

Enterprise emails and landing pages (unformatted) for Cylance

PERSONA 2: Decision maker: Non-C-Suite/CISCO/VP, Sr. Director

PERSONA 2: Email #2

[Subjects]

Effective malware protection that doesn't drain resources? Yep.
Effective malware protection that makes (dollars and) sense
True endpoint protection that doesn't require daily scans. Finally.

[Headline]

How many IT folks does it take to screw in a legacy antivirus lightbulb?

[Subhed]

100. One to screw in the lightbulb. 99 to perform daily scans.

[Email content]

It's no joke. Legacy antivirus solutions place a tremendous strain on your IT staff, requiring at least two or three to tend to the tedious chore of updating antivirus signatures *each day*. Facing a barrage of data from security products distributed across their network, they find little time to address proactive threat management, leaving critical network resources vulnerable to attack.

Meanwhile, productivity wanes, a performance drag whose costs continually erode your bottom line.

There's a better way.

Cylance delivers true endpoint protection that works behind the scenes *without signatures and without daily scans*. Leveraging artificial intelligence-based machine learning, Cylance provides continuous protection at a fraction of the overall cost of legacy AV solutions:

- AI-based solution reduces the number of false alerts.
- No signatures, updates or deep scans required.
- Protection against known and unknown malware, including fillets attacks

The result?

A job that previously required two or three full-time employees now requires the attention of just one (and part-time at that), a productivity boost that looks good on any bottom-line. **That's cost-effective protection.** Can you afford anything less?

To learn more, [CTA].

Enterprise emails and landing pages (unformatted) for Cylance

PERSONA 2: Email #3

[Subjects]

Effective malware protection costing you too much time?
Got time? True endpoint protection that's easy to manage.
Malware prevention that doesn't drain productivity? You bet.

[Headline]

Antivirus solutions leaving you S-T-R-E-T-C-H-E-D too thin?

[Email content]

Malware attacks are relentless, wreaking havoc on systems worldwide. As a result, your IT professionals are overtaxed, continually scrambling to update signatures with little time to attend to enterprise demands.

You can hire more IT folks, sure, but at what cost? At some point, you're merely putting your finger in the proverbial dike, a relentless onslaught of lost time, lost money, lost patience, and let's face it—lost customers. All to delay what seems to be inevitable: BREACH.

There's a better way. A simplified yet truly effective and efficient endpoint security system whose defining attributes are what it **doesn't** require:

No signatures to manage. **No updating**. **No Internet** connection. **No daily deep scans** to bog down system performance. **No team of IT folks**.

No kidding.

Incorporating artificial intelligence-based machine learning, Cylance offers true endpoint protection that prevents both known and unknown **malware**[not sure what the compliance messaging suggestion, if any, should be (from Gia's message map). Compliance with regs?]. And it's all done without signatures, without an Internet connection, and without the need for time-intensive updates nor deep scans.

The result?

Increased productivity. Decreased disruptions. Increased customer satisfaction.

To learn more about how Cylance provides powerful and cost-effective endpoint detection that's easy to manage, **[CTA]**.

Enterprise emails and landing pages (unformatted) for Cylance

PERSONA 3: Evaluator: Sr Director/Director, Sr. Mgr.

PERSONA 3: Landing Page:

[headline and subhed]

The Simple Solution to Complex Security Concerns

Cylance offers simple deployment, maintenance and management.

[body]

Malware attacks are relentless and increasing in frequency, and it's little wonder why: They easily evade legacy antivirus solutions.

The need to adopt more secure technology is paramount, but the migration costs seem overwhelming—or are they?

Cylance solutions are the quick and easy way to deploy effective endpoint protection without draining resources or burdening your existing IT staff. The key? An artificial intelligence-based approach that is smarter, faster and more effective than legacy AV.

But don't take our word for it. A recent study by [xxxxx](#) concluded that Cylance [xxxxx](#). [\[More detail here.\]](#)

To learn more about how Cylance can help you combat today's evolving threat environment, download [\[call to action here\]](#).

PERSONA 3: Email #1

[Subjects]

Trouble keeping up with the onslaught of malware attacks?
Enhance malware protection without adding complexity? Yep.

[Headline]

It's a jungle out there

[Email content]

Ransomware and fileless malware attacks are on the rise, while zero day victims suffer millions in losses. You've spent millions on detection, a "cross-your-fingers" approach that is simply wishing away a zero-day attack.

You know you need better protection—after all, one breach and your company's reputation will suffer, dragging with it customer loyalties, along with Board room support.

With so much invested in your system, the thought of starting over is unthinkable. Yet to do nothing is to delay the inevitable: BREACH.

Enterprise emails and landing pages (unformatted) for Cylance

There's a better way. A simplified yet truly effective and efficient endpoint security system that integrates seamlessly with your existing solution while offering enhanced protection.

Incorporating artificial intelligence-based machine learning, Cylance offers true endpoint protection that prevents both known and unknown malware—even fileless attacks. And it's all done without signatures, without an Internet connection, and without the need for time-intensive updates nor deep scans.

The result?

Simple deployment. Simple maintenance. Simple management. All while enhancing endpoint security.

To learn more about how Cylance provides powerful and cost-effective endpoint detection that's easy to manage, [CTA].

PERSONA 3: Email #2

[Subjects]

How do you know when a security alert is signaling a real breach?

[Headline]

[Email content]

You don't. And therein lies the problem with legacy AV solutions: **false positives**.

You can't simply ignore them. Doing so risks negligence in the face of real compromise, a do-nothing approach that threatens your company's reputation as well as customer loyalties.

So you monitor. And investigate. And monitor. And investigate.

An already taxed IT staff becomes even busier, leaving them little time to address proactive threat management, which by itself leaves critical network resources vulnerable to attack.

There's a better way.

Leveraging artificial intelligence-based machine learning, Cylance delivers true endpoint protection without generating false positives[Can you help here — I'm not sure how Cylance's approach reduces or eliminates the false positives. A stat or something else would work well here to amplify the message.]. The result?

Your IT staff can attend to genuine risk incidents, a critical allocation of resources that maximizes the security of your organization.

To learn more, [call to action/link to landing page].

Enterprise emails and landing pages (unformatted) for Cylance

PERSONA 3: Email #3

[Subjects]

You need global enterprise endpoint protection — but at what cost?
Cost effective, global, enterprise endpoint protection? Yep.

[Headline]

Wherever you are, we've got you covered

[Email content]

Migrating away from legacy antivirus solutions was an important first step in protecting your company's endpoints—remember, the goal is prevention, not simply detection—but hardly the only consideration.

With a growing portfolio of business, your workforce is dispersing, migrating across borders and time zones as they interact with a swelling roster of stakeholders and third parties.

As a result, your security needs have grown more complex, requiring comprehensive, seamless protection that stretches globally. All while accommodating your stateside budget.

And for that, there's Cylance.

Cylance delivers true endpoint protection that works behind the scenes *without signatures, daily scans or even an Internet connection*. Leveraging artificial intelligence-based machine learning, Cylance provides continuous protection for every endpoint in your system at a fraction of the cost of legacy AV solutions:

- AI-based solution reduces the number of false alerts.
- No signatures, updates or deep scans required.
- Protection against known and unknown malware, including fileless attacks

The result?

Cost effective, continuous protection of every endpoint, wherever they are. All in a solution that's easy to deploy, easy to maintain and easy to manage.

Wherever you are, Cylance has got you covered.

To learn more, [CTA].

Enterprise emails and landing pages (unformatted) for Cylance

PERSONA 4: Influencer: Compliance, architect, SE, etc.

PERSONA 4: Landing Page

[headline and subhed]

Endpoint Security That Eliminates Roadblocks

Cylance solutions align with existing corporate goals while scaling to future needs

[body]

Fighting malware is a paramount corporate concern, but its functionality must extend beyond mere protection.

There are myriad corporate concerns—compliance, growth and [concern 3]—and a security solution must align with each and scale appropriately to optimize performance across the enterprise, especially as these concerns evolve.

Cylance leverages artificial intelligence to provide effective endpoint protection while integrating seamlessly with existing infrastructures.

As internal and external factors change, Cylance's smart approach adapts, too. All without compromising performance or efficiencies.

Now more than ever, your security solution needs to do more with less. To learn more about what's at stake, [call to action here].

PERSONA 4: Email #1

[Subjects]

Endpoints overwhelmed but underperforming?

Enhance your existing endpoints without draining resources.

[Headline]

Layered defense? More like *delayed* defense.

[Email content]

Legacy antivirus solutions, in an effort to keep pace with continually evolving malware threats, require continuous signature updates and daily deep scans (none of which protect against a zero day attack, by the way).

The process ends up adding layers of piecemeal security patches to endpoints, which collectively bog down system productivity. Disruptions increase. Customer satisfaction decreases. And your bottom line suffers.

Enterprise emails and landing pages (unformatted) for Cylance

There's a better way. A simplified yet truly effective and efficient endpoint security system that integrates seamlessly with your existing solution:

Cylance.

Incorporating artificial intelligence-based machine learning, Cylance offers true endpoint protection that prevents both known and unknown malware. And it's all done without signatures, without an Internet connection, and without the need for time-intensive updates nor deep scans.

The result?

True endpoint security without draining resources or disrupting system availability.

To learn more, [CTA].

PERSONA 4: Email #2

[Subjects]

Enhancing endpoint protection requires seamless security product integration
Another AV solution? Sure it's compatible?

[Headline]

Is your AV solution a good fit?

[Email content]

Replacing your legacy antivirus solution is an important first step in protecting your company's endpoints—remember, the goal is prevention, not simply detection—but hardly the only consideration.

With so much invested in your existing security infrastructure, anything touching the endpoints must offer seamless “upstream” integration. Otherwise, performance will wane, along with productivity. And let's not even talk about ROI.

There's a better way. A simplified yet truly effective and efficient endpoint security system that integrates seamlessly with your upstream security products:

Cylance.

Incorporating artificial intelligence-based machine learning, Cylance offers true endpoint protection that prevents both known and unknown malware. And it's all done while offering seamless interoperability among existing security products, including SIEM vendors and other network security products.

Enhanced endpoint protection. Seamless integration with existing security products. That's Cylance.

Enterprise emails and landing pages (unformatted) for Cylance

The perfect fit.

To learn more, [CTA].

PERSONA 4: Email #3

[Subjects]

Enhanced endpoint protection that accommodates evolving compliance standards.

Another AV solution? Sure it's compliant? Even tomorrow?

[Headline]

By the book

[Email content]

Evolving compliance standards make choosing a security solution fraught with future-ready challenges.

Consider the work required in complying with general data protection regulations (GDPR). And that's just 2018. What about next year? And the year after that?

No matter your security solution, you need to ensure that it adheres to current compliance standards while standing ready to comply with those adopted in the future. Otherwise, your security investment is compromised, while your company's liability exposure is magnified.

Cylance can help.

Incorporating artificial intelligence-based machine learning, Cylance offers true endpoint protection that prevents both known and unknown malware. And it's all done in a future-ready solution that accommodates evolving compliance standards, preserving the value of your investment.[Can we offer a line or two about why it is considered future-ready? I need some background information to expand this paragraph.]

Enhanced endpoint protection. Strict adherence to today's compliance standards. Future-ready, to accommodate those of tomorrow. That's Cylance.

The right choice.

To learn more, [CTA].

.

SECURITY SUMMIT 2020

Landing page examples

In-depth security topics.
Industry-leading speakers.
Informative sessions.

All in one place.

Security Summit 2020

Experience the Security Summit 2020 from wherever you are, whenever you want. Hear how organizations ensure business continuity, employee productivity and employee safety during COVID-19. See the latest AI/ML and Zero Trust/Zero Touch innovations that secure and manage endpoints. Learn how enterprises improve operational effectiveness with the latest managed services offerings. And watch keynotes from BlackBerry Executive Chairman & CEO John Chen, President Tom Eacobacci and CTO Charles Eagan.

Sessions come from locations around the world, but you won't need to leave your seat. Everything is available on-demand.

ACCESS NOW

Get In Touch

Market Leading Platform for Enabling IoT

BlackBerry provides organizations with software to secure the IoT devices they use, the products they make, the data they share and their communications.



Endpoint
Management



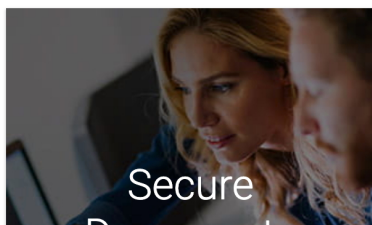
Endpoint
Security



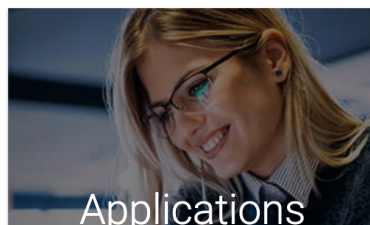
Secure
Communications



Alerts & Crisis
Communications



Secure
Documents



Applications

Get a Demo

See the next generation in endpoint security solutions – and take that first step towards getting your organization to a state of prevention. A BlackBerry expert will provide a demonstration of our solutions, and answer any questions you may have. Please complete the form below to request your demo.

By clicking Submit, I agree to the use of my personal data according to the [BlackBerry Privacy Notice](#). BlackBerry will not sell, trade, lease, or rent your personal data to outside parties. I understand the personal data I provide may be transferred outside of my country of residence to fulfill my request.

- ☐ Yes, I would like to receive communications about BlackBerry products, services and events. By selecting this box I agree to BlackBerry processing my personal data in order to keep me informed through such communications. I understand BlackBerry may also use my registration information to build a profile of my interests to help create a more personalized experience for me. View the [BlackBerry Privacy Policy](#) for details, or [unsubscribe](#) at any time.



I'm not a robot



Submit