Cisco Stealthwatch with Web Security Appliance

How You Benefit

- **Turn your network into a sensor.**
  Get real-time visibility into activity on your network. Stealthwatch uses data produced by your current infrastructure and translates it into actionable information.

- **Obtain contextual awareness.**
  Gain visibility around proxy conversations and add contextual information from the Cisco Web Security Appliance.

- **Improve incident troubleshooting.**
  Reduce complexity and achieve end-to-end visibility into both web and network traffic.

- **Take action on advanced threats.**
  Achieve greater control over user access to content on the web or on your network.

Improve Security by Extending Network Visibility

People are accessing the web through multiple devices and from inside and outside your network. That accessibility helps your business operate smoothly, but it can also leave your organization vulnerable to security breaches. Cybercriminals are adept at exploiting weaknesses, and threats are becoming more advanced. With so many entry points to monitor and protect, detecting anomalous behavior is becoming a real burden for many organizations. It's no longer a question of if you'll be breached, but when.

Your business needs greater network visibility and the additional context associated with web and network traffic. Without access to both elements, securing a complex enterprise is almost impossible.
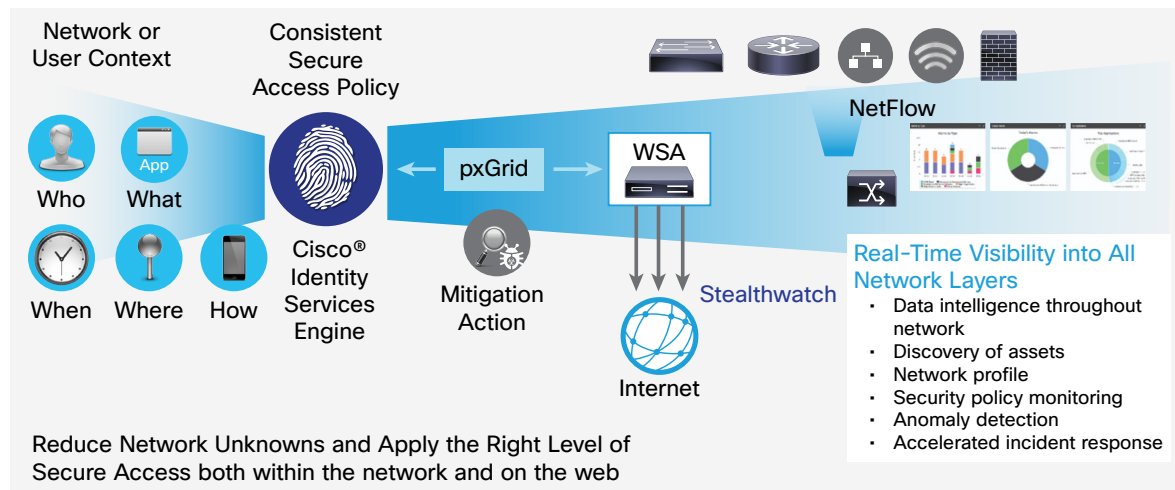
By deploying the Cisco® Stealthwatch Proxy License and the Cisco Web Security Appliance, you can achieve that.

Gain Real-Time Awareness

Cisco Stealthwatch provides situational awareness of all users, devices, and traffic on the network and in the data center. It reduces the complexity and fragmentation of networks and gives you visibility across the expanded attack surface to help you better secure the network.

Cisco Identity Services Engine (ISE) extends these capabilities by delivering superior user and device visibility to support enterprise mobility experiences and control access. It shares data with integrated partner solutions to speed their capabilities to identify, mitigate, and remediate threats.

Figure 1. Visibility, Context, and Control for Highly Secure Web and Network Access

Network or User Context

Consistent Secure Access Policy

Who   What
When   Where   How

Cisco® Identity Services Engine

pxGrid

Mitigation Action

NetFlow

WSA

Stealthwatch

Internet

Real-Time Visibility into All Network Layers
- Data intelligence throughout network
- Discovery of assets
- Network profile
- Security policy monitoring
- Anomaly detection
- Accelerated incident response

Reduce Network Unknowns and Apply the Right Level of Secure Access both within the network and on the web

You Can't Protect What You Can't See

Having visibility into web and network traffic is essential. Stealthwatch collects and translates NetFlow information from various devices and transforms it into actionable information. Cisco web security provides consistent, high-performance web security and policy management regardless of where or how users access the Internet. It is the most effective defense against web-based malware, and it offers the best application controls and URL filtering to manage data loss risks, employee productivity, and bandwidth usage. As part of a pervasive security strategy for the enterprise, Cisco web security enables better data and brand protection and helps to ensure compliance.

Stealthwatch provides real-time visibility into your network by using NetFlow information from devices such as routers, switches, and firewalls. The Stealthwatch Proxy License feature extends that network visibility by working with the Web Security Appliance to see into web traffic. This visibility provides you with the context that you need to respond to advanced threats quickly and streamline investigation and analysis.

Tying It All Together with Cisco ISE

Stealthwatch and the Web Security Appliance together can provide you with extended visibility, but they are even more powerful when combined with ISE. Cisco ISE collects network and contextual information based on user and endpoint identity, which can help you quickly identify bad actors on the web and inside the network. Once identified, those users can be prevented from accessing websites or devices on the network while you continue to investigate the incident. You can create, change, and enforce critical usage policies for each user on the network for improved incident response.

Next Steps

For more information on how Stealthwatch with Web Security Appliance can provide visibility and context around potential threats across your entire network, visit www.cisco.com/go/stealthwatch or contact your local Cisco account representative.