Endpoint Detection and Response Service Description

PDI's Endpoint Detection and Response (EDR) service offers management and monitoring of the Advanced Endpoint Threat Prevention Agent installed on Customer devices. Management activities include service provisioning, threat prevention, and detection policy updates based on a Customer request. Monitoring activities include collection, storage, reporting, and Customer notification of security events. Additionally, tools for self-service reporting and analysis are available through the PDI portal.

Service Components

Agent Deployment

The Advanced Endpoint Threat Prevention Agent is deployed on the Customer's endpoints (servers, desktops, etc.) according to the Customer's current software deployment method while utilizing any existing infrastructure (AD GPO, SCCM, etc.). PDI assists the Customer with an Agent deployment project plan, including - but not limited to - identifying candidate systems, creating deployment groups, and selecting appropriate deployment dates for installing the Agent across the Customer's environment. The Customer owns the initial deployment process and controls the change management process for deploying the Agent to their environment during both the initial and ongoing Agent deployment. Thereafter, Agents update automatically.

Log Collection and Retention

PDI's Advanced Endpoint Threat Prevention Agent collects all device metadata for analysis. The collected data includes all network activity, DNS requests, HTTP requests, processes, file operations, registry modifications, and scheduled tasks. PDI receives all Agent security alerts for analysis and storage via Syslog. As a part of the EDR service, PDI retains 400 days of alerts generated by the Agent.

Tuning

The Advanced Endpoint Threat Prevention Agent is initially installed in "Monitoring" mode, followed by a tuning period. During this time, PDI watches log data and adds the required exemptions if needed. Once the solution has completed the bake-in period, PDI moves the devices to "Protect" mode.

Threat Prevention and Detection

The deployed Advanced Endpoint Threat Prevention Agent employs behavioral analysis and machine learning technologies to prevent advanced cybersecurity threats. The Agent addresses the entire threat execution lifecycle (pre-execution, on-execution, and post-execution) with the smallest impact possible on endpoint performance. The scalable and lightweight Agent can be deployed on Windows, macOS/OS X, & Linux workstations and servers. The Agent looks at advanced malicious behavior across multiple vectors to rapidly eliminate threats and adapt defenses against the most advanced cyberattacks.

Threat Monitoring and Analysis

PDI's Security Operations Center (SOC) is engaged 24x7x365 to monitor, triage, and respond to alerts received from the Advanced Endpoint Threat Prevention Agent. SOC utilizes PDI's proprietary threat detection and response platform to perform advanced analytics and investigate Indications of Compromise. Events are analyzed and escalated to the Customer based on the schedule set in the Support section of this document. If Support hours are defined by alternate Customer contracts already in place, these hours take precedence over the hours defined in this document.

Remediation Guidance

PDI guides the Customer to perform remediation of detected threats. Expert Security Analysts review, research, and recommend best practice actions to minimize impact and restore systems to operational status. The Customer can choose to either accept or ignore PDI's remediation guidance.

Policy Updates

In the event of a false positive or performance impact on a critical application, PDI works with the Customer to configure the proper policy exemptions. PDI also works with the Customer to determine the proper policy to apply to the various devices on the Customer network.

Security Review

As part of the Service, PDI provides a Security Review (via myNuspire) that includes real-time service health/performance, log analytics, reporting, and recommendations. For an additional charge and at the Customer's request, PDI-guided Security Reviews include an analyst-guided review of open recommendations, service health/performance, industry-specific threat intel, and log analytics.

Case Management

As a part of the service, the Customer can open and manage cases in the myNuspire Customer Portal as well as via email and our toll-free service telephone number. For cases to be resolved, the Customer must respond to issues raised in new cases and updates to current cases.