SOLVING THE SECURITY CHALLENGES OF THE SOFTWARE-DEFINED DATA CENTER (SDDC)
Enterprise IT has evolved

Today, enterprise IT is facing pressure to provide new value and differentiation in an increasingly competitive marketplace. In the 1990s, companies concentrated on building and deploying customized systems, where seemingly every application was deployed on an exclusive piece of hardware. This approach resulted in data centers containing a huge variety of custom machines.

As software providers began to decouple hardware from applications, IT departments were able to purchase hardware from a preferred vendor. The mismatched data center of custom mainframes became neat and homogenous. IT processes were streamlined to support a common hardware profile, and IT engineers were relieved. But this new strategy included infrastructure security controls -- to secure the application, IT teams had to secure the hardware that supported it. This meant entire security frameworks were built to secure the underlying hardware.

Security teams were built up within IT, specializing in fighting new and evolving attacks. They focused on securing the hardware and the network first, and then the applications -- and worked with the rest of IT to resolve issues that occurred. Friction occurred between the teams -- when one team is responsible for finding problems and another team is responsible for fixing them, it creates conflict. To solve this, IT departments created the Security Operations (SecOps) function.

SecOps allows IT teams to take a more holistic look at security, and enables both teams to come up with solutions for the common goal of securing the data center. SecOps reduces friction and enables all IT teams to more efficiently prioritize and remediate security findings. Even in an organization with a mature SecOps program, problems and solutions still concern the infrastructure, however, virtualization has revolutionized the data center, and organizations can no longer afford to simply secure the infrastructure alone.

While worldwide spending on IT security continues to climb, the odds of an organization falling victim to a data breach have risen to 1 in 4.1

---

1 Ponemon Institute, June 2017, “2017 Cost of a Data Breach Study: Global Overview”
The virtualized data center revolution

Traditional enterprise data centers were inflexible, inefficient, and unable to meet rapidly changing business needs due to proprietary hardware, application silos, and high equipment costs. In addition, applications would often consume only a fraction of the available computing power, and IT department requirements greatly influenced business decisions.

Server virtualization revolutionized the data center by consolidating applications onto fewer physical server hosts, allowing IT departments to take full advantage of the underlying hardware. Instead of application silos and buckets of computational resources, IT departments are able to create and leverage a shared pool of resources. Today, the virtualization revolution has grown to encompass storage and the network as well, affording these pillars of the data center the same advantages of agility and efficiency as servers have enjoyed for many years.

This revolution was not easy. The ability to abstract applications from the underlying physical hardware created tension between the security and infrastructure teams. Security controls were slower to change than the data center itself, and security teams were left scrambling. Every piece of hardware could host critical business data, and so the shared resource pool had created a shared security risk. This created a significant set of challenges for IT departments and security teams.

Security challenges in the SDDC

1. Traditional security controls are aligned to infrastructure, not applications

SecOps challenge: applications in the SDDC are hardware-agnostic

There are two main challenges with securing applications in the SDDC from an “infrastructure” perspective: 1.) Applications are widely distributed across many servers, located in multiple data centers or even up in the cloud. 2.) Applications are changing constantly to keep up with the needs of business. Virtualization has made it possible for both of these things to happen.

Legacy security controls were designed for static infrastructure, not for modern applications/development methodologies. Security teams struggle to design and enforce adequate security policies for apps that are widely distributed because they don’t have insight into what the application looks like.

Even if they do manage to design security policies for the app, it changes tomorrow without their knowledge, weakening policies.

IT challenge: maintaining security governance

When data centers were structured based on physical hardware, IT had complete control of new hardware requisition and deployment. Each machine had an application manifest that IT needed to load before enabling the device. Because critical applications were contained on physical machines, SecOps had a clear list of security
products included for application manifest. Maintaining security governance for the data center was a predictable and uncomplicated process.

With the introduction of hardware-agnostic applications, maintaining security governance becomes challenging. Given applications can have varying security requirements, understanding which security products are required can be difficult, resulting in churn and inefficient work as IT scrambles to comply with SecOps application security policies.

2. Attacks in the SDDC are different

SecOps challenge: coverage against new attack methodologies

Traditional security solutions exist on the attack surface. Even the best security prevention agents, those that exist at the kernel level of the operating system, are still susceptible to attack. Given enough time and effort, attackers can learn ways to destabilize agents or the underlying operating system. At that point, security agents are unable to stop attacks, or in some cases, even alert an ongoing attack. The only way to prevent issues with certainty is to have a component separate from the attack surface.

The SDDC is not typically the entry point for attacks, and therefore the attack methodologies used are different than those typically seen on end user endpoints. By the time attackers penetrate the data center, they have already secured a beachhead in the environment. Traditional AV solutions that only focus on malware are not equipped to stop fileless lateral movement in the environment, and lack the visibility that security teams need to investigate root cause.

In addition, the SDDC is significantly more complicated than an end user system. Companies cannot stop what they cannot see. Visibility is critical in securing applications and protecting critical data. In the SDDC, the primary concern is how applications are behaving; how are applications communicating and transmitting information within the SDDC. Application behavior is complex – distributed applications mean many VMs running in harmony, which require multiple communication channels to be available whenever necessary. As applications change and expand over time, new VMs are spun up, leading to even more complexity making it harder to understand what the applications’ behavior baseline should be. Of equal importance is what the business context is around the communications and behaviors, as well as the behavior of the underlying guest operating system processes. Security teams requires visibility into what's occurring within the environment “per plan” vs. which are deviations that could indicate a sophisticated data center attack.

IT challenge: the trade-off between performance and security

In addition to being ineffective at stopping attacks, traditional antivirus tools consume too many resources during scans. The shared resource pool of the SDDC is not optimized to support multiple machines needing excessive resources at once, so on top of being ineffective, traditional Antivirus also decreases performance. To stop performance issues from impacting business systems, IT teams focus on minimizing IOPS and preventing saturation of storage arrays, resulting in pushing back or removing antivirus tools from systems.

As with many IT challenges, the problem comes down to agility. Thanks to virtualization, IT can move as fast as the business needs, but security slows down their efforts. This creates friction between IT and security, and often results in IT prioritizing speed over security.

3. Data center applications have a broader scope of impact than end user systems

SecOps challenge: risk is greater

A breakdown of security in the data center is especially dangerous, given that if a critical application is impacted by a threat, many people are affected in addition to the company as a whole. The information contained in the data center is business critical, which means a compromise inside the data center has the potential to be much more damaging than the compromise of an end user device that most likely doesn’t contain much lucrative information stored on it.

IT challenge: remediation actions need to be business-oriented

IT and SecOps teams need to collaborate on focused remediation, balancing the needs of the business with the security impact of an incident. Often, security teams cannot simply take an entire virtual server offline to take action when an alert occurs -- they need ways to take specific action that is minimally disruptive to the business.
Best practices for securing virtualized data centers

1. Application-centric security management

The evolution of the data center has outpaced the approaches for securing it. The increased complexity of data center applications coupled with the fluidity with which applications change make it difficult for IT and security teams to know what’s expected.

• Create security controls around applications instead of hardware to drastically reduce the amount of effort involved in securing critical business data.
• Establish a baseline of the intended state of the data center with “gold images” for each VM, so deviations from expected intended state and behavior are quickly identified.
• To reduce overhead, utilize tools with that can import “blueprints” for greenfield applications, and provide automated behavior analysis for brownfield applications.

2. Reduce business impact

When dealing with attacks affecting the SDDC, security teams need to be especially sensitive to the business impact of remediation actions. Depending on the severity of the event, security teams need access to a variety of options to resolve an issue. In the shared resource environment of the SDDC, an individual machine can be the only resource supporting a given process, or one of 10 virtual servers performing a function.

• Provide IT and security teams visibility into the application context of individual VMs so business impact is clear when alert triage is taking place.
• Ensure visibility includes which applications a VM supports as well as how critical that individual VM is for the successful operation of the application.
• Utilize tools that provide a range of remediation capability so that IT and security teams are able to select the remediation action most appropriate for the scenario, including swift, yet disruptive actions like suspending or quarantining a VM, as well as less intrusive actions such as snapshot or investigation tools for capturing root cause information.

3. Leverage the virtualized infrastructure

Virtualization platforms have a long history as tools for the IT team, but in the new age of the SDDC, security teams can leverage the virtualization infrastructure ecosystem to help secure the datacenter and remediate threats.

• Ensure the SDDC security model includes a hypervisor component able to monitor machine actions - By existing separately from the attack surface, solutions that leverage the hypervisor are able to extend protection to in-guest security agents. They are able to monitor attacker behavior from a secure enclave, and even notify if an attacker attempts to destabilize the OS kernel.
• Expand your toolset of remediation options and maintain business continuity - VM management options like snapshot, suspend, and power-off can be repurposed for security remediation. Automated orchestration such as isolating network sections and creating copies of infected systems, give teams powerful abilities to block security threats, maintain business continuity, and collect attack event behavior data all with one action.
SOLVING THE SECURITY CHALLENGES OF THE SOFTWARE-DEFINED DATA CENTER (SDDC)

• Utilize your virtualization provisioning tools to automate behavioral baselining - Utilize tools for greenfield applications and “gold image” VMs.

4. Full-coverage protection against SDDC-focused attacks
Within the virtualized data center, the attack surface is primarily through network connections. Fortunately, network connections within the SDDC are largely predictable and repeatable. Web applications communicate with database servers in a predictable and consistent manner, as do integration services supporting complex applications. Persistent attackers can analyze and leverage trusted communications to eventually gain access to critical systems.

• Approach security in layers - Combine security models to ensure full coverage.
• Utilize products that can be used on physical and virtual machines - Minimize management overhead of a comprehensive security solution.
• Create a hard outer shell by locking down network connections - Significantly reduce the attack surface by identifying and only allowing approved network connections.
• Introduce process anomaly detection - Utilize tools that alert on deviations from expected environment behaviors.
• Protect the inside, in case something gets through the outer shell - Install security on endpoints that not only detects suspicious behavior, but actively disrupts attacker behavior by terminating rogue processes or denying suspicious operations.
• Utilize products that are strong against known and zero-day malware, ransomware, “living off the land” and fileless attacks.
• Increase visibility at all levels of the SDDC - Equip your team with tools that assist with root cause analysis and provide uninterrupted monitoring of events.

5. IT and SecOps as one team
Similar to the growing trend of CIOs now reporting to CISOs, everyone in IT should consider themselves to be a security professional. With the fast-paced nature of cyber security and the growing complexity of IT systems, tensions may still arise over system management. Additionally, today’s users live in a “now” world where there is a very low tolerance for disruptions, so maintaining business continuity is more critical than ever.

• Ensure IT is an active participant in the implementation of security products - Security teams establish the policies that IT teams need to follow, however, what needs to be implemented is best determined through collaboration between IT and SecOps.
• Ensure you’re protecting the whole application, regardless of what infrastructure supports it - It can be eye-opening when teams realize that a critical application is not holistically secured.
• Understand resource constraints and system limitations - To prevent decreased performance or outages for business critical applications, it’s important for security teams to work with IT to establish the middle ground.
• Establishing buy-in from the IT team can result in better security - There can be a fuzzy line between IT and security tools. IT teams may be able to identify tools that help with both security and IT management.
• Provide ongoing transparency into the security governance state of the data center - Ensure that security governance policies are well documented and accessible by the full IT/SecOps team. IT should have knowledge of any planned audits, so they can prepare. Utilize tools that help IT and security teams have visibility into the current governance state of the datacenter.
• Work together to optimize alert triage - IT understands how application interruptions impact business continuity. Utilize tools that provide visibility into business context during regular alert triage workflow.
• Utilize tools that enable security teams to use virtualization IT actions - So security teams can respond faster to security incidents that previously required the involvement of an IT VM admin.
Kitting VMware AppDefense and CB Defense for VMware

VMware AppDefense and CB Defense for VMware is a jointly-developed solution designed to fully solve the challenges of securing the SDDC. The combined solution leverages the power of the CB Predictive Security Cloud (PSC) combined with the threat detection and response capabilities from AppDefense, embedded directly into the virtualization layer.

Increase visibility within the SDDC

AppDefense and CB Defense for VMware both provide increased visibility into the SDDC. AppDefense captures the business context for virtual servers, showing how many VMs support a given business process, and their function within that process. CB Defense for VMware captures process-level metadata, showcasing what individual processes are doing on a given VM. This combined context gives security and infrastructure teams valuable insight into what is happening in the SDDC, and highlights when abnormal and unexpected behavior occurs.

Align security controls to applications

From inside the vSphere hypervisor, AppDefense monitors data center endpoints and detects when changes are made. By analyzing the intended state of data center endpoints and the applications deployed on them, AppDefense is able to build a manifest of the intended state of the applications. This contextual intelligence removes the guesswork involved in determining which changes are legitimate and which are threats. The application manifest is moved automatically with the virtual machine, wherever it is stored. AppDefense realigns security controls with applications, where sensitive data resides, instead of with the underlying infrastructure.

Prevent SDDC attacks

AppDefense and CB Defense for VMware work in tandem to stop attacks in the SDDC. AppDefense drastically reduces the attack surface by allowing only trusted network connections within the SDDC while also protecting the guest operating system from inside the vSphere hypervisor. By preventing attackers from connecting, the ability to compromise the SDDC is drastically reduced.

Complementing that approach, CB Defense for VMware, a native PSC service, delivers converged prevention, detection, and response through unique streaming prevention technology that stops both malware and fileless attacks, and is optimized for application-centric virtual data centers. Endpoint detection and response technology native to CB Defense provides an additional layer of visibility to ensure that security controls are effective, and enables threat-hunting within the SDDC.

Reduce business impact

Responding quickly to incidents is key to minimizing the business impact. AppDefense and CB Defense for VMware share alerts and remediations across consoles. AppDefense provides tight integration and orchestration through integration with core VMware management solutions, while CB Defense for VMware provides precise remediation actions. The joint solution provides the ability to respond to all SDDC alerts through powerful automated actions such as powering off a virtual server, or taking an automatic snapshot, but also provides precise remediation actions, such as deleting a file or terminating a running process.
Conclusion

The SDDC contains the most sensitive data an organization has, but traditional security solutions do not provide the protection that sensitive data requires. Creating additional challenges, SecOps and Infrastructure teams struggle to find the balance between security and performance. Organizations need a solution that protects applications and the sensitive data they store, while being optimized for the dynamic nature of the SDDC.

VMware AppDefense and CB Defense for VMware provide efficient, layered protection that leverages a secure enclave in the vSphere hypervisor to protect applications, regardless of where they are deployed. Benefits include:

- Visibility into the business purpose and function of applications, and the underlying processes that support them
- Better protection through a reduced attack surface, hypervisor-based protection, and the streaming prevention technology of the PSC
- Unified alert and remediation actions to quickly respond to any incidents that occur

Now is the time for your organization to protect the applications in your SDDC, using the big data and analytics of Carbon Black Predictive Security Cloud and the embedded hypervisor protection of VMware AppDefense.

To see the power of CB Defense for VMware and VMware AppDefense, reach out to your VMware or Carbon Black sales team to see a demonstration of the combined solution.
About Carbon Black
Carbon Black (NASDAQ: CBLK) is a leader in endpoint security dedicated to keeping the world safe from cyberattacks. The company’s big data and analytics platform, the CB Predictive Security Cloud (PSC), consolidates endpoint security and IT operations into an extensible cloud platform that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, Carbon Black has key insights into attackers’ behavior patterns, enabling customers to detect, respond to and stop emerging attacks.
More than 5,000 global customers, including 34 of the Fortune 100, trust Carbon Black to protect their organizations from cyberattacks. The company’s partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world’s leading IR firms, who use Carbon Black’s technology in more than 500 breach investigations per year.

© Carbon Black and CB Predictive Security Cloud are registered trademarks or trademarks of Carbon Black, Inc. in the United States and/or other jurisdictions.