WHITE PAPER

Automating IoT Edge Security & Compliance

A comprehensive, software-defined data center solution for overcoming current and evolving IoT Edge security threats

vmware splunk> INFINIDAT accenture

Table of contents

All product names, trademarks, and registered trademarks are property of their respective owners.
All company, product, and service names used are for identification purposes only.

Introduction: The IoT Edge Security Threat

Edge and Internet of Things (IoT) device adoption is at the forefront of digital transformation, with 94% of enterprises projected to be using IoT by 2021.[1] However, Edge and IoT device networks significantly expand the security attack surface, putting enterprise networks at risk.

IDC predicts that by 2025, there will be 41.6 billion connected IoT devices[2] The proliferation of these devices across all industries helps to perform a wide range of functions including security and surveillance, tracking and tracing, energy management, process and supply chain automation, predictive maintenance, inventory management, fleet management, and facilities management.

Enterprises Are Unprepared

Edge and IoT device networks significantly expand the security attack surface, putting enterprise IT networks at risk. Enterprise security systems and telecommunications (telco) customer premises equipment (CPE) are inadequate to meet evolving threats. Forrester Research reports that 67% of enterprises have experienced an IoT security incident.[3] According to the *Unit 42 IoT Threat Report,* 41% of these attacks exploit device vulnerabilities.[4] Weak device security and a lack of security standards for IoT devices make them easy targets. Nearly three quarters (74%) of enterprise security professionals feel that their current security controls and practices are inadequate for unmanaged and IoT devices.[3]

67%

of enterprises have experienced an IoT security incident.[3]

Gartner estimates that by 2023, the financial impact of cyber-physical systems (CPS) attacks will reach over $50 billion, ten times higher than 2013 levels of data security breaches.[5] The financial, reputational, and compliance risks associated with edge and IoT security threats continue to grow along with conventional and increasingly sophisticated cyberattacks.

Telcos and their enterprise customers require a validated, software-defined architecture that delivers robust security for edge and IoT networks to improve security event detection, automate compliance, and reduce the recovery time from breaches.

The IoT Edge Security Platform

The IoT Edge Security Platform described in this paper provides a validated framework for telcos and their enterprise customers to build consistent, certified security infrastructure in a software-defined data center (SDDC) architecture utilizing best-of-breed components. These include VMware Validated Designs (VVD) for SDDC implementation; Splunk Security Information and Event Management (SIEM) for real-time security monitoring, threat detection, forensics, and incident management; and Infinidat's InfiniBox®, delivering high-performance, high-availability data storage at scale with significantly lower TCO than alternative solutions. This tested and proven solution enables telcos and IoT Edge network owners to achieve the parity in security infrastructure required to significantly reduce risks while cost-effectively meeting governance and compliance mandates.

[1] Microsoft IoT Signal Research Report, July 2019

[2] IDC's Worldwide Global DataSphere IoT Devices and Data Forecast

[3] Forrester State Of Enterprise IoT Security In North America: Unmanaged And Unsecured, September 2019

[4] Unit 42 IoT Threat Report, March 2020

[5] Gartner Predicts 2020: Security and Risk Management Programs

Current and Future State: The Exponential Growth of IoT

Companies across all industries are undergoing digital transformation initiatives by leveraging technology to improve customer experiences, improve efficiency, and enhance operational agility. IoT solutions enable digital transformation by extending software control of physical assets to optimize processes and assets to enhance flexibility, differentiate products and services, drive business growth, and enable new business models for creating competitive advantages.

IoT Enables Digital Transformation

Companies have entered a new era of IoT-enabled production and service delivery by facilitating automatic and real-time interactions among machines, systems, processes, and assets. Challenges throughout the customer lifecycle and supply chain can be minimized by IoT device networks and edge-based compute devices. These sensor networks operate largely outside of traditional enterprise IT infrastructure and security systems. They are used to monitor development cycles, manage warehouses and inventories, and (together with software, cloud computing, and analytics tools) turn raw data from different sources into meaningful predictions that enable maintenance, improve productivity and availability, enhance customer experiences, and add value to business offerings.

Bottom-Line Business Benefits

- IoT reduces repair costs by 12% or more and decreases breakdowns by nearly 70%.[6]
- IoT reduces labor costs by eliminating the need for manual checks, providing 24/7 asset monitoring and control.
- IoT allows organizations to plan better and, as a result, serve customers faster and more effectively.

85%

of enterprises are in IoT adoption, and three-fourths of these have IoT projects in planning.[3]

Exponential Growth

Enterprises across all industries are already making big bets on a connected future. The Internet of Things (IoT) market is expected to grow to 75.44 billion connected devices by 2025, up from 30.73 billion in 2020, with a projected market value of $1.1 trillion by 2026.[7]

The growth of AI-enabled IoT products—which often need to process data and make decisions locally—is one of the key drivers of edge computing. IDC predicts that by 2022, edge computing will be included in more than 40 percent of businesses' cloud deployments, and a quarter of endpoint devices and systems will use AI.[7]

5G Unleashes the Power of IoT

5G telecommunications networks will deliver vast improvements over the current 4G capabilities, enabling extremely fast data speeds at latencies of a mere millisecond. In addition, 5G networks will increase the number of connected devices per unit area by 100x.[8]

Harnessing these advantages will require a comprehensive and integrated approach to security in order to protect telcos, their enterprise customers, and consumers.

[6] Purcell, Tim, IoT Applications in Manufacturing, May 2019

[7] Accenture Technology Vision 2020

[8] Sequeira, Neil, What 5G Means for The Future of Internet of Things, 5G Technology World, January 2019

IoT Edge Security Challenges for Telcos and Enterprises

IoT proliferation presents unprecedented opportunities for telcos and their enterprise customers. However, innovation in the delivery of IoT and edge security infrastructures is sorely needed today. Real-time predictive analytics along with automated network maintenance, threat detection, and remediation are required for achieving competitive advantage.

Much of the promise of a hyperconnected, cyber-physical world is still ahead of us. Klaus Schwab, author of The Fourth Industrial Revolution, predicts that, by 2025, 50% of all internet traffic to homes will be for appliances and devices—not entertainment or communication—and 10% of people will wear clothes and reading glasses connected to the Internet.[9] But, the risks associated with IoT devices today, which already outnumber the world's population by nearly 4X, represent an ever-present and growing threat.

IoT Cyberattacks Surged 300% in 2019

Security researchers at F-Secure reported that cyberattacks on IoT devices increased by 300% in 2019.[10] Aging firmware and architectures, increasingly sophisticated attack vectors, a lack of awareness, and lack of line-of-sight visibility by infosec departments are among the causes of this surge. The reality is that IT departments are often unaware of all the IoT devices on their networks. Traditional security best practices are either inadequate or ineffective for IoT security. In many cases, credentials are hard-coded into the device and may not be unique from device to device, creating a vulnerability that's easily exploited. Further, IoT devices are either completely closed or have limited memory or compute power, making it extremely difficult to install endpoint detection and response software or other security tools. Market pressures to produce low-cost devices, along with the presence of legacy devices further complicate the problem.

The Impact of IoT Cyberattacks

The Irdeto Global Connected Industries Cybersecurity Survey of 700 enterprises in five countries found that 90% of organizations suffering an IoT attack over the past 12 months experienced known (vs. undetected) impacts, which included operational downtime. These included IP theft, compromised customer data, and end-user safety issues.[11] Cyber criminals are aggregating large numbers of infected devices to create botnets that are used in Distributed Denial of Service (DDoS) attacks. In Industrial IoT (IIoT), ransomware attacks are increasingly being used to shut down IoT devices that are vital to operations or critical infrastructure.

The Need for a Telco-Enterprise Partnership

Telecom providers face the same security, governance, risk, and compliance (GRC) challenges as enterprises, as more devices on a network equal more points of vulnerability. Improved network security and data analytics capabilities are required along with traditional core network and service metrics for quality, reliability, and capacity allocation.

74%

of enterprise security professionals feel their current security controls and practices are not adequate for unmanaged and IoT devices.[1]

[9] Schwab, Klaus, The Fourth Industrial Revolution, 2016

[10] Attack Landscape H1 2019: IoT, SMB traffic abound, F-Secure

[11] Irdeto Global Connected Industries Cybersecurity Survey, 2019

Enterprise IoT Vulnerabilities

The security requirements of IoT systems extend well past the traditional information security requirements of confidentiality, integrity, and availability. In general, IoT architecture includes a sensor layer, a network layer, and an application layer. IoT cybersecurity attacks are typically physical, network, software, or encryption attacks.

Physical attacks target the hardware of an IoT system and include breaches at the sensor layer. **Network attacks**, such as DDoS, target the network layer and can be conducted remotely. **RFID attacks** include spoofing, cloning, and unauthorized access to read, change, and delete data.

Sinkhole schemes breach the confidentiality of data and deny service to the network by luring all traffic from a wireless sensor network to a metaphorical sinkhole. **Man-in-the-middle attacks** enable hackers to monitor, eavesdrop, and control communications between two legitimate nodes.

Software attacks represent the greatest risk to IoT networks. Software attacks, such as phishing, can exploit an entire system, resulting in IP or data theft, damage or compromise to devices, and DDoS attacks. **Encryption attacks**, which can take a variety of forms, deduce encryption keys by searching for weaknesses in the encryption algorithm.

Edge Security Challenges

Edge computing fulfills an important role in collecting data from IoT devices and sensors. It enables predictive maintenance, demand forecasting, usage tracking, and more—vital functions for delivering the ROI in IoT. When combined with AI, edge systems can enable continuous improvement for optimizing inventories, reducing errors, and streamlining just-in-time manufacturing processes and supply chain interactions.

Avoiding Upheaval

Just as unmanaged IoT devices represent a significant security threat today, edge devices—which are purpose-built, often with limited security capability—also expand the attack surface. The hard and soft management of a substantial edge infrastructure presents, together with IoT device networks, a challenge for IT and data center staff, who are already stretched thin and dealing with flat or modestly increasing budgets.

Scalability, Security and Manageability

IT, data center, and security teams struggle to enable scalability, manageability, and security as IoT deployments become increasingly complex, and businesses become dependent on edge device-enabled analytics. To help combat these challenges, IoT Edge security platforms need to evolve to include blockchain, machine learning and predictive/prescriptive models that improve security event detection, automate compliance, and reduce the recovery time from breaches.

Operational Challenges

In a Forrester survey of 403 IoT technology decision makers in the U.S. and Canada, 50% indicated that the use of unmanaged IoT devices had grown between 16% and 30% over the previous 24 months.[3] In addition to previously mentioned challenges of poor visibility and inadequate device level security, IT and security teams lack the systems required to address current and emerging threats.

Inadequate Systems

Endpoint systems are designed with agents for managing phones, computers, and tablets. IoT devices, which often run custom or outdated operating systems, lack such ability, rendering them largely invisible to cybersecurity systems.

The lack of integrated asset management functions prevents monitoring by device type, expected behavior, and risk profile. Although network-based security systems have visibility into network connected endpoints, most lack the fundamental ability to accurately identify, track and secure IoT devices.

The Need for Cyber-Physical Convergence

Today's threats are asymmetric, exploiting weaknesses in the physical, digital, and social fabrics of modern enterprises. An Accenture survey revealed that 75% of physical security leaders believe that the convergence of physical and cyber security will reduce threats and vulnerabilities in the physical environment.[12]

Regulatory Challenges

Current regulatory requirements in the U.S. and EU are inadequate for addressing IoT Edge security challenges. Although industry is usually inherently resistant to government regulation, the ubiquitous growth of the IoT landscape, combined with the escalating impact of security threats and breaches, has resulted in widespread recognition of and support for increased government regulation.

Widespread Industry Support

A survey by Gemalto, part of the Thales Group, provides three important points of reference.[13] Nearly half (48%) of respondents indicated that they were unable to even detect if their IoT devices have suffered a breach. Almost all respondents (97%) saw a strong approach to IoT security as a key competitive differentiator.

In addition, 79% said the government needs to provide more robust guidelines for IoT security.

NIST Takes the Lead

The National Institute of Standards and Technology (NIST) issued guidelines under NIST 800-53r4 as a framework for federal agencies and private sector companies in managing IoT risks. NIST has identified what it calls a critical gap regarding baseline IoT security and collaborates with industry on how to better manage risk and privacy in a world where practically every device that uses power will soon be connected to the internet.[15] Integrating these evolving guidelines into daily operations is a challenge for all organizations.

[12] Accenture-Cybersecurity-Report-2020

[13] Gemalto State of IoT Security Report, 2018

[14] NIST Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT), 2018

[15] Considerations for a Core IoT Cybersecurity Capabilities Baseline, 2018

Compliance Challenges

In addition to dealing with security threats and operational challenges discussed on previous pages, IT and security teams must be able to demonstrate compliance with established and evolving regulations, standards, and guidelines for protecting data, privacy, and networks from IoT Edge security threats. Today, few if any teams with large device networks possess the ability to effectively and efficiently meet this need.

Current business challenges, the extension of the attack surface, lack of awareness and visibility, and the immaturity of existing cyber defense systems are part of the problem. A more comprehensive cybersecurity architecture is needed that extends enterprise security compliance and protection to IoT Edge networks and devices.

Compliance is a Moving Target

The operational deployment, management, and day-to-day interactions with IoT Edge devices and configurations, together with the end-of-life data cycle, all need to be dealt with inside of the regulatory set of frameworks that exist today. New architectures must also be highly adaptive, anticipating and responding to a much wider and more rigorous set of industry-level regulatory frameworks that will extend or augment current compliance requirements.

CPE Challenges

Customer Premises Equipment (CPE), which includes a broad mix of hardware, software, applications, and networking technologies has—by and large—not been designed from the ground up with security or integration with the larger connected ecosystem in mind.

Although upgrades to CPE are coming to market at a rapid rate, they are often untested and not designed for holistic monitoring, configuration, and patch management. Wireless routers, for example, are among the most common targets for IoT Edge botnet attacks, which can compromise and degrade both the production network and the reputation of the IP addresses of affected companies.

Global Implications

In connected ecosystems, such attacks can reach unprecedented scale, underscoring the inadequacy CPE/enterprise security integration. The WannaCry cryptoworm did not stop at ransoming the data of individual businesses, but exploited an operating system vulnerability to spread across the globe, infecting 300,000 computers spanning 150 countries in a matter of days. The Mirai malware was used to hijack more than 100,000 Internet of Things (IoT) devices and launch an attack on a domain registration services provider in 2016; since then, even though its original developers were caught, new variants have emerged. One such variant, Satori, spread to 100,000 home routers in 12 hours.[16]

[16] Accenture Tech Vision 2019 Tech Trends Report

The Need for a Comprehensive Solution to Address Current and Evolving IoT Edge Security Challenges

Companies undergoing digital transformation have invested in IoT Edge solutions to improve customer experiences and efficiency, enhance workplace safety, reduce costs, and increase visibility across supply chains. However, escalating cyberattacks and other types of security breaches are resulting in downtime, service degradation, data and IP theft, lack of compliance with evolving regulatory and industry standards, damage to customer relationships, and brand reputation.

Large companies typically have 10,000 to 25,000 network devices in their IT estate, often from over a dozen manufacturers. Most are aging and prone to failure. Further, the sheer scale of devices and connected "things" (growing between 4X and 8X annually for most businesses), creates operational challenges for updates, troubleshooting, and security.

Most companies leave it to the procurement function to replace new devices as they fail, leaving the business with many different types of equipment of varying ages. This low-cost, procurement-led approach may have worked for the previous generation of IT support, where most people accessed data on a PC or in their local data center. But it doesn't work today.

Enterprise IT and security teams lack visibility into and control over IoT Edge networks and devices, and lack the resources, tools, data, and expertise to address IoT Edge security challenges. The opportunities for telcos, particularly with the advent of 5G, are massive, as are the risks as vulnerabilities grow with each new connected device.

The following section presents an overview of a top-down, bottom-up, software-defined data center platform developed through a collaborative partnership between VMware, Splunk, Infinidat and Accenture.

Solution Overview: IoT Edge Security Platform

The IoT Edge Security Platform provides a validated framework for telcos and their enterprise customers to build consistent, certified security infrastructure in a Software-Defined Data Center (SDDC) architecture utilizing best-of-breed components. These include VMware Validated Designs (VVD) for SDDC implementation; Splunk SIEM for real-time security monitoring, threat detection, forensics, and incident management; and Infinidat's InfiniBox, delivering high-performance, high-availability data storage at scale with significantly lower TCO than alternative solutions.

The solution enables telcos and IoT Edge network owners to achieve the parity between security infrastructures required to significantly reduce risks while cost-efficiently meeting governance and compliance mandates.

The IoT Edge Security Platform Addresses Three Fundamental Challenges:

IoT and Edge Security Threats: Edge and IoT device networks significantly expand the security attack surface, putting enterprise networks at risk. Current cyber defense systems and telco provided customer premises equipment (CPE) are inadequate to meet current evolving threats.

Software-Defined Security Architecture: Telcos and their enterprise customers require a validated, software-defined architecture that delivers robust security for Edge and IoT networks to improve security event detection and reduce meantime to recovery from breaches. This requires a scalable, back-end security monitoring platform designed to analyze data from current and evolving CPE.

Compliance and Operational Efficiency: Organizations require a purpose-built infrastructure design that is auditable, scalable, and cost-efficient in order to meet current and evolving governance and compliance requirements.

SOLUTION ADVANTAGES

1 Reduce the risk, liability exposure, and reputational damage associated with IoT Edge security breaches.

Overcome escalating IoT Edge security threats by augmenting current security and CPE product portfolios with robust, validated SIEM infrastructure that significantly increases security event detection and reduces risks from data breaches, fraud, and IP theft.

2 Reduce the cost, deployment, and recovery time for a best-of-breed SDDC architecture for IoT Edge Security.

Implement a proven, validated top-down, bottom-up SDDC architecture for IoT Edge security with automation, orchestration, ITSM, lifecycle management, blueprints, and tools to be deployed in weeks, not months. Top-down design enables alignment with enterprise GRC strategy while bottom-up benefits include automation and simplification of security operations.

3 Ensure compliance with evolving standards and regulations through a proactive, analytic infrastructure.

The sheer volume and exponential growth of IoT device networks, combined with the diversity of connected assets operating outside of the enterprise security perimeter, precludes effective compliance management by security operations teams. The IoT Edge Security Platform is an automated, proactive, self-healing, analytic infrastructure enabling auditable compliance with current and evolving security standards, engineering, and business rules.

4 Achieve previously unattainable scale, performance, cost-efficiency, and volume of data retained.

The effectiveness of IoT Edge security depends on the real-time availability of massive amounts of security information and event data. The combination of Splunk SIEM with Infinidat's multi-petabyte scale data storage in a VMware Validated Design delivered by Accenture enables previously unattainable scale, performance, cost-efficiency, and volume of data retained for analysis to improve visibility, control, and risk mitigation.

Software-Defined Data Center (SDDC) Architecture for IoT Edge Security

The SDDC architecture for IoT Edge Security is a set of validated architectures and designs that encompass the entire set of VMware's Software-Defined Data Center (SDDC) products, Accenture Hybrid Cloud Services, Intel products, and others. These provide standardized architecture designs to help build consistent and certified Hybrid cloud infrastructure with the same value of public clouds.

SDDC Advantages

- Top-down, bottom-up SDDC platform with automation, orchestration, ITSM, lifecycle management, blueprints, and tools to be deployed in weeks not months
- Compliant with Government Rules, Policies and Regulations e.g. NIST 800-53r4, ISO27001, PCI, HIPAA, FISMA, SOX, and CJIS
- Reduces complexity and accelerates time to value
- Integrates converged systems and tools, which meets the business control and compliance demands
- Architecture that maximizes efficiency and reduces TCO
- Delivery by proven integrator and cybersecurity leader Accenture reduces risk and time to deployment

SDDC Deliverables

- Fully integrated, validated, end-to-end cloud solution
- Unified virtual and physical infrastructure management
- Adaptable and extensible automation
- Service-oriented orchestration
- Integration with datacenter management
- Resource monitoring and metering
- Cohesive user experience

Validated Designs Enable Deployment and Operation of the IoT Edge Security Platform

Hardware functions are abstracted and accessed through orchestration building. Functions like routing, switching, firewalling, and storage separation are delivered as a service and integration is made through APIs of the HW and Hypervisor/Governance elements.

Services are built and packaged in profiles through cloud brokerage, offered in a service catalogue. The catalogue can also be integrated into service management.

IT is consumed via orchestration and automation with standard change tickets raised, updated and closed while updating elements and capacity management. Monitors are rolled out as well as security policies such as IDM and Logger agents, while consoles are updated through the process.

Predictive operations update the production system on best practice ops through monitoring event connection to the orchestrator and scheduling.

Governance Advantages

- Driven by risk and maturity models
- Focus on sustainability
- Enables internal discussion driven towards real-world business value

Risk Management Advantages

- Multi-regulation approach
- Purpose-driven architecture design
- Focus on survivability and resiliency
- Allows repeatable outcomes

Compliance Advantages

- Automates management of compliance with multiple, evolving mandates
- Provides audit trail for reporting and mitigation
- Supports best practices for GRC

VMware Validated Designs (VVD)

VMware Validated Designs for the IoT Edge Security Platform provide comprehensive and extensively tested blueprints to build and operate a Software-Defined Data Center.

These provide holistic data center-level designs for adopting the SDDC using VMware software.

What are VMware Validated Designs?

VMware Validated Designs are comprised of a standardized, scalable architecture backed by VMware's technical expertise and a software Bill of Materials comprehensively tested for integration and interoperability that spans across compute, storage, networking, and management. Detailed guidance that synthesizes best practices on how to deploy, integrate, and operate the SDDC is provided to aid end-users and ensure performance, availability, security, and operational efficiency.

Key Benefits for IoT Edge Security Platform

ACCELERATE TIME TO MARKET – Streamline and simplify the usually complex design process of the SDDC, shortening deployment and provisioning cycles

INCREASE EFFICIENCY – Provide detailed, step-by-step guidance to greatly reduce time and effort spent on operational tasks

DE-RISK DEPLOYMENTS AND OPERATIONS – Reduce uncertainty and potential risks associated with implementing and operating the SDDC

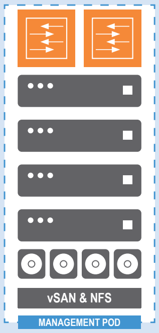
DRIVE AGILITY – Designed for scalability and to support a broad set of scenarios and diverse types of applications, helping IT to respond faster to the needs of the business

IoT Edge SDDC Architecture Overview

MANAGEMENT POD

Physical Layout

- One per Validated Design
- Spans a Single Rack
- 2 Top-of-Rack/Leaf Switches
- Compute: 4 vSAN-Ready Nodes
- Network: vSphere Distributed Switch & NSX
- Storage: vSAN & NFS



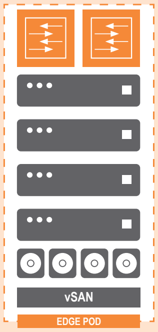
SDDC Components

- Management & Compute Platform Services Controllers
- Management & Compute vCenter Server Instances
- Management & Compute NSX Managers
- Management NSX Controller Cluster
- vRealize Operations Manager Nodes at Scale
- vRealize Log Insight Nodes at Scale
- Additional VMware Validated Design Specific Components

EDGE POD

Physical Layout

- One per Validated Design
- Spans a Single Rack
- 2 Top-of-Rack/Leaf Switches
- Compute: 4 vSAN-Ready Nodes
- Network: vSphere Distributed Switch & NSX
- Storage: vSAN



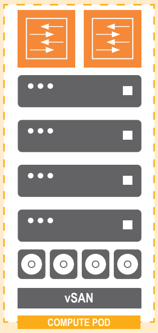
SDDC Components

- NSX Controller Cluster for Compute
- NSX Edge Gateways

COMPUTE POD

Physical Layout

- Multiple per Validated Design
- Spans one or More Racks
- 2 Top-of-Rack/Leaf Switches per Rack
- Compute Capacity to Meet Workload Demands
- Network: vSphere Distributed Switch & NSX
- Any Supported Storage Protocol per HCL



SDDC Components

- Business Workloads
- NSX Logical Switches
- NSX Distributed Firewall
- NSX Edge Gateways for Application Workloads

STORAGE POD

Physical Layout

- NFS, iSCSI and/or FC/CoE, NVMe-oF
- Neural Cache™/ AI/ML
- Triple Redundancy
- Multi-PB scale
- RESTful API, CLI, Web-based

SDDC Components

- Integrations w/ SDDC components vRA, vRO, vROPs, vCenter
- Infinidat's InfiniBox is a software-defined storage platform delivered in a hardened hardware appliance

VMware Validated Designs (VVD) – cont’d

Key Features

Standardized, Data Center-Level Designs: Standardized, scalable architectures comprehensively tested for integration and interoperability among all the software components in the bill of materials.

Proven and Robust Designs: Continuous rigorous interoperability testing validates successful deployment, efficient operations, and ensures that designs stay valid with subsequent versions of components.

Applicable to a Broad Set of Scenarios: A variety of scenario-based architectures – SDDC, IT Automating IT, Intelligent Operations, ROBO – are complemented with guidance to achieve IT outcomes delivered by the SDDC.

Comprehensive Documentation: A comprehensive set of documents describe design objectives, architecture design decisions, a software bill of materials, and extensive documentation on how to deploy, integrate, and operate the SDDC in a single or dual-region environment.

Technical Implementation

VMware Validated Designs are implemented on a collection of common building blocks, referred to as workload domains. Each workload domain represents the logical grouping of hardware and software needed to support specific functions within the SDDC.

Management Workload Domain: Hosts the infrastructure components used to instantiate, manage, and monitor the SDDC, such as Platform Services Controllers, vCenter Server Instances, NSX Managers, and vRealize Log Insight. Cloud management and operations capabilities can be extended with additional solutions (e.g. vRealize Automation). VMware vSAN is recommended for hosting virtual machines running in this cluster, while NFS is used for storing backup images, log, archives, and virtual machine templates.

Shared Edge and Compute Workload Domain: Provides north-south networking access for initial business and end-user workloads. It is located inside the same rack as the management domain.

Additional Compute Workload Domains: As an organization grows, additional compute only workload domains are added to expand the SDDC capacity.

Security Information & Event Management

Disparate and deployed industrial assets and connected devices can provide the enterprise a unique touchpoint to real-world operations and conditions. But collection, storage, and insight of the machine data generated by the Operational Technology (OT) and IoT and Edge Devices can be a challenge.

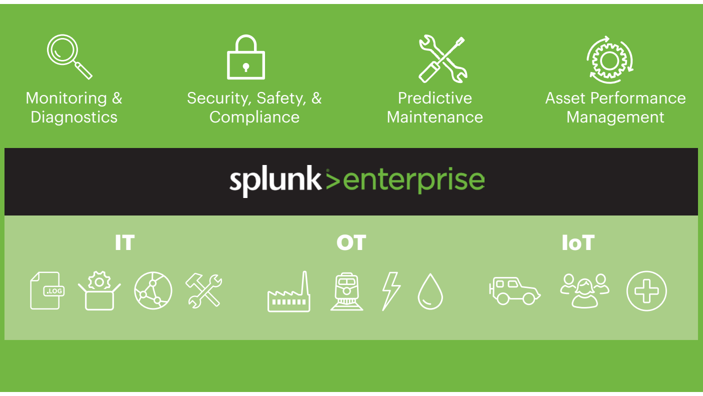
Splunk software collects, analyzes, and visualizes real-time and historical machine data from any source—including operational technology, connected assets, and products—enabling you to improve operations, ensure safety and compliance, perform predictive maintenance, and better manage the uptime and availability of industrial assets. Splunk harnesses the power of the machine data generated by devices, control systems, sensors, networks, applications, and end users connected by industrial networks.

PREDICTIVE MAINTENANCE – Gain real-time insight into asset deployment, utilization, and resource consumption. Recognize patterns and trends, and use operational data to proactively approach long-term industrial asset management, maintenance, and performance.

ASSET PERFORMANCE MANAGEMENT – Achieve real-time insights into the health and performance of your industrial assets. Use machine learning to detect anomalies and deviations from normal behavior to take corrective action—improving uptime, reliability, and longevity.

VMWARE VALIDATED DESIGNS – Enable self-healing, proactive actions based on business and engineering rules, and events generated from integrated components.

- Gain real-time insight from sensors, devices, and industrial and operational technologies
- Collect, manage and analyze the velocity, volume, and variety of data
- Complement and integrate with existing operational technologies



Advantages of Splunk for IoT Edge Security

Monitoring and Diagnostics: Ensure that equipment in the field operates as intended. Monitor and track unplanned device or system downtime. Understand the cause of failure on a device to improve efficiency and availability. Identify outliers and issues in device production or deployment.

SECURITY, SAFETY, AND COMPLIANCE – Help protect mission-critical assets and industrial systems against cybersecurity threats. Gain visibility into system performance or set points that could put machines or people at risk and satisfy compliance reporting requirements.

Splunk Integrates With Leading Cloud IoT Platforms and Services

As businesses build and deploy connected devices, they are also deploying a new generation of commercial IoT platforms and services. These platforms and services enable device connectivity, visibility, and simple provisioning and remote device management. They act as both a gateway to device operations and provide a platform for interaction with remote device operations and performance. Splunk software integrates with leading IoT platforms and enables powerful machine data analytics for the IoT and eliminates the need to build them from the ground up.

.

Enterprise Storage Infrastructure

INFINIDAT

InfiniBox by Infinidat provides multi-petabyte enterprise storage with scalability exceeding 8PB in a single 42U rack, faster-than-all-flash performance, 100% availability, and multi-protocol support with incredible ease of use.

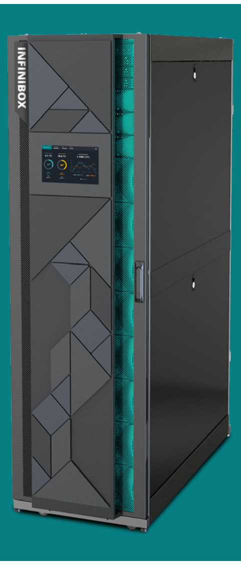
With a disruptive price point, InfiniBox also provides unprecedented value for modern enterprise storage. Available in multiple configurations, InfiniBox enables customers to acquire, store, and analyze the most data to achieve competitive advantage.

Overcoming Traditional Storage Deficiencies for IoT Edge Security

As part of the IoT Edge Security Platform, Splunk enables organizations to gain real-time insight from sensors, devices, and industrial and operational technologies. Splunk SIEM facilitates the collection, management and analysis of the velocity, volume, and variety of data, while complementing and integrating with existing operational technologies. However, the volume of data produced on a daily basis from large IoT Edge networks overwhelms conventional data storage systems, which are not designed to operate cost-efficiently at multi-petabyte scale.

Infinidat Maximizes Splunk Performance and Value for the IoT Edge Security Platform

With Infinidat, Splunk implementations are simpler to implement, operate, and protect while reducing costs and delivering the results that help companies discover, innovate, and drive their success. By running Splunk on InfiniBox, customers can focus on the needs of the business instead of worrying about the cost and complexity of the storage infrastructure. InfiniBox provides the best reliability, the fastest performance, and the lowest TCO at multi-petabyte scale.



InfiniBox®

- Reduce the cost and complexity of storage
- Achieve large capacity at scale to enable long-term data retention and expanded search potential

Infinidat Advantages

SIMPLICITY – With InfiniBox, storage is guaranteed to be fast and reliable – and it can grow without adding servers

FASTER INGEST – Increase the ingest speed and overall amount of data ingested WHILE supporting multiple user reports

FASTER SEARCH – Infinidat AI / ML-based Neural Cache drastically increases cache hit rates versus competitive platforms, guaranteeing faster speeds for Splunk

LONGER RETENTION – Retain massive amounts of security information and event data within primary storage for analysis, eliminating the complexity of managing numerous tiers of storage

FLEXIBLE CONSUMPTION – Match the consumption of Splunk to the amount of storage purchased (multiple CapEx and OpEx options including Elastic Pricing)

LOWEST TCO – InfiniBox provides increased speed and large-scale capacity, at reduced Total Cost of Ownership (typically 30-50% savings)

ANALYTICS AT SCALE – Higher-volume data retention increases the accuracy and resulting value of the analytics

Solution Design and Deployment

Recognized as a global leader in IT services, cybersecurity and the delivery of VMware Validated Designs, Accenture is responsible for the design and deployment of the IoT Edge Security Platform. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains, and services that span the security lifecycle, Accenture protects an organization's valuable assets, end-to-end with services that include strategy and risk management, cyber defense, digital identity, application security, and managed security.

The Accenture VMware Partnership

Since 2004, Accenture has partnered with VMware in the delivery of proven project methodologies and deployments for clients across a wide range of industry sectors. Accenture's VMware Validated Designs encompass reference architecture for the implementation of the IoT Edge Security Platform based on VMware's software-defined data center (SDDC) technology. Benefits include server, network, and storage virtualization along with integrated management and automated provisioning. Accenture brings proven delivery methodologies, architecture frameworks, global delivery networks, and experience in large-scale, industry-specific IT transformation strategies and projects.

Accenture SDDC Validated Design Deliverables

Intelligent Infrastructure and Private Cloud: Leveraging Intelligent Infrastructure enables optimized utilization of converged infrastructure and maximized Return on Investment (ROI).

Automation, Provisioning, and Orchestration: Automation and orchestration is key to ensuring consistency in delivery and the containment of costs. Users can seamlessly provision desired applications, VMs or any other IT need which is offered from the self-service portal.

Intelligent Operations: The intelligent operations suite provides comprehensive visibility across the virtual and physical infrastructure. This is also highly predictable and self-healing, detecting early alerts before impacting business operations.

Metering and Billing: Metering of services introduces improved cost transparency to drive new behaviors with regard to usage. This will reduce over-provisioning and free up underutilized computing and storage capacity.

Hybrid Cloud: Seamlessly integrates with Public and Private cloud for extending the Private cloud for provisioning and workload movement.

Accenture SDDC Solution Advantages

- Fully integrated, validated, end-to-end cloud solution
- Unified virtual and physical infrastructure management
- Adaptable and extensible automation
- Service-oriented orchestration
- Integration with data center management
- Resource monitoring and metering
- Cohesive user experience

Business Benefits

ACCELERATE TIME TO VALUE: Achieve faster deployment of your data center to begin solving IoT Edge security and compliance problems sooner.

GAIN CONFIDENCE IN YOUR SDDC: Build your SDDC using a design validated by experts.

SYSTEM-LEVEL DESIGN: Benefit from comprehensive, top-down, bottom-up data center design, built on VMware product knowledge, and expertise spanning cybersecurity, industry sector, and functional domains.

Summary: IoT Edge Security Platform Advantages for Telcos and Enterprises

IoT Edge Security challenges pose significant security, compliance, and business risks for telecom service providers and enterprises across a wide range of industry sectors. The lack of visibility, security controls, and discovery tools for these assets threatens the economic promise of IoT in facilitating digital transformation for the enterprise and the growth of 5G networks and services for telcos.

The IoT Edge Security Platform provides a validated framework for telcos and enterprises to build consistent, certified security infrastructure in a software-defined data center (SDDC) architecture utilizing best-of-breed components. These include VMware Validated Designs (VVD) for SDDC implementation; Splunk Security Information and Event Management (SIEM) for real-time security monitoring, threat detection, forensics, and incident management; and Infinidat's InfiniBox, delivering high-performance, high-availability data storage at scale with significantly lower TCO than alternative solutions. This tested and proven solution, designed and delivered by Accenture, enables telcos and IoT Edge network owners to achieve the parity in security infrastructure required to significantly reduce risks while cost-effectively meeting governance and compliance mandates.

	TELCOS	ENTERPRISES
CHALLENGES	• Telco-provided CPE is inadequate to meet evolving IoT Edge threats • Cyberattacks against enterprise systems pose ecosystem-wide risk • IoT Edge security risks threaten growth and adoption of 5G	• IoT Edge device networks significantly expand the security attack surface, putting enterprise networks at risk • Enterprise security infrastructures and teams lack visibility and control over IoT Edge device networks
IMPACTS	• Growth of IoT Edge cybersecurity attacks brings increased regulatory, compliance and reputation risks • Cybersecurity will be a critical differentiator for winning 5G network and service market share	• 67% of enterprises have experienced an IoT security incident • 74% of security professionals feel their IoT security controls are inadequate • Cyberattacks on IoT devices increased by 300% in 2019

ADVANTAGES

IoT EDGE SECURITY PLATFORM ADVANTAGES

- Reduce the risk, liability, and reputational damage associated with IoT Edge security breaches through a comprehensive, automated GRC infrastructure.
- Reduce the cost and time to deployment for a best-of-breed, tested, and validated SDDC platform for IoT Edge Security.
- Ensure compliance with evolving governance and regulatory requirements while reducing TCO for security infrastructure and operations.
- Achieve previously unattainable scale, performance, cost-efficiency, and volume of data retained for analysis to improve visibility, control, and risk mitigation.

vmware

VMware software powers the world's complex digital infrastructure. The company's cloud, app modernization, networking, security, and digital workspace offerings help customers deliver any application on any cloud across any device. Headquartered in Palo Alto, California, VMware is committed to being a force for good, from its breakthrough technology innovations to its global impact. For more information, please visit vmware.com.

splunk>

Splunk is the world's first Data-to-Everything Platform. Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver. Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future. With more than 5,000 employees in 27 offices worldwide, we're focused on creating lasting data outcomes for our customers. Visit splunk.com.

INFINIDAT

Infinidat was founded in 2011 by a team of storage industry experts focused on returning business value to customers by eliminating the compromises between performance, availability, and cost, at multi-petabyte scale for enterprise storage. The Infinidat team, spanning generations of storage industry experience and previous product successes, has become an industry leader by developing a better, faster way to store and protect multiple petabytes of data, with the highest possible availability, at the lowest possible cost. All of this work was done with a single goal in mind — help customers empower data-driven competitive advantage at multi-petabyte scale. Visit infinidat.com.

accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, digital, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries — powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 509,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit accenture.com.

IoT EDGE SECURITY PLATFORM

The IoT Edge Security Platform provides a validated framework for telcos and their enterprise customers to build consistent, certified security infrastructure in a Software-Defined Data Center (SDDC) platform utilizing best-of-breed components. The solution enables telcos and IoT Edge network owners to achieve the parity in security infrastructure required to significantly reduce risks while cost-efficiently meeting governance and compliance mandates.

vmware® splunk> INFINIDAT accenture