Trend Micro™
DEEP DISCOVERY™ NETWORK ANALYTICS

Prioritized actionable threat intelligence to mitigate current and existing threats

We call on security products and services to keep our businesses and organizations safe. Most of the time they do exactly what we want them to do; detect, alert, and block threats trying to land a successful attack. However, the downside is that they produce a lot of data, some of it relevant, some of it not. It is up to the security professional(s) in the organization to comb through the potential thousands of alerts or events each day to determine what is actually a threat and decide whether or not they need to respond. Compounding this problem is a worldwide shortage of cybersecurity staff or personnel that needs to be trained to decipher these events. Trend Micro™ Deep Discovery™ Network Analytics automates the correlation of advanced threat events. This provides faster resolution with fewer people involved, while providing an in-depth picture of the full attack. In some cases, you may believe the attack started today, but in fact, the initial breach happened weeks or months ago.

Deep Discovery Network Analytics:
- Continuously analyzes current and historical network metadata and correlates these related threat events into a single view for full visibility of the attack cycle.
- Uses advanced and sophisticated machine learning techniques to detect network traffic anomalies.
- Correlates the events and maps out every step of the attack, quickly answering the questions of of "what", "who", and "where": Giving you a better idea of how to respond and prevent future attacks.
- Utilizes expert intelligence to correlate and connect threat detection events against network and endpoint* access events, presenting threat investigators with complete view of the attack lifecycle.

KEY CAPABILITIES

- **See the full attack lifecycle** An attack isn’t just a point in time. Advanced or targeted attacks take time and use multiple attack vectors to execute. Deep Discovery Network Analytics gives you the chronological order of correlated threat events to easily visualize the entire lifecycle and truly understand the attack and protect yourself from future attacks.
- **Full visibility into the “what”, “who”, and “where”** Deep Discovery Network Analytics will correlate and help simplify threat events to show you: What was the first point of entry of the attack? Who else in the organization has been impacted by the attack? Where was the threat calling out to? (i.e. command and control communication) With visibility and answers into these three questions, you will have a better understanding of the threat’s impact on your organization and how to prioritize your response.
- **Prioritize your response** By knowing the extent of an attack and its severity you can determine which threat requires immediate response and which threats may be able to wait.
- **Play out the attack** With the click of a button you can see the entire attack play out chronologically from the URL redirects, to the initial infection point, to the lateral spread across the network. See every movement or scale it down to just see what happened this morning or over a weekend.
- **Dig deeper into each step of the attack quickly** It is great to have visibility into an attack but sometimes you need the details. Just by hovering your mouse over an attack event, you can immediately see pertinent details of the attack at network and endpoint event levels such as; protocol used, severity, triggered rule, SHA1, number of transactions and dates they span, etc.
- **Correlate retroactively against historical network data** The average threat can go undetected for over three months once it slips past your existing security. In most cases, when you finally see it you may never know when it first entered your network or how. By storing the events for six months or more you can look back at delayed attacks and see not only how it spread, but also the infection point to make sure you put the right safeguards in place so it doesn’t happen again.
- **Flexible deployment options** Prefer to keep everything in-house? Want to offload everything to the cloud? Deep Discovery Network Analytics has a deployment option to meet your needs by offering an on-premises solution or an “as-a-service” solution hosted in the cloud.

**Attack Visibility**
- Correlate six months of events
- See the full attack lifecycle
- Go beyond the infection point
- Watch the attack play back
- Learn the methods used in the attack

**Prioritization of Response**
- Understand the scope of the attack
- Know the attack severity
- Quick detection and analysis of comprehensive attacks

---

"Trend Micro Apex One™" endpoint detection and response required