CYLANCE™

SMB Platform

Solution Brief

> *"Signature and behavioral anti-malware are no match for next-generation adversaries who utilize mutating hashes, sophisticated obfuscation mechanisms, self-propagating malware, and intelligent malware components."*
>
> – James Scott,
> Institute for Critical
> Infrastructure Technology

Cylance Endpoint Security for SMBs

Small to medium-sized businesses represent a unique set of challenges to cybersecurity providers. While enterprises often have a dedicated team and an executive in charge of securing endpoints and the data on those endpoints, IT administrators of SMBs wear many hats. As such, enterprise solutions do not always serve SMBs effectively. To effectively serve this segment, the security provider needs to understand what motivates an SMB to act. Psychographics are also different among SMB IT administrators. Whereas enterprise IT admins are often focused on optimization and advanced security practices, SMBs tend to favor options that provide maximum benefit for minimum budgetary impact and can be very cost conscious, choosing 'good enough' security measures that meet the minimum criteria to preserve business continuity. The reason for this and other behaviors is simple: often an SMB lacks discretionary budget, security expertise, and the scale to deploy and manage complex security measures that are more common in enterprises.

SMBs Are Resource Constrained: According to the 2017 Verizon DBIR, "Over three-quarters of these victims are small businesses and may not have dedicated security staff and/or processes. The data-loss numbers can be massive, but they are (typically) considered less sensitive than regulated data varieties (e.g., Payment Card Information, Protected Health Information). The site administrators may not be as concerned about disclosure of usernames and passwords, and it may be easier for them to notify and force password changes than to implement two-factor authentication, conduct penetration testing, or ensure the Content Management Platform is up to date."[1]

SMBs Lack Cybersecurity Expertise: Attackers often target the SMB. "For SMBs, there's a 90% likelihood of a single data breach costing more than $200,000, and a 10% likelihood of a single data breach costing more than $450,000, with a median (50% likelihood) cost of about $357,000."[2]

SMBs Are Prime Targets For Cyberattacks: This danger magnifies the importance of a simple yet effective cybersecurity solution to serve SMBs. The objective of this document is to provide a framework for positioning Cylance® products under the additional scrutiny of reducing the complexity and alert volume that makes it difficult to detect, contain, and respond when threats occur. Further, forward-thinking SMBs have recognized that a signature-based approach is outmoded and only exacerbates the challenge of providing cybersecurity with a smaller staff.

"Signature and behavioral based anti-malware are no match for next-generation adversaries who utilize mutating hashes, sophisticated obfuscation mechanisms, self-propagating malware, and intelligent malware components. It is no longer enough to detect and respond. Artificial intelligence offers the predictive quality that can give organizations a much-needed edge on their more sophisticated, less burdened, and more evasive adversaries."[3]

The Cylance Solution For SMBs: Cylance recognizes that SMBs are subject to the same cyberthreats as enterprises, but are further challenged by the constraints described above. Cylance offers full-featured, artificial intelligence driven products and services, including CylancePROTECT®, CylanceOPTICS™, CylancePROTECT Home Edition, and Consulting Services that are perfect for SMBs. These offerings simplify endpoint security, giving you the confidence and peace of mind to focus on running your business.

With **CylancePROTECT** and **CylanceOPTICS,** you get real-time predictive threat prevention combined with prevention based detection and incident response. Built from the ground up to scale with your business without compromising simplicity or effectiveness, the solution delivers the following security functionality:

CylancePROTECT	CylanceOPTICS
AI driven malware prevention	AI driven root cause analysis
Real-time memory protection	SMB-optimized threat hunting
Integrated script and application control	Dynamic threat detection
Device usage policy enforcement	Automated incident response

CylancePROTECT Home Edition protects corporate employees and their family's personal devices using artificial intelligence to detect and prevent malware. Ensuring employees' personal devices are safe reduces companies' risk of malware spreading from the home to the corporate network. By utilizing machine learning techniques instead of reactive signatures, CylancePROTECT Home Edition keeps families safe by rendering new malware and unknown future variants useless, making security simple with a 'set it and forget it' experience. CylancePROTECT Home Edition lets consumers benefit from Cylance's enterprise-grade technology that delivers the best protection without bogging down their systems with the bloated features and annoying pop-ups associated with traditional consumer security products.

Not all SMBs have the security expertise to install and maintain these best of breed products. Cylance offers a complete set of **Consulting Services** to assist:

Cylance Service	Description
ThreatZERO™	Configure CylancePROTECT with policies tailored to your environment and network configuration.
Incident Containment and Compromise Assessments	Determine if a security breach has happened or is actively occurring. Know when, where, and how a compromise occurred.
Red Team Services	Cylance identifies and prioritizes risks though penetration tests, assessments, and social engineering.
Industrial Control Systems	Enjoy the perfect combination of deep experience in critical infrastructure that delivers an unrivaled level of service and protection.
Internet of Things and Embedded Systems	Secure IoT and embedded devices, and their associated ecosystems.
Training	Attend a variety of ICS/SCADA security-focused training for developers, testers, engineers, project managers, and security professionals.

Cylance provides a complete set of endpoint security products and services that are optimized for SMBs. To lean more or to schedule a demonstration, please see Cylance.com or your sales representative for details.

[1] Source: 2017 Verizon DBIR, 10th edition, April 2017

[2] Source "The State of SMB Security Risks: Why Most SMBs are Looking to MSSPs", Aberdeen Group, November 2016

[3] Source: "Signature Based Malware Detection is Dead", James Scott, Institute for Critical Infrastructure Technology, February 2017

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

CYLANCE™