Anatomy of a Threat Report

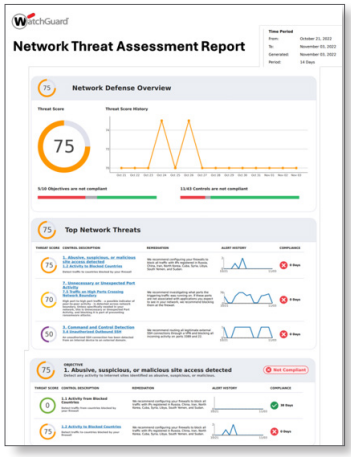
Introduction

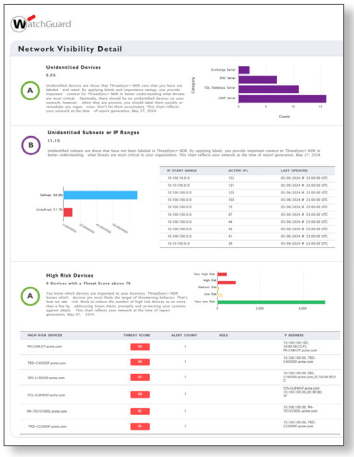
How much visibility do you have into what is happening on your network? Which devices are communicating with each other, and what types of data are being transmitted to and from your network? Understanding your network's activities and identifying its risks and threats are crucial for protecting your entire organization and your suppliers, partners, and customers.

By proactively assessing your network's security status with automated risk and threat reports, you can identify vulnerabilities or cyberattacks that may have evaded your perimeter defenses. This proactive approach empowers you to address these issues before damage occurs, strengthening your cybersecurity strategy and safeguarding your organization.

Core Network and Ransomware Reporting

ThreatSync+ NDR includes a Network Threat Report and Ransomware Defense Report. Both reports start with a summary section that displays the entire network's overall risk score and trend. They then provide detailed information on various policies and controls actively monitored by the NDR system. Each sub-section shows the individual threat score and trend line for each policy or control being monitored, and if any gaps or failures are found, guidance on how to remediate them. These reports are easily customizable to meet the specific needs of organizations or cyber defense programs. Their purpose is to highlight existing issues and provide managers with a way to establish network defense goals and track progress and improvements toward them.



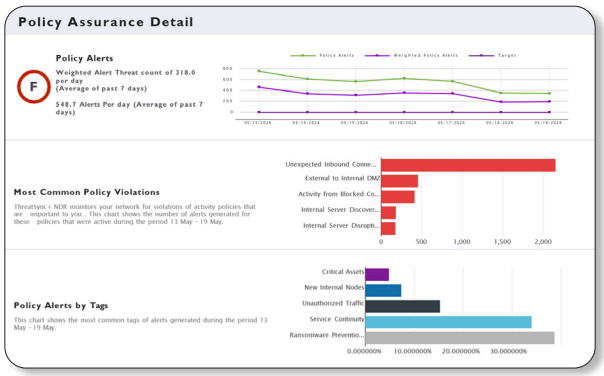


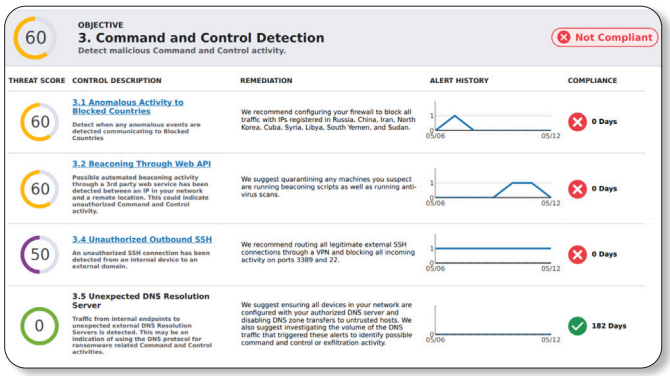
Network Threat and Ransomware defense reports provide highly detailed assessments of what is happening inside your network. They are essential to your cyber defense program because they provide the information needed to understand your security posture and what steps to take to improve it. The specific information included will vary depending on the assessment findings but typically include:

- A list of all the security risks that were identified.
- The criticality level of each risk, typically classified as critical, high, or medium.
- A description of each risk, including the type, severity, and potential impact.
- Recommendations for removing each risk, such as installing security updates, removing malware, isolating devices, changing credentials, or configuring security settings.

Examples of specific security risks that may be identified in the assessment:

- Activity on unsecured ports
- Command and control detection
- Unauthorized remote access
- Failed backups
- Unnecessary and unusual port activity
- Actively exploited vulnerabilities
- Open alerts
- Unidentified and high-risk devices
- Policy violations
- Malicious network activity
- SMB leakage
- Unusual VPN activity





To learn more about the WatchGuard Network Threat Report and Ransomware Defense Report, please contact your WatchGuard representative.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com

WatchGuard

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com