Skills to Secure the Data Center

Organizations now rely on data centers to do business. Therefore, executives and customers expect them—and especially the data within them—to be safe and available.

Digital transformation is creating great new possibilities for many types of businesses. Eventually, it will affect nearly every facet of business operation, but the data center is the hub of the action.

It can enable companies to reach new customers, speed innovation, and streamline operations. Today's data center puts a multicloud strategy first, is application-aware, is hardware-innovative, and captures the intent of its users.

This approach can deliver impressive business benefits. But as digital applications and devices multiply, so do the complexities. This means that businesses and their data centers must become more agile, intuitive, and secure.

That last word is key. Security is a rapidly growing business concern, keeping management awake at night.

Here's why. Organizations now rely on data centers to do business. Therefore, executives and customers expect them—and especially the data within them—to be safe and available. This means that security is critical to keep business moving and growing.

That calls for the intent-based data center, which we will explain in more detail below. This new type of data center is constantly learning, adapting, and protecting. Because of its higher level of capabilities, the intent-based data center has created a demand for people who can understand, develop, and help secure it.

This white paper will aim to accomplish the following:

- Discuss the factors driving the need for the intent-based data center
- Address security as it relates to the data center
- Reveal how organizations are responding
- Explain the importance of certifications in creating and securing data centers to enable business transformation

Data centers today are required to do much more

Right now, billions of devices are connecting to the Internet. In fact, connected devices now outnumber people. This includes a mind-boggling variety of devices, along with their various applications.

This is making data centers much more complex to manage, so businesses must make them more efficient.

Companies are adding data center computing, networking, and storage resources to carry that rapidly growing load. But it's not just about adding more of the same resources.

The new intent-based data center is the next leap forward. This data center must learn from every packet and every transaction.

Data centers must become smarter and much more responsive so they can provide the required resources for applications and devices when they need them.

This includes providing continuous and faultless security as an integral part of data center operation because it is becoming even more imperative to shield information and infrastructure from unauthorized access and use. This is the only way that resources will be safe and available to support business goals and processes.

These measures are increasingly important because data centers have become mission-critical for businesses in the following ways:

- Supporting internal applications
- Enabling customer-facing applications and services
- Delivering true business intelligence

What is the intent-based data center?

The new intent-based data center is the next leap forward. This data center must learn from every packet and every transaction. It must be able to adapt, benchmark, compare, and measure. And it must protect vulnerable applications, data, devices, infrastructure, and users from expensive malfunctions and security disasters. In other words, it must be impressively smart.

Cisco's intent-based data center uses network intelligence to automate functions, analyze data, and deliver optimal performance. It supports an organization's move to become a true digital business.

In today's digitized organization, business needs have evolved. Businesses and data centers must be smarter in how they work. To enable that, the intent-based data center can aggregate, automate, and draw insights from available data.

Cisco's new data center solution captures the intent of users and applications. It interprets the context of every application transaction, user experience, and infrastructure use. It constantly learns, adapts, and protects, growing smarter every day.

The intent-based data center allows an organization to make the most of its data—even to manage, leverage, and monetize it as a real asset. That aligns with the big data trend now occurring, in which predictive analytics, machine learning, and cognitive computing are becoming more valuable.

Most new data center investments are earmarked for analytical and client-facing applications, as opposed to back-office systems such as enterprise resource planning. Through 2018, 65 percent of the new data center investments will be for data analytics, IoT, and systems of engagement.[1]

1. IDC, "IDC FutureScape: Worldwide Datacenter 2016 Predictions," November 2015.

The goal is to help businesses become more agile, efficient, scalable, and simple to manage.

Forrester expects the big-data market to grow three times faster than the overall tech market.[2] In fact, big data should represent 27 percent of data stored in data centers by 2020.

Data and analysis are important from an internal perspective. Businesses want to analyze application behaviors and to build policy models for application segmentation and automated enforcement. They also must view, control, and secure networks end to end.

That requires pervasive visibility into every flow, which is important whether data runs on containers, uses micro-services, or operates in physical or virtual environments.

Pervasive visibility allows data centers to detect policy deviations in real time to ensure compliance. It can support multicloud strategies, it allows data centers to move to a zero-trust security model, and it helps optimize disaster recovery models.

Simplicity is among the benefits of the intent-based data center, which fits perfectly with other marketplace trends.

For example, a great deal of data center consolidation is taking place lately, with some major businesses moving from multiple smaller data centers to fewer, larger ones.

These hyperscale data centers have 10-GB to 100-GB bandwidth capacity to support cloud operations while supporting a wide range of other digital technologies.

Studies indicate there were 259 hyperscale data centers at the end of 2015. Forecasts suggest there could be 485 of them by 2020.[3] At that point, hyperscale data centers will represent 47 percent of all installed data center services, and traffic within them will have quintupled.

But hyperscale is not just about being big. It's about simplification and economies of scale. The goal is to help businesses become more agile, efficient, scalable, and simple to manage. With all that, the data center's total cost of ownership also must be reasonable.

One way the intent-based data center keeps costs under control and enables simplicity is through automation. Applications analysis and policy creation across the hybrid cloud takes place on the front end, making manual intervention no longer necessary for every operation.

Data center automation delivers many benefits, including greater agility and reduced human resource costs. It also allows IT teams to focus on innovation rather than on maintenance. IDC predicts that 60 percent of companies will embrace automation in the data center by 2018.[4]

2. Forrester, "Forrester Forecasts Big Data Tech Market Will Grow ~3X Faster Than Overall Tech Market," September 2016.
3. Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2015-2020," 2016.
4. IDC, "IDC FutureScape: Worldwide Datacenter 2016 Predictions," November 2015.

Cisco helps its customers build data centers that maximize application performance, mitigate risk, and increase operational agility.

The intent-based data center also addresses several important aspects of security, including compliance, along with data center and network security. It also includes physical security, plus data security in motion and at rest. And it provides security consistently across any combination of clouds that an organization implements by leveraging constant visibility, automation, real-time contextual awareness, and microsegmentation to place the correct security exactly where it's needed.

Of course, every organization's data center is different, so there will be variations in what will be required. But as we can see, digital transformation does call for the more advanced intent-based data center.

Cisco helps its customers build data centers that maximize application performance, mitigate risk, and increase operational agility. This requires complete visibility across data centers and networks all the way through to endpoints across the cloud infrastructure. Equally important, it involves securing the data and infrastructure all along the way.

A safe and secure environment has become essential

A quick scan of the daily news illustrates the critical importance of security. New threats such as ransomware and user-initiated breaches such as phishing are growing exponentially. No organization is immune because cybercrime is now a multibillion-dollar business with a low cost of entry. In fact, software to carry out attacks is even sold online.

The Internet of Things (IoT) is helping fuel the growth of distributed denial of service (DDoS) attacks because nearly any connected device can be commandeered to stage attacks. Then those devices can feed information back to data centers, generating a serious data center security issue.

Gartner calls IoT an increasingly attractive early link in attack chains, and it expects about 25 percent of enterprise attacks to involve IoT by 2020.[5] Despite this, the firm expects that IoT will account for less than 10 percent of IT security budgets.

As another form of attack, ransomware has also seen considerable growth.

A daily average of more than 4000 attacks occurred in the first quarter of 2016. Deloitte says that's a 300 percent increase from the 1000 daily ransomware attacks in the prior year.[6]

Organizations are reacting accordingly. Research indicates that many of them are increasing their cybersecurity budgets. They're spending on security solutions, implementing outsourced security services, and investing in cybersecurity-related training.

5. Gartner, "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016," April 2016.
6. Deloitte, "Ransomware Holding Your Data Hostage," August 2016.

Businesses and governments must become much more sophisticated about guarding against cyberattacks, and they must be ready to respond immediately when attacks and breaches do occur.

Worldwide revenues for security-related hardware, software, and services are poised to reach $81.7 billion for 2017. That's up 8.2 percent from 2016, according to the Worldwide Semiannual Security Spending Guide from IDC.[7]

Digital transformation is growing rapidly, says Eileen Smith, IDC's program director for customer insights and analysis. That's putting pressure on companies across all industries to invest in security, she adds.

In fact, 46 percent of companies will increase security budgets by an average of 21 percent this year, according to the 2017 Cybersecurity Trends Report from Crowd Research Partners.[8]

Here are some other statistics from the same study:

- Thirty-three percent of that spending is related to the cloud.
- Twenty-three percent is being dedicated to secure mobile devices.
- Another twenty-three percent is being set aside for cybersecurity training and education.

Because no business is immune from this spreading epidemic, it's becoming a high-stakes game for nearly every industry.

That means businesses and governments must become much more sophisticated about guarding against cyberattacks, and they must be ready to respond immediately when attacks and breaches do occur.

But there is a bright side within that doom and gloom. Although attacks and cybersecurity challenges are increasing, most organizations recognize the problem and are working to address it.

One method is by boosting their workforce of skilled data center professionals.

Data center cybersecurity experts are a new reality

As we have noted, the modern data center houses the information, applications, and services that are foundational for business success.

It is critical that the IT staff managing the data center are aware of cybersecurity practices and can interface with the organization's cybersecurity team to ensure that information is protected and risks are reduced.

Some of these risks are as follows:

- Insufficient threat visibility in the network, workloads, or applications
- Inconsistent policies across workloads
- A confusing number of point security vendors

7. IDC, "Worldwide Spending on Security Technology Forecast to Reach $81.7 Billion in 2017, According to New IDC Spending Guide," March 2017.
8. Crowd Research Partners, "2017 Cybersecurity Trends Report," 2017.

To combat these risks, conventional wisdom is starting to conclude that there should be security specialists in the data center. This is creating opportunities for people like you who want to advance their careers by becoming more valuable assets.

- Increasing sophistication of cybercriminals
- Breadth of the attack surface

To combat these risks, conventional wisdom is starting to conclude that there should be security specialists in the data center. This is creating opportunities for people like you who want to advance their careers by becoming more valuable assets. Leaders in this area are truly needed.

As a security specialist you will help inform the organization's essential technology buying choices and security architecture. You'll gain expertise in compliance requirements. You'll help your company stay on top of regulatory changes.

You'll also be in charge of deciding if and when you need to make other changes.

For example, over time, companies change data retention or data warehousing policies, including what should be encrypted. The old mindset was to lock down everything in the name of cybersecurity. However, that can limit a company's flexibility.

Security specialists working in an intent-based data center can use more advanced security processes to allow greater freedom. Automated intelligence can handle tasks that previously required manual input. That will free up security staff to focus on more sophisticated projects to help organizations move faster toward new opportunities.

Of course, not every business or data center will have a security specialist in-house. But every member of the data center staff should have at least a basic understanding of the compliance requirements for that particular industry.

That can ensure a more secure data center and help an organization avoid unplanned audits. It can also remind team members that security is everybody's responsibility.

In recent years, more organizations have been putting greater emphasis on accountability. Data centers must document those efforts so it's clear which person made particular decisions, along with who approved and signed them.

This means an organization will be ready if and when audits are needed, and they will have accurate and reliable documents.

Data center security could be an exciting journey for you

By now, it should be apparent that securing the intent-based data center is not a one-and-done endeavor. It's truly a multifaceted journey.

That journey is part of digital transformation. And it will require you to be prepared.

People, processes, and technologies must evolve to meet growing and changing cybersecurity challenges. That's no small feat considering the existing shortage of experts in this field.

People, processes, and technologies must evolve to meet growing and changing cybersecurity challenges. That's no small feat considering the existing shortage of experts in this field.

But it's worth the effort, because you will be in great demand. The Bureau of Labor Statistics projects the rate of growth for jobs in information security at 28 percent from 2016 to 2026.[9] And more than one-third of employers ask cybersecurity job candidates for industry certifications.

Cybersecurity is an important new discipline amid a growing threat. Yet forecasts suggest there will be 3.5 million cybersecurity job openings by 2021.[10] So we need to create the workforce for this new world.

Cisco certifications can help you and your organization do that. They position people like you with more clout in the talent marketplace. And they help your employer ensure its data centers and all that they do are safe and secure.

Cisco can prepare you to execute important initiatives related to the following:

- Streamlining operations through automation
- Establishing policy-driven infrastructure across the physical and virtual resources related to data centers
- Implementing unified communications and advanced virtualization
- Ensuring data center infrastructure security

That will allow your organization to benefit in several important ways:

- Faster deployments
- More efficient data center operations
- Higher returns on investment
- A higher level of security and peace of mind

Cisco continues to develop its industry-respected certification portfolio. That way, its certifications support the latest skills and technologies necessary for world-class digital business transformation.

Cisco Security certifications go in-depth

Cisco certified cybersecurity professionals have in-depth expertise and proven knowledge in cyberthreat detection and mitigation.

CCNA Security is an excellent starting point for cybersecurity training. It teaches all the necessary basics to begin building and administering a secure network infrastructure as an Associate-level player on the network security team.

9. Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, Information Security Analysts, on the Internet (visited October 25, 2017).
10. Herjavec Group, "2017 Cybersecurity Jobs Report," 2017.

Cisco's Data Center certifications validate specific skills that let the IT team apply that knowledge to the intent-based data center.

This is an attractive option for any IT personnel who are currently building a network infrastructure, and who wish to move into a security function, learning how to secure the networks they are building and the data centers they are connecting.

CCNP Security certification builds upon the skills of CCNA Security. It specifically corresponds to the job role of Cisco network security engineer—someone who is responsible for securing networks, devices, appliances, and applications. CCNP Security certified professionals are frequently also in charge of choosing, deploying, supporting, and troubleshooting security products and services.

Cisco's CCIE Security certification prepares IT personnel for the evolving technologies at the Expert level. CCIE Security covers skills for managing advanced cybersecurity technologies and solving cybersecurity problems. They "build the castle," solving cybersecurity problems and designing, deploying, and adapting cybersecurity technology to the widest range of cybersecurity problems facing a digital organization.

The CCIE certification also includes a new assessment approach on the latest security technologies. These include advanced threat protection, advanced malware protection, next-generation intrusion prevention systems (IPSs), virtualization, automation, and information exchange. The goal is to ensure that candidates demonstrate firm knowledge of and skills for handling evolving technologies such as network programmability, cloud, and IoT.

Security is also an important part of Cisco's Cloud and IoT curricula.

Data Center certifications carry it farther

Cisco's Data Center certifications validate specific skills that let the IT team apply that knowledge to the intent-based data center.

CCNA Data Center includes the latest content and extensive hands-on learning related to the basics of cloud computing, and automation and orchestration of the data center infrastructure. It also includes Cisco UCS Director basic functions and Cisco Application Centric Infrastructure (ACI).

CCNP Data Center certifies experienced, Professional-level skills in data center technologies. That includes Cisco ACI, automation, cloud orchestration, configuration, high-availability architecture, networking, programmability, servers, and storage. It also includes traffic design, troubleshooting, unified fabric, and virtualization. The accompanying curriculum expands the emphasis on data center virtualization, automation, and ACI management and monitoring. Content on data center security and data center storage connectivity is also included in this program.

CCIE Data Center certifies Expert-level skills focused on in-depth data center solutions and emerging technologies. These are skills needed to design, implement, and manage a complex and modern data center infrastructure.

Organizations and their new data centers and networks have a promising opportunity to use the vast resources offered by intent-based technology to improve and grow.

The CCIE program includes policy-driven infrastructure, automation, and orchestration, storage networking and computing, and evolving technologies. The latter includes IoT, SDN, and the cloud. It provides learners with insight about their impact on architectural framework, deployment models, implementation, and operations.

Together, these certifications and tools help professionals manage and control enterprise-wide deployments consistently and securely.

Cisco is here to help

All this training is extremely important, as we are entering an entirely new era in data center operations and management. This is a time of connected devices—billions of them. It's a time of big innovation, and potentially big gains. That's why it calls for more secure solutions and entirely new skills.

Now organizations and their new data centers and networks have a promising opportunity to use the vast resources offered by intent-based technology to improve and grow.

As always, Cisco will be here as a trusted partner for this exciting new journey.

We invite you to join us. Visit our Data Center site to learn more.

DEC17CS5492-5 01/18