Cisco Tetration Platform – Cloud Workload Protection

Holistic workload protection for multicloud datacenters

What is a data center? You are free to ponder that, but by all means you do not want your data center security to be defined by the infrastructure you pick. Today's data centers consist of a hybrid multicloud infrastructure using bare-metal, virtualized, and container-based workloads or anywhere in-between.

As everything revolves around software today, applications running on your infrastructure are the crown jewels, these are dynamic—these are constantly evolving. One of the key challenges is how do I provide a secure infrastructure for applications without compromising agility. Even today, the majority of data centers are designed with traditional perimeter-only security, which is insufficient. A new approach is needed to address this challenge.

Benefits

- Automate whitelist policy to enable a zero-trust model
- Minimize lateral movement through efficient application segmentation
- Identify anomalies faster using process behavior deviations
- Reduce the attack surface within the data center by quickly identifying common vulnerabilities and exposures
- Gain better workload protection for on-premises and public-cloud data centers

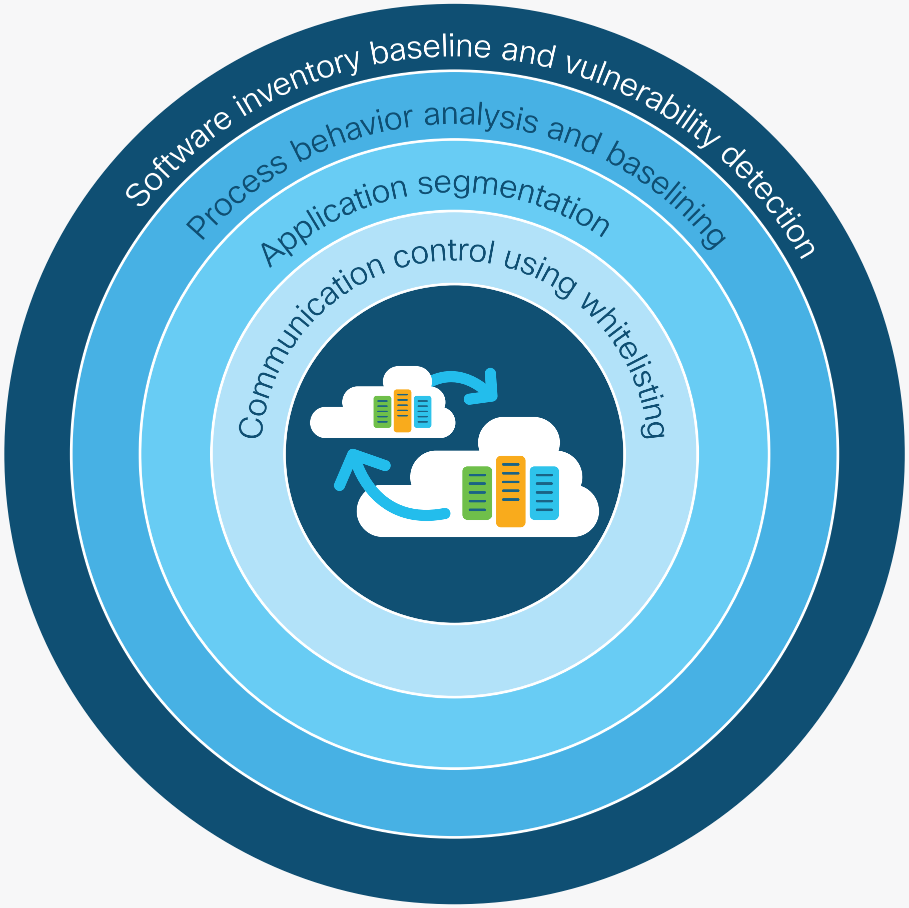
The Cisco® Tetration platform is designed to address this challenge in a comprehensive and scalable way. Tetration enables holistic workload protection for multicloud data centers by using:

- Whitelist-based segmentation, allowing operators to control network communication within the data center, enabling a zero-trust model
- Behavior baselining, analysis, and identification of deviations for processes running on servers
- Detection of common vulnerabilities and exposures associated with the software packages installed on servers
- The ability to act proactively, such as quarantining server(s) when vulnerabilities are detected and blocking communication when policy violations are detected

By using this multidimensional workload-protection approach (See Figure-1), Cisco Tetration significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and more quickly identifies Indicators Of Compromise (IOCs).

The Cisco Tetration platform is powered by big-data technologies to support the scale requirements of data centers. It can process comprehensive telemetry information received from servers in near-real time (up to 25,000 servers per cluster). Tetration can enforce consistent policy across thousands of applications and hundreds of millions of policy rules. And it is designed for long-term data retention to enable powerful forensics for such things as identifying incidents and operational troubleshooting.

Figure 1. Multidimensional workload protection approach using Cisco Tetration


Software inventory baseline and vulnerability detection
Process behavior analysis and baselining
Application segmentation
Communication control using whitelisting

For more information

For more information about the Cisco Tetration platform, please visit https://www.cisco.com/go/tetration.

Make informed security decisions for your data center

Redefine your data center security using comprehensive capabilities offered by the Cisco Tetration platform. With Tetration, operators can:

- **Implement a whitelist-based, zero-trust model:** By using advanced algorithms, Tetration generates a granular segmentation policy for each application. It provides the ability to merge business policy requirements with policies that are generated based on application behavior. This normalization and hierarchical merging of policies helps ensure that administrators with reduced scope cannot override higher level business policy intentions
- **Control communication using segmentation:** The platform provides consistent policy enforcement through server operating system capabilities across the multicloud infrastructure. Because policy is enforced on the workload itself, Tetration supports virtualized, bare-metal, and container-based environments in unison. This approach ensures that policy moves along with the workload, even when an application component migrates from a bare-metal server to a virtualized environment
- **Identify process behavior deviation:** Behavior of the servers can be determined by baselining the processes that are running on the server and identifying any deviations in behavior from those baselines. In Cisco Tetration, algorithms are available to match the behavior deviations to malware execution patterns, enabling faster detection. The behavior-pattern matching includes serious threats such as Specter and Meltdown
- **Detect vulnerabilities associated with software packages:** The Cisco Tetration platform also baselines installed software packages, package versions, patch level, and publisher. Tetration includes 19 years' worth of Common Vulnerabilities and Exposure (CVE) database. Using this information, Tetration checks whether any of the software packages have known information-security vulnerabilities listed in the CVE database. When a vulnerability is detected, you can find complete details, including the severity and impact score, identify all servers that have the same version of the package installed, and define policies with specific actions, such as quarantining a host when servers have packages with certain vulnerabilities

The Cisco Tetration platform is unlike any other in the industry. Holistic workload capabilities allow you to build a more secure infrastructure for applications and significantly reduce the risk of exposure. It offers a turnkey approach for security and minimizes the time and effort required to operationalize the platform.