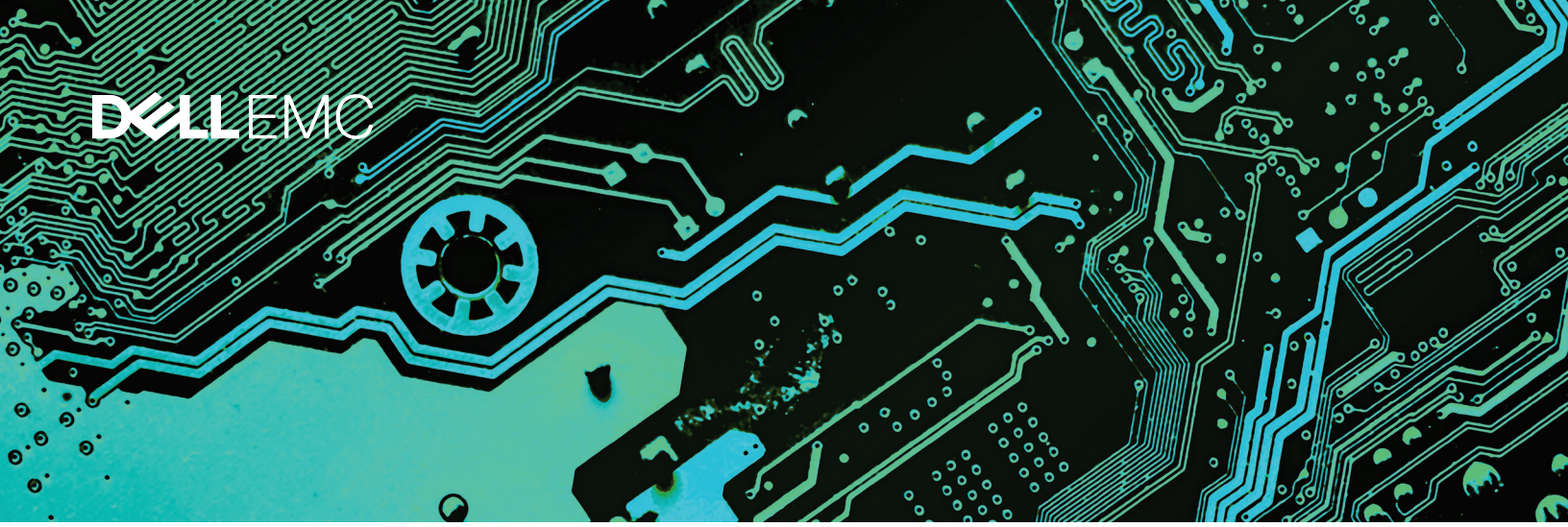


Dell EMC Ready Architectures for Splunk

Harness machine data with simplified deployment of optimized solutions that scale with ease

Table of Contents

Data, data everywhere... . . . 2
Leverage solutions built for Splunk . . . 2

Do any of these challenges sound familiar? . . . 3
Top Splunk use cases . . . 3
Turning machine data into answers in real-time . . . 4

Ready Architectures for Splunk . . . 5
Splunk on VxRail specifications . . . 5
Splunk on VxRack FLEX specifications . . . 6
Splunk on PowerEdge specifications . . . 7

Why Dell EMC? . . . 8

Services and financing . . . 9
Dell Financial Services . . . 9
Dell Customer Solution Centers . . . 9

Take the next step toward harnessing data . . . 9

Harness machine data

100s

of apps and add-ons enhance productivity[1]

Simplify deployment

82%

decrease in time to deploy VxRack FLEX[2]

Scale with ease

5

minutes to add a new node with VxRail[3]

Data, data everywhere...

Machine data is one of the fastest-growing and complex areas of big data. It also contains a definitive record of events that can reveal information about transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Making use of this data, however, presents real challenges. Traditional data analytics solutions are not engineered to handle this high-volume, high-velocity and highly diverse data.

Splunk® Enterprise is an industry-leading software for machine data analytics. It's the easy, fast and secure way to search, analyze and visualize the massive streams of machine data generated by IT infrastructure, business applications, computers, mobile phones, embedded systems and other networked devices — physical, virtual and in the cloud — helping you deliver real-time visibility across the entire business. But many organizations find it complex and time-consuming to architect, test and tune hardware for Splunk.

Leverage solutions built for Splunk

Dell EMC and Splunk have partnered to make adopting Splunk simpler by engineering a portfolio of purpose-built solutions with non-disruptive scalability and performance optimized for Splunk workloads. Together, Dell EMC and Splunk enable you to harness the power of machine data analytics with simplified deployment and scalability.

Harness machine data

Splunk makes it simple to collect, analyze and act upon the untapped value of the data generated by infrastructure, security solutions and business applications — for the insights to drive operational performance and business results. Dell EMC Ready Architectures for Splunk are purpose-built for the needs of Splunk, helping consolidate, simplify and protect machine data.

Simplify deployment

Maintaining consistent performance — so you get fast query and search capabilities from Splunk — requires a thoughtful approach to infrastructure design. Dell EMC Ready Architectures for Splunk have been tested and tuned with Splunk software to optimize your Splunk deployment.

Scale with ease

Splunk scales easily from a single focused use case to an enterprise-wide analytics backbone. Dell EMC Ready Architectures for Splunk are designed from the start to dynamically fit your current and future needs. When it's time to grow, you can scale without interrupting Splunk operations.

[1] Splunk.com, "Enhance and Extend the Value of Splunk," December 2018.

[2] Wikibon.com, "Hyperconverged Infrastructure as a Stepping Stone to True Hybrid Cloud," March 2018

[3] Enterprise Strategy Group, "VxRail Hyper-converged Appliances from Dell EMC," January 2017.

Do any of these challenges sound familiar?

We could benefit from machine data — but don't know how to get a handle on it

Machine data is the largest and fastest-growing section of data. Every second of every day, hundreds to thousands of devices record what's happening in your business, with records coming in an array of unpredictable formats. Dell EMC Ready Architectures for Splunk combine the power of Splunk to make machine data accessible, usable, and valuable to everyone, with simplicity and scalability.

Deploying infrastructure for Splunk is complex and time-consuming

One of the main benefits of Splunk is advanced functionality for a variety of well-defined use cases right out of the box. But who wants have to spend weeks and months architecting, deploying and tuning the underlying infrastructure? Tested and tuned Dell EMC Ready Architectures for Splunk reduce the time, effort and resources required to architect and build a Splunk solution. In fact, Dell EMC is one of the only partners to offer Splunk-validated solutions.

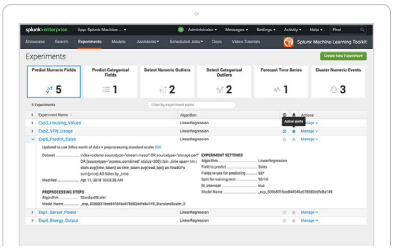
It's hard to anticipate what our future needs will be for Splunk

Many organizations find that once they use Splunk for one use case, they want to add more. In addition, data sets keep growing exponentially, with no end in sight. Dell EMC Ready Architectures for Splunk address your current and future needs by offering flexible solutions that allow you to scale compute and storage independently, or as a single, hyper-converged system.

Top Splunk use cases

Application delivery	Splunk software provides an approach to managing applications, helping developers deliver applications faster with a positive user experience. It spans silos to collect, index and analyze the machine data that provides insight into the availability, performance and usage of applications. As a result, DevOps organizations can deliver faster releases, operations teams can reduce mean time to resolution (MTTR) and development teams can optimize application quality, performance and costs.
Business analytics	Splunk software analyzes, visualizes and monitors machine data from any source — such as applications, mobile devices and servers — to provide insights to IT and business operations on-premises and in the cloud. Delivering these enhanced business insights in real time to executives, and to sales, product, marketing, operations and customer service teams can help transform an organization into a market leader.
Cloud	Splunk enables centralized visibility across cloud, on-premises and hybrid environments, so customers can leverage cloud with the security, visibility and assurance they require. Whether a customer is managing applications, infrastructure or security operations in the cloud, Splunk delivers operational intelligence for a real-time understanding of what's happening across the business and IT, so customers can make better-informed decisions.
IoT	Splunk software ingests, analyzes and visualizes real-time and historical machine data from any source — including industrial control systems and connected devices — enabling customers to improve operations, enhance safety and compliance, perform predictive maintenance, and better manage the uptime and availability of industrial assets.

IT operations	Splunk collects and correlates machine data so customers can quickly troubleshoot issues and outages, monitor service levels and detect anomalies. Splunk can help reduce MTTR, lower monitoring costs, improve uptime and support strategic initiatives like data center optimization and tool consolidation.
Log management	Splunk can consolidate and index log and machine data, including structured, unstructured and complex multi-line application logs. Customers can collect, store, index, search, correlate, visualize, analyze and report on any machine-generated data to identify and resolve operational and security issues in a faster, repeatable and more affordable way.
Security and fraud	Splunk enables collaboration and implementation of best practices to address modern cyber threat challenges. With Splunk as a nerve center, security teams can leverage statistical, visual, behavioral and exploratory analytics to drive insights, decisions and actions.



Turning machine data into answers in real-time

With Splunk Enterprise, you can analyze and ask questions of data from any source to get the insights you need. Splunk offers AI solutions that provide applied machine learning to get value from all of this data, through packaged or custom machine learning options, as well as platform capabilities to help organizations achieve fast time to value with their machine learning initiatives.

Data wrangling is one of the most difficult, time-intensive steps in getting value from machine learning. This is one of Splunk's strengths—handling data prep and addressing problems with the data set so that organizations can focus their time on using machine learning to make decisions and avoid bigger problems later on. Splunk's software platform approach provides the ability to prep the data without the need to move it for analysis.

Splunk IT Service Intelligence and Splunk User Behavior Analytics are pre-built, use case-specific solutions that leverage packaged machine learning via advanced adaptive thresholding and anomaly detection techniques, helping organizations proactively detect incidents, reduce resolution times, and predict and prevent undesired outcomes, without the need for a data scientist.

The Splunk Machine Learning Toolkit (MLTK), a free app available on Splunkbase, enables custom machine learning for any use case on the Splunk platform. It provides a guided workbench for creating, testing, and deploying models, and includes commonly used machine learning algorithms that can be applied to the data. In addition, the MLTK provides an extensible API for developers to import any machine learning algorithms (proprietary or open source) and operationalize them as a Splunk dashboard, alert, or report.

Splunk allows organizations a range of options for getting value from their data, with solutions that are packaged for less advanced users, as well as those that are more customizable for advanced users. The result is a single software platform that is both easy to use yet flexible enough to be customizable.[3]

[3] ESG Research Insights Paper: "Leveraging AI and ML for Greater Impact," December 2017.

Ready Architectures for Splunk

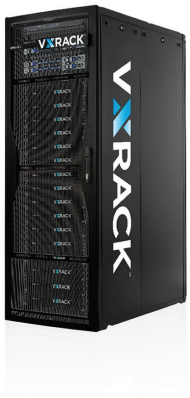
Ready Architectures for Splunk are available with: Splunk, VMware, Red Hat and Dell EMC software. Hardware options include: VxRail, VxRack FLEX, PowerEdge servers, Dell EMC Networking and Isilon scale-out NAS. Available services include: consulting, education, deployment, support services; and financing.

Splunk on VxRail specifications

Sizing	50GB/day single/ combined	500GB/day distributed 250GB/day clustered	1TB/day distributed	1TB/day distributed or clustered
Retention	90-day			7-day for hot/warm buckets and configurable retention for cold storage
Number of VxRail E560	3	4	7	7
Memory	64GB – 3072GB			
Storage	1.2TB-30.7TB per node[4]			
Network	4x 10GbE SFP+ per node			
Software	Splunk Enterprise Splunk Universal Forwarder Red Hat® Enterprise Linux® 64-bit VMware vSphere Enterprise VMware vCenter Server® VMware vSAN Enterprise VMware vRealize® Log Insight™ VxRail Manager			
Isilon Scale-Out NAS X410 configuration				
CPUs				2x Intel® Xeon® E5-2698 v4
RAM				128GB
SSD capacity				3.2TB
HDD capacity				64TB
Network				2x 10GbE 2x 1GbE

Refer to "Using Splunk Enterprise with VxRail Appliances and Isilon for Analysis of Machine Data" for more detail.

[4] The net effective usable capacity of the VxRail cluster is half the raw capacity. This is due to the Virtual SAN FTT=1 policy setting applied to each VM.



Splunk on VxRack FLEX specifications

Sizing	250GB/day clustered	500GB/day clustered	1TB/day distributed	1TB/day clustered
Retention	90-day			30-day for hot/warm data and configurable retention for cold storage
Number of VxRack nodes	1x search head 2x indexers 1x admin	1x search head 5x indexers 1x admin		1x search head 5x indexers with Isilon for configurable retention of Splunk cold storage 1x admin
Compute	PowerEdge R640 Servers			
Processor	2x Intel Xeon SP-6132 V1 per node			
Memory	512GB (16x 32GB)			
Storage	10x 3.84TB SSD			
Hot/warm storage	7.2TB			
Cold storage	15TB			Configurable
Networking	25GbE Cisco Nexus®			
Software	Splunk Enterprise Splunk Universal Forwarder Red Hat Enterprise Linux 64-bit VMware vSphere Enterprise VMware vCenter Server Dell EMC Vision Intelligent operations Dell EMC VxFlex OS			
Isilon Scale-Out NAS X410 configuration				
CPUs				2x Intel Xeon E5-2698 v4
RAM				128GB
SSD capacity				3.2TB
HDD capacity				64TB
Network				2x 10GbE 2x 1GbE

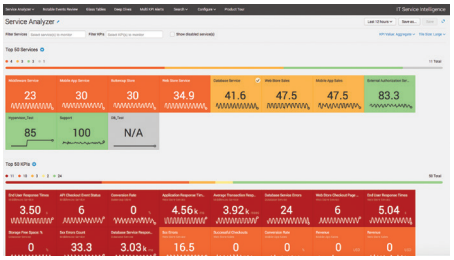
Refer to "Splunk Enterprise on VxRack FLEX for Machine Data Analytics" for more detail.

Splunk on PowerEdge specifications

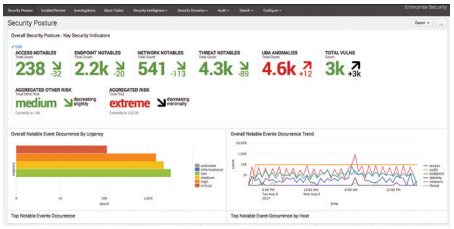
Sizing	250GB/day single instance	250GB/day distributed	250GB/day clustered	250GB/day clustered high-performance	250GB/day clustered	Test/dev single instance
Retention	115-day				210-day with Isilon cloud bucket expansion	N/A
Compute	1x PowerEdge R740xd combined search and index head	1x PowerEdge R740xd indexer 1x PowerEdge R640 search head 1x PowerEdge R640 admin	2x PowerEdge R740xd indexers 1x PowerEdge R640 search head 1x PowerEdge R640 admin	2x PowerEdge 740xd or R940 indexers 1x PowerEdge R640 search head 1x PowerEdge R640 admin	2x PowerEdge R740xd indexers with Isilon for configurable retention of Splunk cold storage 1x PowerEdge R640 search head 1x PowerEdge R640 admin	1x PowerEdge R440 combined search and index head
Processor	2x Intel Xeon Gold 5120	R740xd: 2x Intel Xeon Gold 5120 R640: 2x Intel Xeon Gold 5118		R940: 2x Intel Xeon Platinum 8180 R640: 2x Intel Xeon Gold 5118	R740xd: 2x Intel Xeon Gold 5120 R640: 2x Intel Xeon Gold 5118	R440: 2x Intel Xeon Silver 4114
Memory	128GB per node					
OS storage (RAID1)	300GB per node					
Hot/warm storage	4,800GB					960GB
Cold storage	14TB				63TB with Isilon	3.6TB
Networking	2x 10GbE or 2x 25GbE (check suppliers for interoperability support)					
Software	Splunk Enterprise Splunk Universal Forwarder Red Hat Enterprise Linux 64-bit OpenManage OneFS					
Isilon Scale-Out NAS H600 configuration						
CPUs					1x Intel Xeon E5-2680 2.4GHz	
RAM					256GB per node	
SSD capacity					4x 800GB	
HDD capacity					8x 400TB	
Network					2x 40GbE 2x 10GbE per node	

Refer to "Splunk Enterprise on Dell EMC PowerEdge Servers with Isilon for Machine Data Analytics" for more detail.

splunk>enterprise



Splunk IT Service Intelligence



Splunk Enterprise Security

Splunk Enterprise software enables collection, indexing and visualization of machine-generated data gathered from different sources in the IT infrastructure. These sources can include applications, networking devices, host and server logs, mobile devices and more. Splunk turns silos of data into operational insights and provides visibility across the IT infrastructure to enable faster problem solving and informed, data-driven decisions. Splunk also:

- Blends metrics and events from both structured and unstructured data sources
- Delivers powerful visualizations to reveal relationships, track trends and accelerate investigations
- Collects and correlates multiple data sources to rapidly pinpoint service degradations and reduce mean time to repair (MTTR)
- Monitors infrastructure to detect anomalies and prevent problems in real time

Dell EMC PowerEdge Servers create the foundation for an adaptive IT solution, delivering superior agility and reliability, outstanding operational efficiencies, and top performance at any scale. Versatile, powerful in-server storage accelerates performance of targeted applications with flexible configurations designed to enhance data center efficiency.

Dell EMC VxRail is a preconfigured and pretested VMware hyper-converged infrastructure appliance. Powered by industry-leading VMware vSAN and vSphere software, the VxRail appliance streamlines and extends the VMware environment while dramatically simplifying IT operations with a known and proven building block for the software-defined data center (SDDC).

Dell EMC VxRack FLEX delivers virtualization, compute, networking and storage in a scalable, easy-to-manage hyper-converged solution. It integrates VMware vSphere virtualization software, delivering industry-leading application virtualization with a highly available, resilient, efficient on-demand infrastructure. VxRack FLEX supports multiple hypervisors, operating systems and bare-metal configurations enabling independent scaling of compute and storage, eliminating stranded resources and improving utilization.

Dell EMC Isilon X-Series is a flexible storage product that provides large capacity and high performance. Isilon storage uses intelligent software to scale data across a large number of commodity hardware units, enabling explosive growth in performance and capacity.

Why Dell EMC?

Dell EMC holds leadership positions in some of the largest-growth categories in the IT infrastructure business, and that means Dell EMC will be there for you now and in the future.

- #1 in servers[6]
- #1 in converged and hyper-converged infrastructure (HCI)[7]
- #1 in traditional and all-flash storage[8]
- #1 cloud IT infrastructure[9]
- #1 in data protection[10]
- #1 in software-defined storage[11]

See Dell Technologies Key Facts.

[5] Dell Technologies, "Dell Technologies Code of Conduct," 2018.

[6] IDC WW Quarterly Server Tracker, May 2018, Vendor Revenue — Q1 2018.

[7] IDC WW Quarterly Converged Systems Tracker, June 2018, Vendor Revenue—Q1 2018.

[8] IDC WW Quarterly Enterprise Storage Systems Tracker, June 2018, Vendor Revenue—Q1 2018.

[9] IDC WW Quarterly Cloud IT Infrastructure Tracker, June 2018, Vendor Revenue—Q1 2018.

[10] Gartner, "Magic Quadrant for Data Center Backup and Recovery Solutions," July 2017.

[11] IDC WW Semiannual Software Tracker, April 2018.

Services and financing

Solutions customized for your needs

- Dell EMC Consulting Services are delivered by experts to help you get the business value of data analytics. The services include a data analytics assessment, workshop, testing, proofs of concept and production implementation. These experts help determine where data analytics applications are a good fit for your organization. They also help you build your own internal team of experts through knowledge transfer at each step.
- Dell EMC Education Services offers courses and certifications in Data Science and Advanced Analytics. Through self-paced online labs and instructor-led workshops, the Deep Learning Institute provides training on the latest techniques for designing, training and deploying neural networks across a variety of application domains.
- Dell EMC offers a broad menu of deployment services for data analytics solutions. Services include on-site hardware and operating system software installation, optional rack integration at a Dell EMC facility and testing/validation of the installed solution. Software deployment is a custom project with delivery based on your needs. Dell EMC takes care of project management, from order to your acceptance of the implementation.
- Dell EMC support services offer a single point of accountability from experts with solution-specific training, along with premium hardware and software support available 24x7x365. Choose next-business-day, on-site service with four- and eight-hour parts and labor response options, and escalation with customer-set severity level options.

Dell Financial Services

The wealth of leasing and financing options from Dell Financial Services can help you find opportunities when you're facing decisions regarding capital expenditures, operating expenditures and cash flow. Dell offers a wide range of payment options to make it easier than ever to meet your needs.

- Leasing and financing solutions are available throughout the U.S., Canada and Europe.
- Dell Financial Services can help finance your technology purchase.
- Electronic quoting and online contracts offer an efficient purchase experience.

Dell Customer Solution Centers

Our global network of 21 dedicated Customer Solution Centers are trusted environments where world-class IT experts collaborate with customers and prospects to share best practices; facilitate in-depth discussions of effective business strategies using briefings, workshops, or proofs-of-concept (PoCs); and help businesses become more successful and competitive. Dell Customer Solution Centers reduce the risks associated with new technology investments and can help improve speed of implementation.

Take the next step toward harnessing data

Machine data is everywhere, and it holds the key to better understanding user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Contact your Dell EMC or an authorized partner for more details on how to leverage your machine data, today.

Contact us

To learn more, visit dellemc.com/splunk or contact your local representative or authorized reseller.