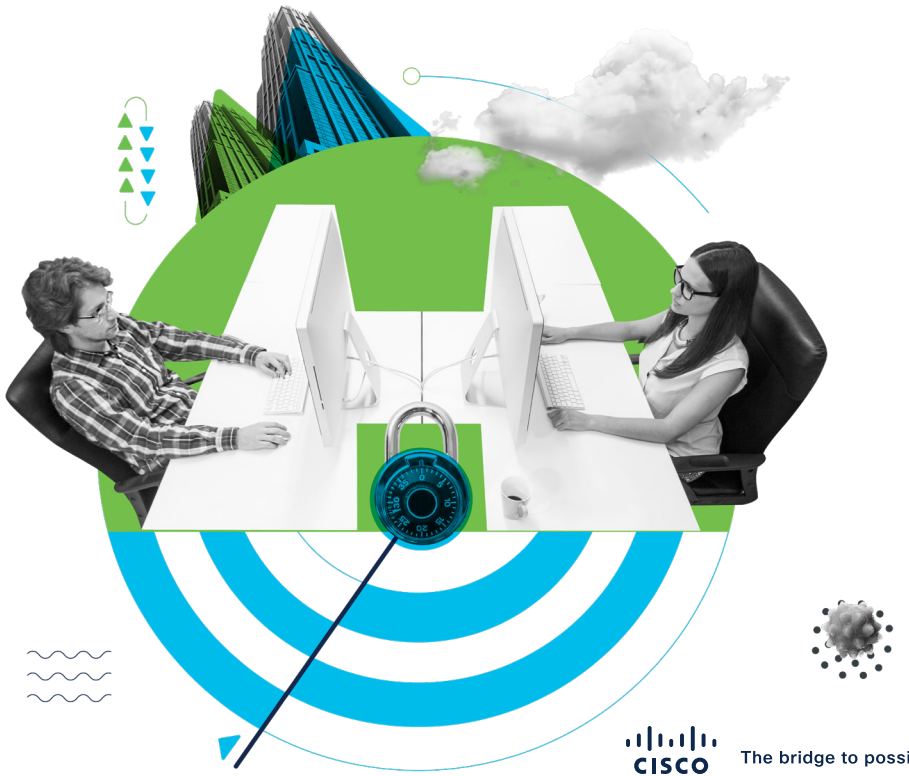
Cisco Stealthwatch and Cisco Tetration Workload Security

Robust workload protection, microsegmentation, and pervasive threat visibility for any cloud-based infrastructure

Achieve Visibility and Security in the Cloud

Enterprise networks are increasingly becoming more complex as applications and their workloads move to the multi-cloud and leverage containers and microservices, effectively creating new security, reporting, and compliance challenges. This transformation is rapidly expanding as organizations with growing remote work forces migrate more infrastructure to cloud environments and expand their virtual desktop infrastructure footprints. This shift to the cloud often has a direct trade-off with security, visibility, and control, and stands to inadvertently increase the likelihood of vulnerabilities and high-severity threats being missed. The need for comprehensive visibility of all network traffic down to the individual workload level for effective security policy management and enforcement has never been more important than now.

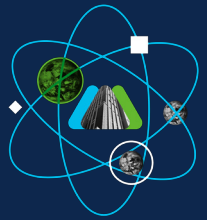


© 2020 Cisco and/or its affiliates. All rights reserved.

Benefits of Cisco Stealthwatch and Cisco Tetration

Greater visibility

Achieve network visibility and security analytics both on-premise and across all cloud-based applications and workloads



Better detection

Detect and respond to threats at the application workload level in your cloud infrastructure environment

Enhanced protection

Robust multi-cloud workload firewall via microsegmentation to contain lateral threat movement

Enabled zero trust

Implement a zero trust model via continuous behavioral monitoring and automated enforcement of microsegmentation policies to every workload

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Stealthwatch

Network-based threat detection through scalable visibility and security analytics

Cisco Stealthwatch is a network detection and response (NDR) solution that leverages pre-existing infrastructure to offer enterprise-wide, contextual visibility of network traffic from the private network to the public cloud. Stealthwatch collects and stores all network telemetry and applies advanced security analytics to detect and respond to threats in real-time. Using a combination of behavioral modeling, machine learning and global threat intelligence powered by Cisco Talos, Stealthwatch can quickly and with high confidence, detect threats such as command and control attacks, ransomware, DDoS attacks, illicit cryptomining, unknown malware, as well as insider threats. Stealthwatch then provides additional guidance on how best to respond to expedite incident response efforts. With a single, agentless solution, Stealthwatch offers comprehensive threat monitoring across the data center, branch, endpoint and cloud, and even into encrypted traffic.

Stealthwatch can also conduct forensic analysis on stored network telemetry to aid in lateral threat movement investigations, ensure ongoing zero trust verification by continually monitoring behavior after access is provided, and can even detect threats in encrypted traffic, without decryption to further augment threat detection and cryptographic compliance. And since it is agentless, Stealthwatch is a cost-effective, automated, network-based threat detection and response solution that scales easily to growing networks and cloud infrastructures.

Comprehensive multi-cloud security posture management

Organizations that have moved resources and workloads to public cloud environments like AWS, Azure, and Google Cloud Platform face a multitude of new security, policy, and compliance-related challenges. Stealthwatch offers robust cloud security posture management (CSPM) capabilities such as monitoring risk exposure levels related to configuration, network segmentation, user, and system events to guarantee sound policy management and protect against data leakage. Stealthwatch also provides behavioral threat & IoC (Indicator of Compromise)-based detections, response & remediation capabilities, and collects and stores all your workload network telemetry to ensure that compliance standards are met.

Complete visibility of network traffic across on-premises and public cloud environments

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Tetration

Contain lateral movement using application microsegmentation

Cisco Tetration is a holistic workload protection platform that enables security teams to implement a secure, zero trust model for application workloads in heterogeneous, multi-cloud environments through microsegmentation.

Using the Cisco Tetration platform, you can automatically generate highly specific microsegmentation policies based on complete visibility of application communications, running processes and their dependencies. Tetration is built for scale, providing fully automated enforcement of a dynamic microsegmentation policy to every workload. A discrete policy set is computed for each workload, distributed via the Tetration software agent and programmed for enforcement by the native operating system firewall capabilities (either iptables or Windows Advanced Firewall).This approach delivers stateful and consistent segmentation across multi-cloud data centers at scale by preventing lateral threat propagation and providing automated updates to microsegmentation policies as application dependencies and communication patterns change. Additionally, for virtualized and containerized environments, segmentation policies move with their associated workloads, allowing for increased application mobility without the need for infrastructure-specific segmentation policies.

Reduce risk and attack surface using cloud workload protection capabilities

In addition to microsegmentation, Cisco Tetration helps reduce security risks and the attack surface by identifying workload behavior anomalies and identifying software vulnerabilities. It monitors workload processes and communication activities to detect and alert on malicious behaviors such as privilege escalations, shell-code execution, MITRE techniques and tactics, and more. It also maintains a real-time full inventory of all software packages, operating systems and detects common vulnerabilities and exposures (CVEs) associated with installed software. In addition, Tetration identifies vulnerable workloads, by enabling dynamic policies to be provisioned to protect these vulnerable machines from exploit or applies effective quarantine policies until the necessary patches are applied.

Enable implementation of consistent microsegmentation across application workloads

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Stealthwatch and Tetration Together

Improve security with analytics and enforcement for cloud applications and workloads

Networks are growing to the point where they're too large and complex to manage manually at every touchpoint. Deploying Cisco Stealthwatch and Tetration expedites incident response efforts and reduces the overall attack surface across both hybrid and multi-cloud environments by providing the pervasive visibility needed to quickly detect and respond to suspicious network events, automate policy generation and enforcement for all application workloads, and contain lateral threat movement through microsegmentation.

Enable zero trust via network analytics and workload segmentation

Achieving comprehensive zero trust and true end-to-end visibility across on-premises and multi-cloud environments requires robust network-based detection and response, as well as automated microsegmentation, policy generation, and enforcement capabilities. Stealthwatch's best-in-class analytics enable zero trust via continuous behavioral monitoring to flag any suspicious activity and to simplify compliance. Tetration enables zero trust through deep workload visibility and adaptive enforcement of microsegmentation to effectively reduce the attack surface.

Easily extend threat detection and remediation to the cloud

Stealthwatch provides comprehensive visibility and threat detection across your private network that can be easily extended to the multi-cloud. And with Tetration, you can automate policy generation and enforcement, and prevent threat propagation by containing lateral movement across workloads running in multi-cloud environments through microsegmentation. Together, these solutions ensure that you don't have to compromise on security as you adopt hybrid and multi-cloud. Detect threats using Stealthwatch, and then prevent them from spreading across your workloads and take action to remediate them using Tetration.

Next steps

Cisco Stealthwatch and Tetration work together to provide visibility, threat detection, microsegmentation, and policy compliance and enforcement across all cloud-based infrastructures.

To learn more about stealthwatch, visit
www.cisco.com/go/stealthwatch

To learn more about tetration, visit
www.cisco.com/go/tetration

Or, contact your local account representative.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

PROJ2183566 08/18