The bridge to possible

Securing Remote Workforce and Optimizing Resources with Visibility and Security Analytics from Cisco Stealthwatch

Businesses need to be flexible with most, if not all, of their workforce going remote. Ensuring availability and uptime is paramount. They quickly need to assess how and when users are accessing the network and applications, and whether they are doing it securely. With the attack surface expanding exponentially, it's more important than ever to gain visibility into who is on the network and what they are doing in order to detect threats immediately.

Organizations can do this easily with Cisco Stealthwatch®, a solution that provides enterprise-wide visibility, from the private network to the public cloud, by collecting network telemetry. It then applies advanced security analytics using behavioral modeling and machine learning to pinpoint anomalies and further reduce them to critical alerts for the detection of advanced threats in real-time. With a single, agentless solution, you get comprehensive threat monitoring, even in encrypted traffic.

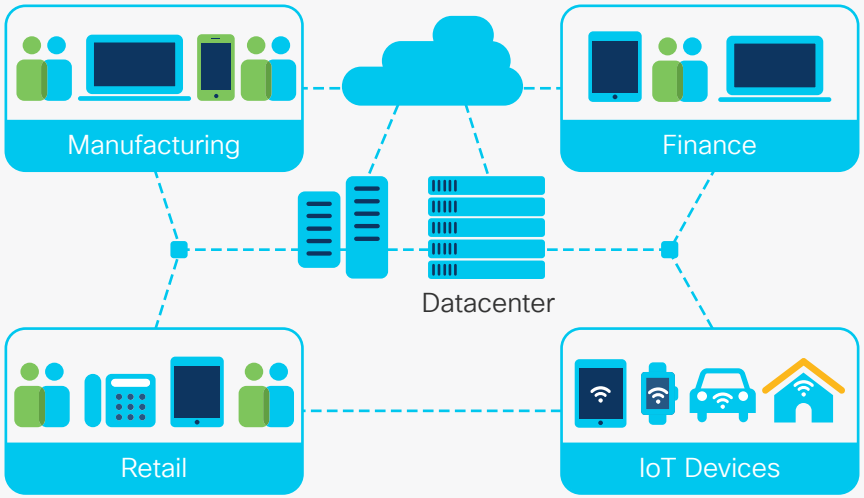
Stealthwatch provides simple and effective management and monitoring capabilities to organizations for multiple use cases involving a remote workforce. Let's take a look at a few of these.

The bridge to possible

Monitoring remote users

The ability to monitor and control remote access tops the list of security concerns as the number of remote workers, third-party partners who need access, and adoption of the cloud continue to rise. Using Cisco Stealthwatch host groups*, you can define, identify, and monitor remote users. You can create a host group that contains internal VPN IP addresses to keep track of the remote users who have network access.

*A **host** within Stealthwatch is defined as any entity or device connected to the network. A **host group** is essentially a virtual container of multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology.



Create logical groupings customized to your business within Stealthwatch.

There are different ways you can gain insights from Stealthwatch with the remote user host group:

- **Visibility into network traffic:** With Stealthwatch, you can see which users within the host group are responsible for the most traffic, determine the top applications being used by remote users, see how they are interacting with other users as well as corporate assets, and even get visibility into communications occurring outside the organization. You can also perform a flow search based on multiple parameters, filtered by time period, for more granularity. By specifically monitoring the traffic between remote users and critical assets within the network, you can make optimal decisions to ensure access and availability.
- **Policy violations:** Stealthwatch also has the ability to create security events that will trigger if a particular security policy is being violated. In this way, you can customize the security of your organization based on business and regulatory workflows. For instance, if the corporate policy is to restrict access from remote users to the PCI servers, you can create an event for it within Stealthwatch. In this way, Stealthwatch can ensure that the policies you have set using other tools are actually being enforced.

"Cisco Stealthwatch has been **absolutely critical** in our characterization of network traffic during Disaster Recovery/ Business Continuity Planning (DR/BCP) scenarios – it was able to seamlessly rebaseline our expectations for VPN bandwidth capacity. This led to strategic planning decisions around application usage, video teleconferencing, remote patch management, collaboration solutions, and much more. Stealthwatch was essential in diagnosing at least **6 critical network issues** in the past 4 weeks – and it did so **in minutes**, not hours or days. More people have demanded access to this capability, and now even our endpoint engineering team is leveraging it to capacity plan remote software deployments."

– Senior VP, Cybersecurity
Large Financial Services Company

- **Threat detection:** The core value of Stealthwatch, beyond providing visibility, is that it can pinpoint suspicious behavior that might be an early indicator of a larger security incident. Using a combination of behavioral modeling, machine learning, and the industry-leading threat intelligence from Cisco Talos®, Stealthwatch can process billions of network sessions, create a baseline of what normal network behavior looks like, identify anomalies, and further reduce them to a few critical alerts that your security team needs to look at. So if a remote user suddenly starts downloading a large amount of data from a sensitive data server, and further exfiltrates it outside the network, the user might be infected with malware, and Stealthwatch will alert the security analyst on this behavior and provide enough information to effectively investigate and respond to the incident.

Optimizing resources and critical assets

As described above, by monitoring the top applications and assets that remote users are accessing, Stealthwatch can aid you in making optimal capacity decisions surrounding resources.

You can definitely expect a spike in VPN traffic and demand to go along with the rise in remote workers. But this sudden spike could also be the result of a security incident. With Stealthwatch, you can easily determine if the VPN gateway interface is either overloaded or close to capacity, and identify the applications, users, or hosts that are taxing the network. You can further investigate the concerned traffic to determine if the utilization is due to a legitimate business workflow, or if it can be attributed to a threat. Based on that, you can either plan for additional resources or take steps to remediate the security incident to address potential response time issues.

Enhanced endpoint visibility

Cisco AnyConnect® Network Visibility Module (NVM) collects rich flow context from an endpoint on- or off-premises to enhance the flow details Stealthwatch is receiving from the network, specifically providing Stealthwatch with the ability to understand the:

- Device – the endpoint, irrespective of its location
- User – the one logged in to the endpoint
- Application – what generates the traffic

This enhanced endpoint telemetry further increases the accuracy and context of Stealthwatch alerts for faster incident response for your organization.

The bridge to possible

About Cisco Stealthwatch offers

Stealthwatch can be deployed without any agents or probes and is available in two offers - on-premises as a hardware appliance or a virtual machine called Stealthwatch Enterprise. Or as a Software-as-a-Service (SaaS) solution called Stealthwatch Cloud.

To get started with Stealthwatch, sign up for a free visibility assessment.

Conclusion

You need visibility to determine how remote users are accessing the network for optimal capacity planning as well as monitoring this increased attack surface for security threats. A tool like Cisco Stealthwatch enables you to do so effectively.

Additional resources

- Use case: Monitoring remote access users
- Use case: Detecting policy violations
- Use case: Monitoring interface for security operations
- Use case: Monitoring interface for network operations

You can find all the Stealthwatch use cases here.

- Video: Monitoring remote VPN traffic - Cisco Stealthwatch Enterprise
- Video: Monitoring remote workers - Cisco Stealthwatch Cloud
- How-to guide – Deploying Cisco Stealthwatch Endpoint License with Cisco AnyConnect NVM

C22-743675-00 04/20