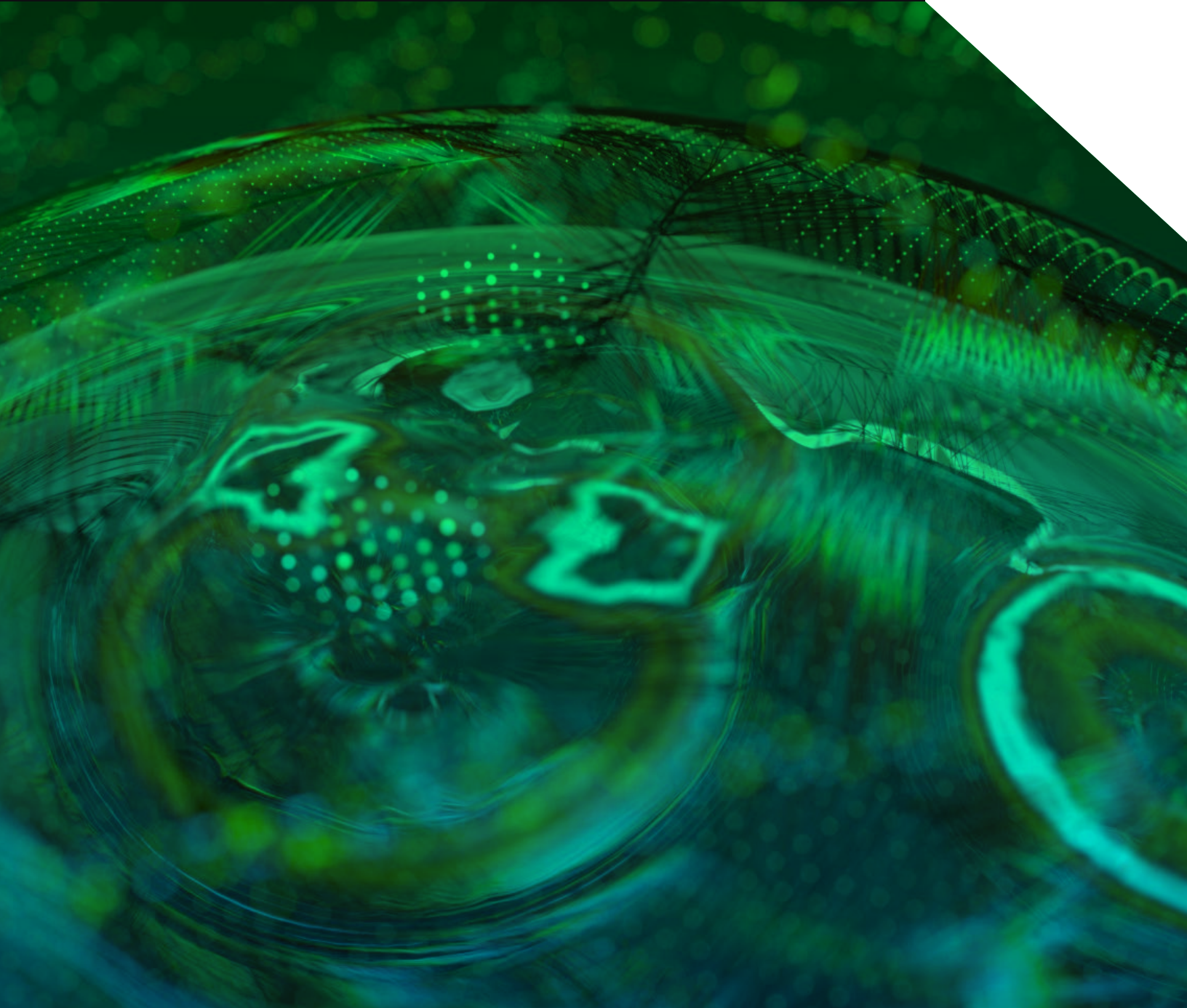



BlackBerry Cylance and SafeBreach

SOLUTION BRIEF





With BlackBerry Cylance and SafeBreach, customers can improve their overall security posture.

Introduction

BlackBerry Cylance and SafeBreach provide advanced cybersecurity solutions that customers can test in their own environment. Many companies claim their security products use artificial intelligence (AI) but offer few details on how it benefits their customers. With BlackBerry Cylance and SafeBreach, customers can identify security gaps, prioritize and get guidance on security configuration changes based on potential business impact, and improve their overall security posture.

Value Statement

Witness how BlackBerry Cylance is preventing security breaches and protecting environments on a step-by-step basis, through SafeBreach safe simulations. Using the industry's largest playbook of breach methods, *The SafeBreach Hacker's Playbook*, SafeBreach enables customers to safely run thousands of controlled forms of cyber attacks, visualize an attack path, and see the countermeasures BlackBerry® Cylance® products use to halt cyber threats at each phase. This joint solution automatically correlates and reports data in real-time, revealing the overall state of customers' security posture and its current impact on their business. It also offers the ability to prioritize remediation activities based on the business risk.

Use Cases

Measure Effectiveness of Controls

- **Challenge:** Threat response teams use multiple security products without knowing the precise effectiveness of each tool. This makes creating optimal threat remediation processes unnecessarily challenging.
- **Solution:** BlackBerry Cylance’s prevention-first methodology can be validated by security teams using SafeBreach automatic and continuous simulations.
- **Additional Benefit:** Customers can reduce threat risk, improve security posture, and quantify the effectiveness of prevention tactics to business leadership.

Continuous Security Validation

- **Challenge:** The security of an organization is under constant threat from both internal and external agents. Continuously monitoring against environmental drift and mapping the current state of the attack surface is difficult, if not impossible, without automation.
- **Solution:** Customers can prevent attacks before they execute with BlackBerry Cylance tools while preventing security misconfigurations with SafeBreach. BlackBerry Cylance’s endpoint detection and response (EDR) solution provides intelligence that can drive automated response playbooks.

- **Additional Benefits:** Security analysts will better understand the functionality of their cybersecurity tools, leading to more effective remediation and threat response actions.

Easily Demonstrate ROI To Management

- **Challenge:** BlackBerry Cylance delivers AI-driven predictive threat prevention, advanced threat hunting, and automated remediation capabilities. Security teams see the positive impact of a prevention-first security posture immediately, but how will they demonstrate the ROI to management?
- **Solution:** SafeBreach allows analysts to observe how AI-driven threat prevention performs on a step-by-step basis. By understanding how BlackBerry Cylance products respond to each step of the cyber kill-chain, analysts can better describe security ROI to business leadership.
- **Additional Benefit:** By watching how the joint solution responds to each phase of a cyber attack, analysts may discover and remediate new vulnerabilities or misconfigurations.

The screenshot below shows a SafeBreach Hoplight malware host level simulation result. The simulation was blocked and SafeBreach detected a preventive action based on events generated by CylancePROTECT®.

#2287 Write ELECTRICFISH malware to disk

Prevented

Simulation Result: Blocked
Detected Action: Prevent

Summary
Attack Phase: Host Level
Attack Type: Malware Drop
Target OS: Windows
Target: Win10-Cylance

Simulation Info
Last Change (UTC): 09/09/2019 11:18:21
Simulation Time (UTC): 09/09/2019 11:18:21
Simulation Id: 5305341

Add Label

Simulation Flow | Parameters | Classifications | **Security Events (1)**

Search

Generated: 11/05/2019 09:57:06 UTC | Copy | Refresh

Event Time	Action	Log Source Controller	Source	Destination	Port
09/09/2019 11:18:15	Quarantined	CylanceProtectAPI	172.31.28.121	172.31.28.121	

```
{"name": "bdata.bin", "sha256": "A1260FD3E9221D18C5B9ECE6E7A5A98669C79E124453F2AC58625085759ED388", "file_status": "Quarantined", "file_path": "C:\\Windows\\Temp\\sb-sfm-temp-pc1atk\\sb_5305341_bs_a1jykk\\bdata.bin", "cylance_score": -1, "classification": "Malware", "sub_classification": "Backdoor", "date_found": "2019-09-09T11:18:15"}
```

About SafeBreach

SafeBreach is a leader in breach and attack simulation. The company's groundbreaking patented platform provides a hacker's view of an enterprise's security posture to proactively predict attacks, validate security controls, and improve security operations center (SOC) analyst response. SafeBreach automatically executes thousands of breach methods from its extensive and growing Hacker's Playbook™ of research and real-world investigative data. Headquartered in Sunnyvale, California, the company is funded by Sequoia Capital, Deutsche Telekom Capital Partners, DNX Ventures, Hewlett Packard Pathfinder, PayPal, and investor Shlomo Kramer. For more information, visit www.safebreach.com or follow us on Twitter [@SafeBreach](https://twitter.com/SafeBreach).



About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.



CYLANCE.

+1-844-CYLANCE

sales@cylance.com

www.cylance.com

