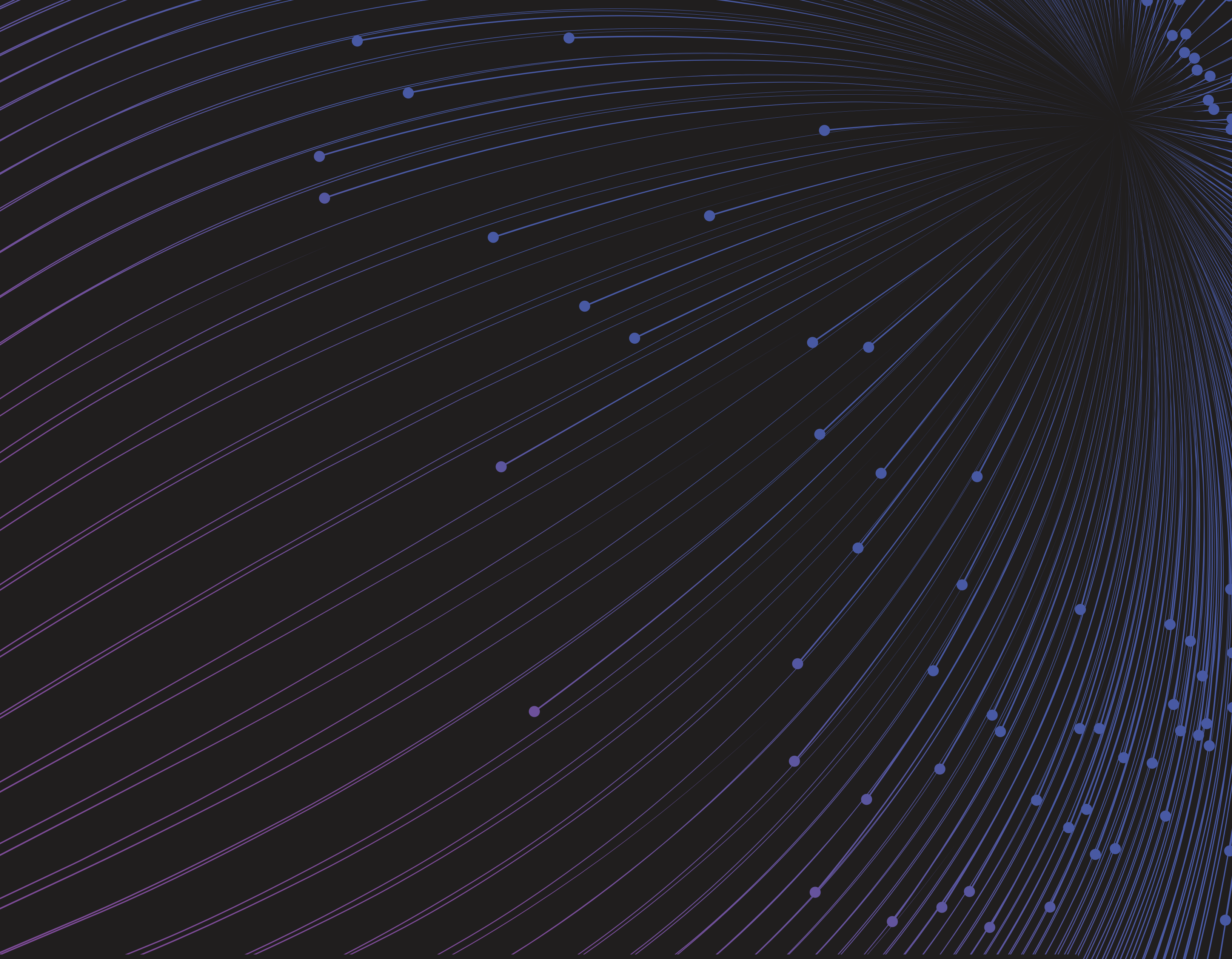

Cylance® and Thycotic Join To Prevent Malware from Exploiting Endpoints

Lowering Risk by Ensuring Only Authorized Applications Are Running in Your Environment

CYLANCE

thycotic

Introduction

Cylance and Thycotic have formed a technology alliance which combines their proactive strategies to prevent malware from exploiting endpoints. This two-step prevention process involves removing local administrative rights from endpoints and using artificial intelligence (AI) to identify and block malware before it executes.

Value Statement

The integration between Cylance and Thycotic offers organizations AI driven threat prevention capabilities and enterprise-wide privileged account management (PAM). This integration reduces operational friction by ensuring that application whitelisting, blacklisting, and privilege elevations are correctly set proactively on day one of deployment and automatically correlated thereafter in an ongoing basis. Cylance provides the continuous protection by blocking malicious and unwanted or unauthorized applications before they execute and also stopping file-less attacks from using legitimate system resources. Exceptions can be made by policy based on business need for different users and groups within the organization. This gives the ability to match the right application privileges to each user or user group, which provides greater control over risk throughout the company. Cylance and Thycotic both employ very lightweight solutions which demand considerably fewer system resources than their competitors.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first security solutions and specialized services that change the way organizations approach endpoint security. Cylance security solutions combine AI-driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise. Visit www.cylance.com for more information.

About Thycotic

Thycoctic's privileged account management (PAM) system is easily managed and readily adopted. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, D.C., Thycotic operates worldwide with offices in the UK and Australia.

Use Cases

Reputation Report

- Challenge: During an investigation, security analysts must navigate between multiple applications to gather all available threat intelligence to determine if endpoints and applications are safe.
- Solution: Cylance uses a prevention-first approach to security which leverages AI to proactively stop threats. Along with Thycotic, this allows incident responders to conduct investigations in a low-risk state, and analyze aggregated data for speedier downstream decision making of both endpoint access and the reputation of applications.
- Additional Benefit: With Thycotic, enterprise accounts or endpoints flagged as suspicious can quickly have their access permissions modified, reducing the risk of further system infection.

DATA Global List Management

- Challenge: Managing application whitelists and blacklists is critical to ensuring the robustness of an organization's security posture. Without proper maintenance, these lists can obstruct daily functions or become high-risk vulnerabilities.
- Solution: The Cylance and Thycotic integration combines both safelist/quarantine hashes and file reputations to provide detailed information to security teams. A one-click link to the Cylance Threat Details page allows security administrators to easily perform file validations for further safelist/quarantine additions.
- Additional Benefit: Additions to the quarantine list based on external intelligence creates lateral consistency across the organization.

Workflow Integrity for Application Control

- Challenge: Application control cannot be based on user request or justification alone. Safelisting an application without understanding its full impact on the rest of the environment creates security risks.
- Solution: With the Cylance and Thycotic integration, application control policies can be quickly configured using information collected on the software in the environment. Knowing which programs require administrative rights, which are trusted files, and which are malicious, will aid security admins in crafting effective access policies. The Privilege Manager provides a simplified console view specifically designed for the help desk. Workflow approval options are integrated with a mobile app which allows admins to approve/deny application executions on the endpoint in real time.
- Additional Benefit: CylanceOPTICS™ can be configured to take aggressive containment actions when a harmful endpoint is discovered. It can also take response actions when a pre-defined rule is triggered, leaving security teams free to take other actions.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE