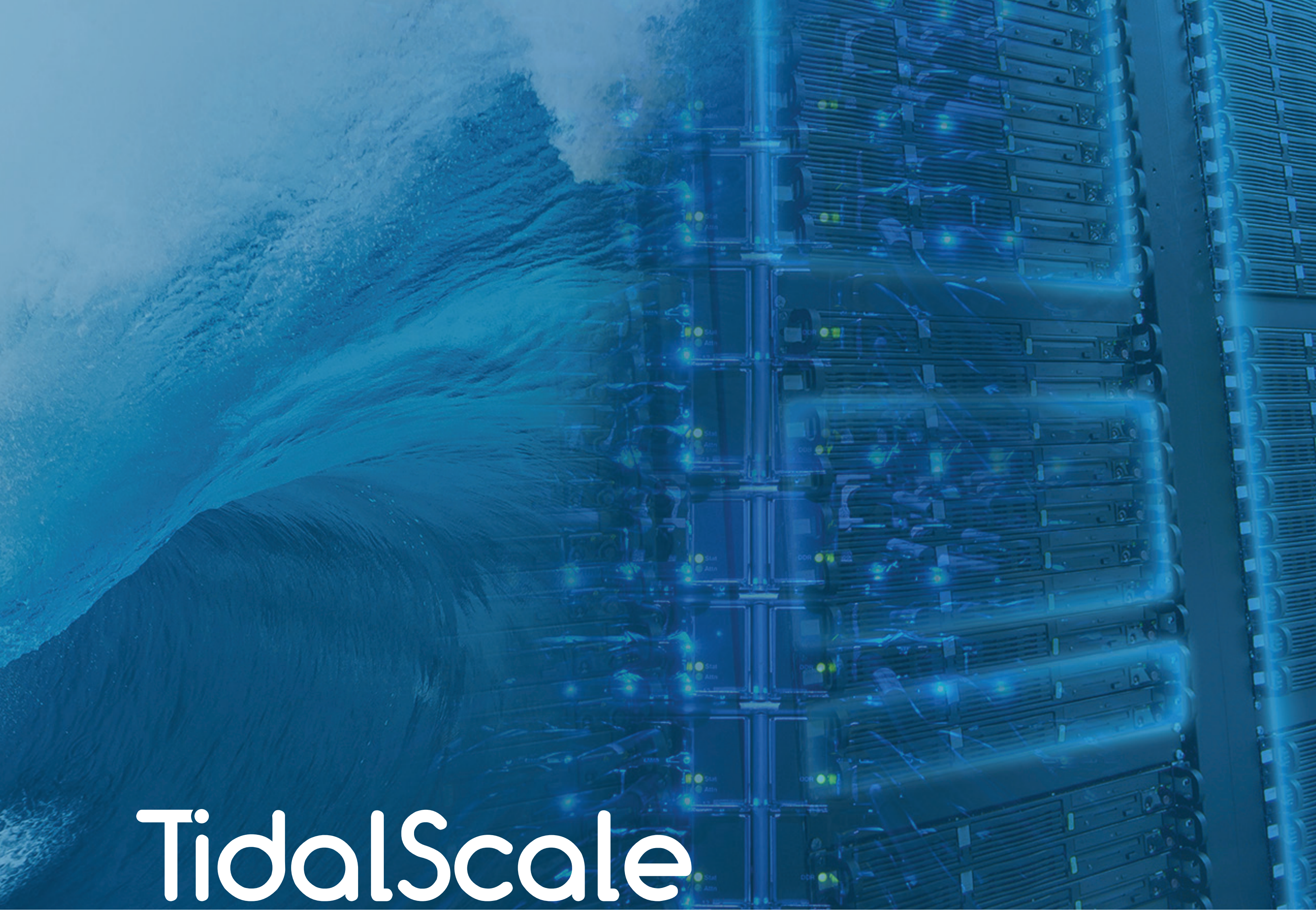


TidalScale

Shifting the Balance of Security from Attacker to Defender with TidalScale's Software-Defined Server Technology

New advances mean new threats

Often new technologies provide new areas for exploitation and malicious attack by bad actors. Technologies act as a new frontier, offering a wide expanse of advantages for both good and bad. In many ways, new platforms and infrastructure are the Wild West of the cyber world.

Naturally, IT professionals are eager to take advantage of the new advances. But they are wary of what it could mean for security. The advantages of virtualization and cloud infrastructure are too important to ignore, yet security concerns linger.

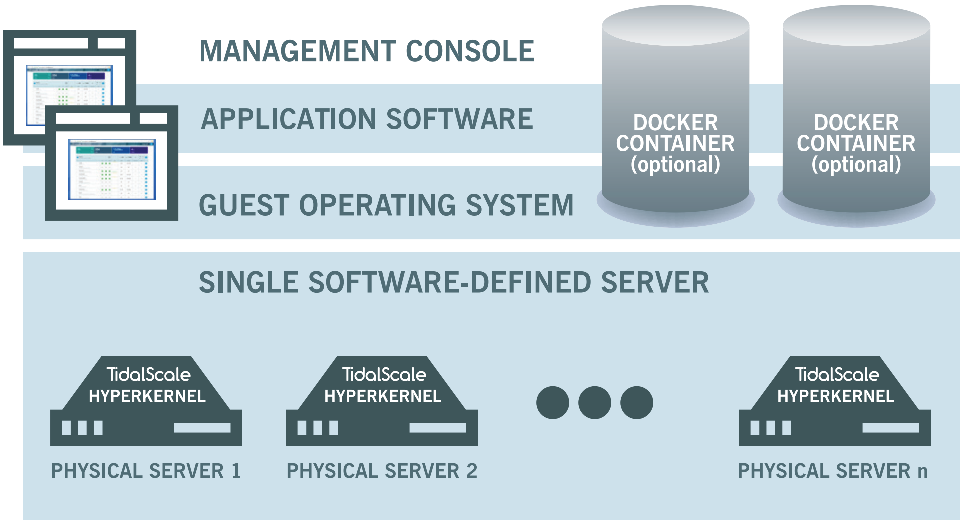
Reducing the attack surface

Security questions arise over three areas:

- The vulnerability of the new architectures;
- The defensibility of new architectures compared to conventional architectures; and
- The likelihood of an outside attacker using these new platforms to launch attacks.

TidalScale has found a way to address all of these concerns with its Software-Defined Server technology. Software-Defined Servers offer a unique approach to virtualization—one that not only solves several problems for business users and data center administrators, but several security issues as well.

The key to this is TidalScale HyperKernel software, which is powered by TidalScale's inverse hypervisor technology. Unlike traditional virtualization hypervisors, which enable multiple virtual machines to run on a single physical server, TidalScale HyperKernel binds multiple physical computers into a single, coherent virtual system that allows users to run an unmodified guest operating system, with no changes to existing applications or operating systems. All the resources associated with the aggregated systems – memory, cores, storage and I/O – are available to the application. This allows users and datacenter administrators to dynamically size servers to meet any workload, whether compute- or memory-intensive or both, while greatly reducing the usage-per-unit-cost of both hardware and software. TidalScale's inverse hypervisor works between the Guest operating system and bare metal hardware. Low-level and fast, it acts as the hardware level interface to the Guest OS.



Compared to traditional virtualization, TidalScale's inverted approach to virtualization reduces much of the attack surface over conventional virtualization technology. In fact, it even closes gaps found on traditional physical hardware.

The security benefits of inverse virtualization

Inverting the virtualization model does several important things for security. One of the most obvious is that VM-to-VM "side-channel attacks" are not possible, since there is only one VM. Another common concern, a VM escape, although still possible on TidalScale, has reduced value to an attacker. Memory space appears as being uniform, but, in reality, memory is split up between the various servers allocated for an instance. If an attacker manages to break out of the VM, memory mapping breaks which will cause the instance to restart. Additionally, an attacker will have no idea where they are in memory. They are in effect stranded. Escaping from the VM and launching new attacks is less likely.

Secure by design and by default.

Security in TidalScale is by design and by default. An instance in TidalScale has a virtual NIC with an internal IP address assigned to it from the management system. The IP address is non-routable and cannot be accessed externally. The network connection only allows SSH communication by default, so all communication to and from it is encrypted. Configuration is all through an encrypted channel; the only way to get to the management plane of the system is using the proper SSH keys. The control server, known as WaveRunner, is hardened and only allows connections on ports 443 (TLS 1.2 or above) and 22 (SSH). You also need an SSH key to get a shell prompt.

Blocking routes for data breaches.

Another major area of concern in the data center is the prospect of a data breach. Data breaches are becoming all too common, and damages are skyrocketing. Increasingly, security professionals and organizations ranging from Gartner to the FBI have agreed that a motivated attacker will find a way to gain access to the data center. Often access may come from the theft of valid credentials.

Once inside, an attacker needs to investigate the network and its resources and to move towards the assets. So, the primary mechanisms for a breach are mainly east and west activities, reconnaissance and lateral movement. In TidalScale, east and west activities are simply not possible. Since there is only one instance and it is completely isolated, there is nowhere else to go. At the same time, there is no way for an attacker to establish a meaningful representation of where they are in the data center—nothing to see and nowhere to go. Traffic sniffing would require a non-standard and difficult-to-perform specific configuration and SSH keys. Even if an attacker could sniff traffic, it is all encrypted. Furthermore, each component of the TidalScale system is separate; the OS has no access to the administrative ethernet backplane of the TidalScale HyperKernel system, and the resources are physically partitioned.

The north and south attacker activity—command and control and data exfiltration—is also pointless, since attackers cannot increase their privilege by escaping the guest. Without this increase in access there is no benefit from downloading more tools or code nor have meaningful reconnaissance information to upload. If attackers cannot get to assets, there is, of course, nothing to exfiltrate.

Total control over hardware.

Typical hardware vulnerabilities can be better managed with TidalScale. Since an instance works together as a single piece of hardware, managing various aspects is far simpler than with traditional virtualized environments. For instance, you can enforce a no USB policy and it will apply to all machines supporting an instance. You can specifically hide what aspects of hardware you would like and expose others. Every aspect of hardware is under your specific control. You explicitly configure and control what hardware is available to a guest.

Hardware-assisted means hardware-protected.

As a hardware-assisted inverse hypervisor, TidalScale makes use of Intel VT-x extensions. These extensions allow TidalScale to run a guest/host OS that expects to run in kernel mode, in lower privileged rings. With hardware-assisted virtualization, the operating system has direct access to resources without any emulation or OS modification which dramatically increases performance while maintaining higher levels of security and control.

Creating protected device and I/O domains.

Device and I/O virtualization is another area where TidalScale has important advantages for security as compared to other virtual technologies. The architecture makes use of Intel VT-d features for superior control of managing and routing I/O requests. Intel VT-d enables system software to create multiple Direct Memory Access (DMA) protection domains. Each protection domain is an isolated environment containing a subset of the host physical memory. Depending on the software usage model, a DMA protection domain represents either memory allocated in a guest-OS driver running in the host OS, or as part of the TidalScale HyperKernel itself.

The VT-d architecture enables TidalScale to assign one or more I/O devices to a protection domain. TidalScale achieves DMA isolation by restricting access to a protection domain's physical memory from I/O devices not assigned to it. This occurs by using address-translation tables, thereby providing the necessary isolation to assure separation between the virtual machine's computer resources and those of the physical hardware. When any given I/O device tries to gain access to a certain memory location, DMA remapping hardware looks up the address-translation tables for access permission of that device to that specific protection domain. If the device tries to access what is outside of the range it is permitted to access, the DMA remapping hardware blocks the access and reports a fault to the TidalScale HyperKernel.

Stay Ahead of a Moving Target

Of course, security is always a moving target. Bad actors are always pursuing new ways to steal or damage assets. Security is a primary design priority for TidalScale, and we are constantly considering new elements to stay ahead of attackers. Take, for example, bare metal processor exploits, such as Meltdown and Spectre. TidalScale implements Intel patches quickly, and we continually consider ways to prevent a successful bare metal attack to gain any further advantages. We regularly review attributes of hardware and software to keep several steps ahead. While the TidalScale performance and economics are particularly compelling, we work to ensure security continues to be an area of uncommon strength.

Learn more at www.tidalscale.com