to include in their procurement processes. As has been shown, cybersecurity compliance and operational requirements should support each other. They should ensure that the vendors and solution providers can provide detailed documentation and guidance for the following:

- How cybersecurity is built-in not bolted-on
- The solutions or products have detailed security control mapping documentation to help the customer assess how to integrate the solution into their cybersecurity framework
- Capabilities to monitor and alert on cybersecurity incident response and compliancy requirements

The Dell Technologies Trusted Hybrid Cloud provides a full solution from a single vendor that can help control costs, track, maintain and unify cybersecurity operational and compliance goals with assurance through third party validations.

To learn more about the Dell Technologies Trusted Hybrid Cloud Please contact your Account Rep.

[i] Regulatory Overload, Assessing the Regulatory Burden on Health Systems, Hospitals and Post Acute Care Providers, https://www.aha.org/system/files/2018-02/regulatory-overload-report.pdf

[ii] Malewarebytes Reports a 60 Percent Jump in Healthcare Endpoint Threat Detections, https://press.malwarebytes.com/2019/11/13/malwarebytes-reports-a-60-percent-jump-in-healthcare-endpoint-threat-detections/

[iii] Databreach Calculator, Cost of a Data Breach Report 2019, https://databreachcalculator.mybluemix.net/

[iv] SecurityIntelligence, Government Agencies Must Work with Private Sector to Bolster Infrastructure Security, https://securityintelligence.com/government-agencies-must-work-with-the-private-sector-to-bolster-infrastructure-security/

[v] Databreach Calculator, Cost of a Data Breach Report 2019, https://databreachcalculator.mybluemix.net/

[vi] NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

[vii] NIST NCCoE Trusted Cloud Reference Architecture, https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud/hybrid

Whitepaper: H18115 02/20