

Forward Threat Exposure

Compute every attack path. Defend what matters.

Overview

Security tools identify vulnerabilities, but teams also need to know which ones attackers can reach. Security teams still make decisions based on assumptions: that a subnet is isolated, that a vulnerability cannot be reached, or that an attacker on a compromised endpoint cannot reach production. Replacing those assumptions with evidence requires a complete, verified view of every device, path, and control along the way.

Forward Threat Exposure computes every attack path to your critical assets using a mathematically accurate digital twin of the production infrastructure, built from its actual configuration and state. It accounts for the routing, firewall, and host-based controls along each path, so results reflect the defenses already in place, without injecting test traffic or running exploits in production.

The Outcome

A moderate vulnerability that an attacker can reach can outrank an isolated, critical one. Forward Threat Exposure combines scanner findings, reachability, and business importance to prioritize exposed assets. It shows the paths and enforcement points where teams can block access, so they can reduce exposure while patching is underway.



Forward Threat Exposure use cases

- **Crown jewel risk prioritization:** rank business-critical assets using the Forward Risk Score, combining reachability, vulnerability severity, and business importance.
- **Pre-patch exposure containment:** trace attack paths hop by hop and identify where teams can block access while patching is queued.
- **Lateral movement exposure analysis:** map indirect paths to critical systems through adjacent hosts and security domains.
- **Vulnerability management:** identify which vulnerable systems attackers can reach from the internet and other untrusted networks and prioritize remediation accordingly.
- **Compensating control validation:** confirm where existing controls contain exposure, so teams can focus urgent remediation on systems that remain reachable.
- **Stepping stone and risky asset triage:** identify vulnerable internal hosts that are reachable from untrusted networks and could provide a path to critical assets.

Capabilities

Complete path visibility

See direct and lateral paths to critical assets across on-premises and multi-cloud environments, including paths where no monitoring agent is installed.

Automatic mitigation analysis

See the devices and firewall rules along each attack path, so your team can apply mitigations, such as threat signatures or access control changes.

Deterministic answers

Reachability calculated from complete device configuration and state, providing evidence of which paths are permitted, rather than relying only on observed traffic or logs.

Read-only and agentless analysis

Collection is read-only and agentless. Attack path analysis runs on the digital twin without injecting test traffic or executing exploits in production.

Risk-ranked prioritization

Prioritize exposures in one ranked queue using the Forward Risk Score, which combines reachability, vulnerability severity, and business importance.

Validate existing controls

Account for the routing, firewall, and host-based controls along each path, so risk scores reflect the defenses already in place.

Why it matters

See every exposure

Perimeter controls block direct access to critical systems, but they often leave indirect routes open. Forward Threat Exposure computes direct and lateral paths from exposure points to critical assets, including the firewalls and controls along each one. Path analysis accounts for routing, NAT, load balancers, and cloud policies.

Scope incidents with confidence

During an incident, teams need to know which systems a compromised endpoint can reach. Forward Threat Exposure identifies every host, port, and vulnerable service reachable from that endpoint, enabling teams to focus on log searches, investigation, and containment.

Prioritize risk by reachability and impact

Severity alone cannot tell teams which vulnerabilities put critical assets within an attacker's reach. Forward Threat Exposure combines reachability, vulnerability severity, and business importance so teams can prioritize assets exposed directly or through intermediate vulnerable hosts.

Reveal paths monitoring hasn't observed

Traffic-based monitoring sees only the flows that have crossed monitored links, so a path that has never carried traffic can remain unseen. Forward Threat Exposure computes those paths from configuration and operating state, revealing potential access before traffic uses it.

Limit what AI-driven attackers can reach

As AI accelerates reconnaissance and vulnerability testing, defenders need to identify exposed paths before attackers use them. Forward Threat Exposure computes attack paths to critical assets from the network's configuration and state, so teams can identify where to block access before a patch is available.

Enforcement point analysis: inspect the full path to an exposed asset, including the devices, firewall rules, and NAT boundaries along the way. Identify the device and rule where your team can block access.

Pre-patch containment: close reachable paths at the network layer while the patch is pending, as exploitation increasingly begins before a fix is released.

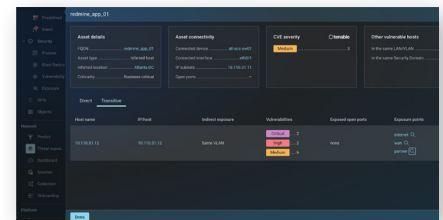
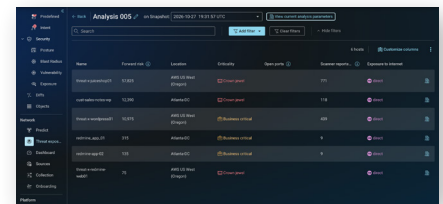
Focus on reachable risk

Forward Threat Exposure ranks each critical asset by how easily an attacker can reach it, how severe its vulnerabilities are, and how much it matters to the business.

Exposure points: define up to four external or untrusted traffic origins, such as the public internet, partner connections, or guest subnets, each with an assigned trust level.

Asset criticality: assign assets to crown jewels, business critical, or critical infrastructure tiers, so rankings reflect operational importance rather than CVSS scores alone.

Forward Risk Score: calculates a composite score for each critical asset: Exposure Score multiplied by Vulnerability Score multiplied by Asset Criticality. The analysis accounts for existing controls, so a reachable moderate vulnerability can outrank an isolated critical one.



Analyzed end-to-end
in one model



Google Cloud



Built for the way security teams work

Security boundaries mapped

Firewalls, virtual systems, and zones protecting each host are mapped, and unsegmented paths to internet gateways are identified.

Works with your tools

Ingests vulnerability findings, operating system information, and open port data from Tenable® and Rapid7®.

GET STARTED Talk to an expert at www.forwardnetworks.com/contact