Delivering Application Microsegmentation with Cisco Tetration
Contents

Market overview and background ........................................ 3
Steps to application microsegmentation ............................... 4
Cisco Tetration approach to application microsegmentation ... 6
Conclusion ........................................................................... 17
For more information ......................................................... 18
Market overview and background

Data security breaches are on the rise, and the average cost per incident is estimated to be $3.62 million.¹ Customers are evaluating ways to mitigate the devastating effects of these breaches. Some examples of products, solutions, and business processes garnering much attention include security audits, awareness training, zero-trust model, visibility and management tools, cloud workload protection, and even cyber liability insurance.

The zero-trust model specifically received great attention following the 2015 U.S. Office of Personnel Management (OPM) data breach. In an investigative report by the House of Representatives Committee on Oversight and Government Reform, the committee’s second recommendation was “Reprioritize Federal Information System Efforts Toward a Zero Trust Model.”² Zero-trust redefines the classic trust model; the legacy notion of trusting “inside” and not trusting “outside” no longer applies. For example, Verizon reports 25 percent of security breaches involve internal actors.³ The other 75 percent of breaches are perpetrated by outsiders who find a weakness and move laterally from there. Therefore, it is imperative to restrict perpetrators’ movement should they find a vulnerability. One of the five criteria by which Forrester Research judges an enterprise’s zero-trust maturity is “Data and Network Segmentation.”⁴

The term “segmentation” has been used for decades to describe network-based separation, such as VLANs, for both management and security purposes. More recently, “microsegmentation” has emerged as a security method for isolating workloads by permitting only required (allow-list) traffic. “Application microsegmentation” adds further context to workload segregation, by introducing application context. Essentially, it means that a hacker who has breached a workload serving an application cannot move laterally to attack another application host. In this model, the hacker is isolated to the workload servicing the specific tier of the compromised host of the application.

This white paper examines the steps required to achieve application microsegmentation and describes uniquely scalable and innovative approach the Cisco Tetration™ solution takes to fulfilling the requirements in each step.

---

Steps to application microsegmentation

There are six steps to deploying application microsegmentation successfully, as shown in Figure 1.

![Diagram showing the steps to successful application microsegmentation]

**Figure 1.**
Steps to successful application microsegmentation

**Step 1: Inventory and flow discovery**

First, customers need to know what exists in their environment. As Rob Joyce of the National Security Agency’s Office of Tailored Access Operations states, “If you really want to protect your network, you really have to know your network. You have to know the devices ... the things inside it.”\(^5\) The requirements for this discovery step include:

- Pervasive visibility and accounting for all devices, all packets, all network flows, all processes
- Discovery across different environments, including private data center or public cloud, wherever customers’ services and data exist

---

[https://www.youtube.com/watch?v=bDjbBWOYdA](https://www.youtube.com/watch?v=bDjbBWOYdA)
Step 2: Application mapping and insight

Structure and context need to be applied to the large set of devices and raw flows discovered during the previous step so that this data becomes organized in a meaningful manner at the application level. The requirements for this step include:

- Associating all workloads and flows to applications in an automated fashion
- Identifying tiers of an application via intelligent clustering algorithms and mapping the dependencies (protocols, ports, services) between these tiers
- Identifying external dependencies of these applications
- Creating application blueprints showing all the internal and external dependencies

Step 3: Policy recommendation

Once application insight is gained, a first pass at an application microsegmentation policy can be made. The requirements for this step include:

- Recommendation of policy based on accurate empirical evidence; that is, based on a comprehensive set of network flows that have been collected during step 1, and processed with the context provided in step 2
- Intent-based policy expressed in natural language and abstracted from network constructs; for example, allowing Security Operations (SecOps) to create a policy that says the development lifecycle can never communicate with the production lifecycle without having to reference IP addresses or VLANs
- Export of policy in standards-based format such as normalized JSON or XML so the policy can be consumed by open enforcement points or orchestrators

Step 4: Policy validation and simulation

Nothing beats tribal knowledge, and very likely the recommended application microsegmentation policy requires fine-tuning using this knowledge. Although the customer would have performed discovery for a representative duration in step 1, flows and inventory may still be missing due to seasonal effects. The requirements in this step include:

- Continued monitoring of live traffic against the recommended policy, validating for any flow violations
- Fine-tuning of policy and simulation of policy with modifications against a historical data lake
- Controlled and human approval of policy after validation and simulation
Step 5: Policy deployment and microsegmentation

Step 4 results in a “golden policy.” This policy can now be deployed at enforcement points. The requirements in this step include:

- Policy deployment that translates the natural human language described in previous steps into infrastructure and network language
- Software-defined application microsegmentation that can be deployed in any cloud and any data center, wherever customers’ applications and workloads exist
- Support for enforcement options in network (software-defined networking [SDN] or firewall) or at workload (virtual machine, bare metal, or container)

Step 6: Compliance and day-2 operations

Once application microsegmentation has been deployed, day-2 operations tasks include ongoing monitoring and maintenance of the policy as applications update, migrate, and/or scale up and down. The requirements include:

- Continued monitoring of the efficacy of the application microsegmentation deployment for any packet and flow violations and compliance to policy
- Dynamic software policy updates that follow workload scale and mobility, (location and IP address independence)
- Audit trail of changes
- Alerting of third-party tools, including security information and event management and network management systems
- Ability to perform forensics search of flows and processes going back months as something suspicious arises

Cisco Tetration approach to application microsegmentation

The Cisco Tetration solution uses big data technologies and artificial intelligence, leveraging unsupervised machine learning and behavior analysis, to deliver application microsegmentation. Cisco Tetration applies consistent microsegmentation policy for each application, regardless of whether the applications live in private data centers, in public clouds, or both. This means customers can migrate their workloads while the policy remains intact.

The Cisco Tetration solution is composed of the sensor framework and the analytics platform. Sensors collect precise telemetry, which is processed in a big data analytics platform. Figure 2 describes the architecture.
Figure 2.
Cisco Tetration solution comprising a sensor framework plus an analytics platform

The Cisco Tetration platform addresses the requirements in each of the six steps in a uniquely precise, scalable, automated, and efficient way.

**Step 1: Inventory and flow discovery: The Cisco Tetration sensor framework advantage**

Inventory and flow discovery has matured over time, as shown in Figure 3.

![Diagram showing inventory and flow discovery maturity](image)

Decades ago, projects with inventory, flow communications, and application dependencies required consultants to comb through spreadsheets and documentation, as well as interview operators and application owners. This was a time-consuming method and produced results that were often inaccurate or quickly became outdated.

This method was improved with scripting and horizontal discovery using a combination of ping or Simple Network Management Protocol (SNMP) polling and Secure Shell (SSH)/rlogin scripts, along with Windows Management Interface and other management tools. While this was a major improvement over the manual process of interviews and static documentation, it represented a point-in-time snapshot of the network, which can be inaccurate, akin to looking at a traffic intersection at rush hour versus midnight. Furthermore, these polling scripts were sometimes blocked, as they were mistaken as illegitimate probes.
Additional improvement was made with Test Access Points (TAPs) and Switched Port Analyzer (SPAN). A continuous TAP/SPAN session collecting all traffic can be very accurate if deployed pervasively, but rarely is that the case. Inserting a TAP can be disruptive and SPAN sessions come with a high overhead cost (both CPU and bandwidth). Furthermore, the large volume of data collected is rarely retained for more than a week, and often not for only a few hours. Dramatic improvements to data retention and greater horizontal visibility were introduced with NetFlow, a technique initially implemented by Cisco and described in information document RFC 3954. However, one drawback is that NetFlow aggregates flow data into records, causing the specificity at the packet level to be lost, along with awareness of directionality of the client–server relationship (who initiated the session).

Point-in-time snapshots of the network, and sampled and aggregated views, may be adequate for real-time troubleshooting, but they are inadequate for security use cases such as application microsegmentation. For an accurate microsegmentation policy, visibility needs to be pervasive and comprehensive. Cisco Tetration overcomes these limitations by employing a sensor framework based on a next-generation intelligent sensor. Multiple options for software sensors that run at the workload are available for the customer, as are network sensors based on Cisco Nexus® 9000 Series Switches: custom Application-Specific Integrated Circuits (ASICs), Encapsulated Remote Switched Port Analyzer (ERSPAN), and NetFlow. These sensors examine every packet header of every single flow. Some 150 telemetry data points are collected and sent to the data analytics platform for upstream processing. Software sensors can also collect system-level information, including process, Process ID (PID), parent PID, and owner. Because only metadata is sent from the intelligent agent upstream to the analytics platform engine, the bandwidth overhead is very low compared to SPAN and TAP solutions, which replicate the full packet header. If not the full packet.

Cisco Tetration sensors can be deployed across different environments, such as private data center or public cloud, and across host types, including virtual machines, bare metal hosts, and containers.

In short, the Cisco Tetration intelligent-sensor approach allows for collection of the richest telemetry based on examining every packet header of every flow with system process and other context, without sampling and aggregation. In this way, the most comprehensive and accurate inventory and flow communication is discovered.

Step 2: Application mapping and insight: The Cisco Tetration big data and algorithmic differentiator

The value of big data in vertical industries such as healthcare, retail, manufacturing, and hospitality has long been recognized. With Tetration, Cisco is pioneering the use of algorithmic approaches and big data for IT applications, operational analytics, and security use cases.

Following the precise inventory and flow communication discovery using the intelligent sensor framework described in previous step, the telemetry continues to be processed through the Cisco Tetration big data analytics platform shown in Figure 2. Millions of events per second from tens of thousands of sensors are processed at this platform. Other inputs to the platform include load balancer configuration and IP Address Management (IPAM), Configuration Management Database (CMDB), and other tags or annotations. Through unsupervised machine learning and behavior analysis, patterns are identified and application insight is gained at data center scale.

---


Workloads that behave similarly are automatically identified and grouped together in a cluster, and clusters are automatically identified in the application. Dependencies within, among, and external to the clusters are identified and mapped, as shown in Figure 4. These dependencies include protocols, ports, and services.

Figure 4.
Chord chart view of relationships

The result is a highly accurate application blueprint that allows the customer to understand the true communication patterns within the environment and where business intelligence and sensitive data reside. Figure 5 shows an example. From here, microsegmentation policies can be applied consistently within and external to the application, across environments and host types.

Figure 5.
Application view of dependencies
Step 3: Policy recommendation: The Cisco Tetration intent-based policy differentiator

In the previous step, Cisco Tetration employed an algorithmic approach and automatically mapped the relationships based on accurate live communication in the environment(s). Tetration now uses the application dependency mapping results to automatically generate a allow-list composed of permit/deny rules, which can be used as a first-pass application microsegmentation policy recommendation. An example is shown in Figure 6.

![Automatically generated microsegmentation permit/deny rules](image)

**Figure 6.**
Automatically generated microsegmentation permit/deny rules

On top of the automatically created microsegmentation policy rules, Cisco Tetration allows absolute policies based on customer’s intent to be added. **Figure 7** shows how a Tetration operator can easily create a rule using natural language to block HIPAA workloads from communicating with non-HIPAA workloads, and PCI workloads from communicating with non-PCI workloads.

![Readable absolute policies based on intent](image)

**Figure 7.**
Readable absolute policies based on intent
These human-readable, user-friendly rules are automatically rendered to associated network and infrastructure constructs at the time of deployment or export. This policy can be exported in (Figure 8) JSON, XML, and YAML formats or a northbound system can subscribe and consume the same information through the open API.

Figure 8.
Open Export Options

By leveraging intent-based policies and abstracting these policies from the infrastructure, Cisco Tetration enables business logic automation, rather than requiring customers to understand every single VLAN, IP subnet, and network construct, resulting in meaningful microsegmentation policies.

**Step 4: Policy validation and simulation: The Cisco Tetration big data and simulation differentiator**

Before the recommended policy is approved, human validation is typically required. No machine will have the understanding of business requirements and the tribal knowledge that customers have. This human understanding is key to perfecting the microsegmentation policy Cisco Tetration has recommended based on its machine-learning algorithms. Incorporation of business requirements into policy was already discussed in step 3 along with intent-based policy. In this step, Tetration supports passive policy analysis by continuing to monitor every packet of every flow to assess the compliance of the flows against the recommended policy. Tetration analyzes both complete and incomplete flows. Figure 9 explains the four flow categories and illustrates how Tetration classifies all flows against these four categories:

- **Permitted:** Flows that are permitted per policy, and completed
- **Mis-dropped:** Flows that are permitted per policy, but did not complete
- **Escaped:** Flows that are not permitted per policy, but did complete
- **Rejected:** Flows that are not permitted per policy, and did not complete
Figure 9.
Four categories of flows

Because Cisco Tetration continues to analyze all flows, customers have the assurance that live flows that are in violation of policy are flagged for investigation (Figure 10).

Figure 10.
Analysis of policy
In addition, Cisco Tetration leverages superior big data technologies so that customers can modify, delete, and experiment with policies and run simulations of these policies against the vast hundreds of terabytes in a data lake deep store. This experimentation is critical to the success of any application microsegmentation deployment, as it gives customers the confidence that their policy is not only accurate for live traffic but is based on historical data. For example, it is not easy to arrange for end-to-end application testing with partner connections, so an app team may be limited to running a comprehensive suite of user tests during a short maintenance window. It may be impossible to arrange for a longer duration or multiple windows to test application microsegmentation policies. But, because Tetration keeps the historical flow information in a vast data lake, SecOps and apps teams can now go back to this testing interval and run repeated simulations with different policies until the policy rules are perfected. Figure 11 shows an example of a policy experiment called sim1 running against historical data from months before.

![Figure 11. Simulation comparing an experimental policy to the data lake of flows from previous months](image)

Once the simulations show no violations against policy, the customer can approve the policy to become the “golden” or baseline policy. Cisco Tetration will continue to monitor all flows against this baseline policy for violations as described.
Step 5: Policy deployment and microsegmentation: Multiple enforcement options across heterogeneous environments

Following live policy analysis and simulations, the customer will have confidence in the policy, which can then be used for application microsegmentation. Cisco Tetration automates the deployment of the application microsegmentation policy with a single click. The policies are pushed to a variety of workloads, such as virtual machines or bare metal, on which Tetration software sensor agents are running. The software sensors orchestrate the stateful policy enforcement using operating system capabilities such as IP sets and IP tables in the case of Linux servers, and Windows advanced firewall in the case of Microsoft Windows servers. The Cisco Tetration approach allows application microsegmentation to be achieved across environments, including on-premises data center and public cloud, as shown in Figure 12.

![Tetration enforcement option]

1. Leverages final version of Tetration policy
2. Pushes relevant policy rules to each workload
3. Workload deploys policy using host firewall
4. Continuously recomputes policy from identity and classification changes

**Figure 12.**
Application microsegmentation across environments

Furthermore, Cisco Tetration ensures the application microsegmentation policy moves with the workload in a virtualized environment, enabling customers to achieve application mobility without compromising security.

In addition, a customer may choose to enforce a coarse grained version of the policy at other infrastructure elements such as network firewalls. Cisco Tetration is an open platform, and ecosystems partners such as security orchestrators Algosec\(^9\) and Tufin\(^10\) consume the microsegmentation policy and then translate and push it to network security device configurations and workflows.

In summary, when it comes to application microsegmentation, Cisco Tetration offers customers the most flexible policy deployment options at the host, network firewall, or any combination thereof. Furthermore, the one-click host-based enforcement in Tetration works across any workload (bare metal, virtual machine), across any environment (public cloud or private data center).

---


Step 6: Compliance and day-2 operations: The Cisco Tetration compliance and ecosystem differentiator

The customer will manage and monitor the application microsegmentation implementation as part of day-2 operations. Cisco Tetration continues to monitor every packet of every flow as illustrated in Figure 10, thereby ensuring policy compliance. As workloads scale up or down in day-to-day operations, and as workloads migrate between servers or between environments, the Tetration platform updates the policy automatically so that the customer does not have to be concerned with infrastructure-specific segmentation policy.

Cisco Tetration also integrates with customers’ existing tools, including SIEM (Security Incident and Event Management), IPAM (IP Address Management), and CMDB (Configuration Management Database), to improve IT operations with its deep visibility and insight. Over 20 ecosystem partners integrate with Tetration via Open API, Kafka message bus, or user apps.  

For example, Cisco Tetration can be configured to send an alert to a SIEM if a compliance violation occurs or an anomaly is detected. A Tetration app on Splunk is available for multiple use cases, including compliance events.

Another ecosystem integration is with CMDB. As described earlier, Cisco Tetration performs comprehensive inventory discovery, which can be pushed to CMDB and result in the creation of a common interface, if one does not exist. This capability helps with asset management and operations. Furthermore, once Tetration identifies an exception, it can trigger a workflow to automatically create a service desk ticket. Figure 15 shows the Tetration app for ServiceNow.

---


12 See https://splunkbase.splunk.com/app/3632/

For day-to-day security operations, Cisco Tetration allows the customer to perform a forensics search of suspicious activity going back months, as shown in Figure 16 for a potentially vulnerable service, NetBIOS.

Figure 14.
Forensics search analyzing potential vulnerable flow/service
Conclusion

The Cisco Tetration solution’s microsegmentation capability enables data center and security operations teams to automate the enforcement of highly specific policies for their mission-critical applications running in both on-premises data centers and the public cloud. By applying a consistent policy across virtual machines and bare-metal hosts, this model significantly reduces the data center attack surface.

The Cisco Tetration approach can be summarized as follows:

- By starting with a rich telemetry collection based on every packet of every flow and context that includes process ID, the most accurate inventory and network flow information are discovered.
- The collected data is processed in a big data platform. Big data is used for data center scale, and an algorithmic approach leveraging machine learning and artificial intelligence is used to automatically identify patterns and workload clusters and to gain application insight.
- A recommended policy is generated from the automated application dependency discovery. This policy may be supplemented with intent-based rules determined by the customer’s specific business logic, such as “non-HIPAA can never speak to HIPAA.”
- Big data is further leveraged as customers run simulations against historical data in the vast data lake, while the application microsegmentation policy is tweaked and perfected.
- The deployment of the application microsegmentation policy is automated and extensible across heterogeneous environments (cloud, data center) and enforcement points (network firewall, network fabric, host) and type of host (bare metal or virtual machine).
- For day-2 operations, the platform identifies application behavior and compliance deviations and invokes appropriate workflows for policy updates as workloads scale up or down or move. More than 20 ecosystem partners, including IPAM, SIEM, and CMDB vendors, integrate with Cisco Tetration to improve overall IT operations management.

The Cisco Tetration solution’s precise, intelligent, intuitive, and scalable approach differentiates it as the industry-leading application microsegmentation solution. Customers can have confidence that their microsegmentation policy is accurate and secure and will not break applications when deployed, because of the precise inventory and discovery, automated application insight garnered from unsupervised machine learning, historical simulations against the deep data lake, and compliance and day-2 support tools in Cisco Tetration.

It is also important to recognize that, beyond application segmentation, Cisco Tetration supports other IT operations management, IT services management, network performance management and diagnostics, and Development and Security Operations (DevSecOps) use cases. Therefore, an investment in Tetration for microsegmentation also represents an investment in these other important IT functions. And because Tetration leverages an algorithmic approach using artificial intelligence and big data analytics, it also helps ensure compatibility with future developments, given this strategic direction for next-generation data centers.
For more information

https://www.cisco.com/go/tetration