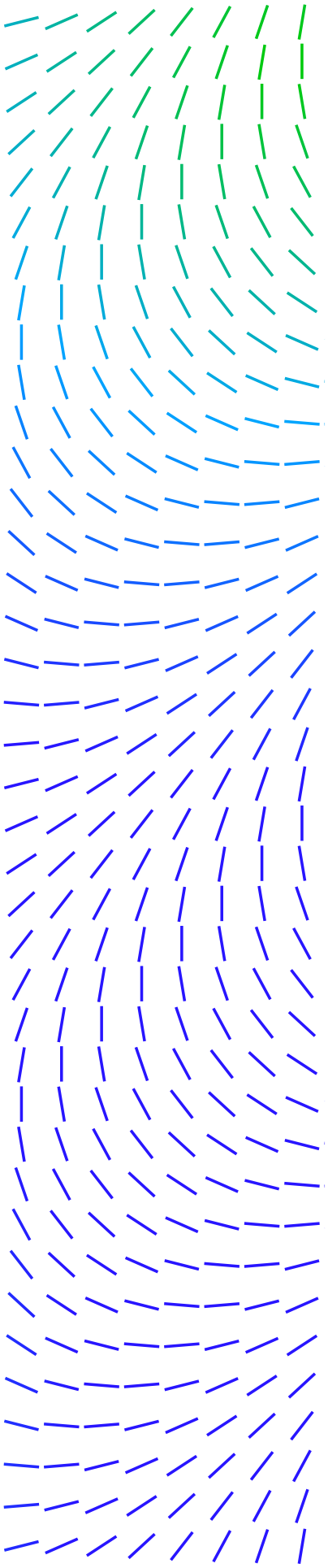


WHITE PAPER

Taking control of security operations

3 ways an intelligent, integrated approach can help streamline SecOps

Trellix

Executive summary

> 75% of large organizations will be actively pursuing a security vendor consolidation strategy by 2025.[1]

The threat landscape is constantly evolving—and the tools you used to protect your business yesterday certainly won't keep you safe tomorrow.

Static and siloed tools can only do so much to secure your company. Organizations like yours need a fresh approach. A new way to bring all your security products together to create a single united front.

With an intelligent, integrated approach to security operations, you can:

1. **Improve your visibility**
   Seeing more clearly enables you to not only detect threats but predict attacks.
2. **Accelerate your response**
   Integrating your products and adding intelligence empowers you to defend against attacks and respond to threats in real time.
3. **Increase efficiency and cost savings**
   Streamlining your security defenses and increasing your proactive readiness enhances your ability to strengthen your security posture and boost your bottom line.

The time to act is now—and the answer to increasing the efficiency of your security operations is simple: **product integration and intelligence**.

1. Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy? Gartner, 2020

A brand-new era in security operations

In today's dynamic world, new threats appear almost daily.

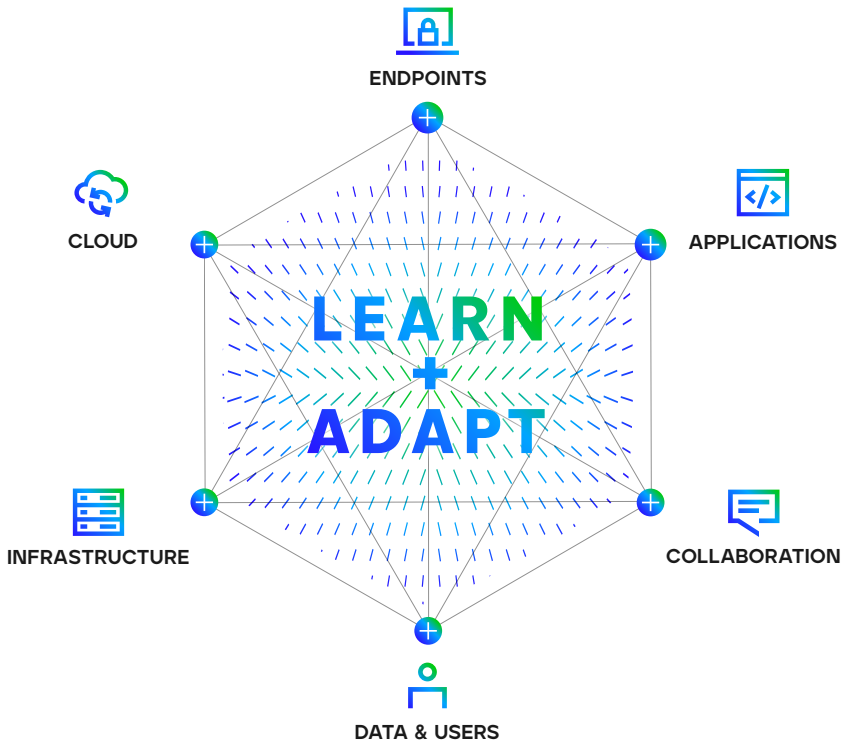
To stay one step ahead, many companies are investing in their future by improving their security posture.

Of course, increasing security is no easy task. It often comes with a need for substantial financial resources, an increase in human capital, added complexity, more manual processes, and—worst of all—a rise in risk if the new security measures are incorrectly implemented.

Fortunately, a new, more holistic approach has arrived.

With an integrated approach to cybersecurity, your business is better equipped to predict and prevent attacks. But bringing your security products together in a single solution is about more than just protection. It's about unlocking efficiencies.

In this white paper, you'll learn three ways an intelligent, integrated approach can streamline your security operations.



1. Improve your visibility

> 45% of security alerts end up being false positives.[2]

Seeing is securing. Blind spots in infrastructure can lead to major issues. Poor visibility can create an inability to detect threats. It can prevent you from gaining a better understanding about alerts. It can keep you from accurately assessing the impacts of attacks.

As the cyberthreat landscape evolves, new visibility gaps can emerge—in vendor connection points, subsidiary organizations, and more.

The burgeoning use of cloud also introduces vulnerabilities. Companies that use cloud to run critical business applications and store confidential data run the risk of information mismanagement or even data breaches.

An intelligent, integrated approach to security can help improve your visibility, giving you the power to:

Quickly identify that a breach has occurred

In a world where every minute of a breach can potentially cost thousands of dollars, it's vital to get to the bottom of your breach as rapidly as possible. Improved product integration offers you quick detection capabilities, so you can recognize threats, measure risk exposure, and use that information to prevent attacks—in minutes, not days.

Make sense of your alert volume

Bad alerts aren't just noisy—they're expensive. Organizations can waste numerous hours of employees' time investigating inaccurate or inconsequential alerts. With the right integrated ecosystem, you can automatically validate alerts and eliminate false positives, saving your company precious time and money.

Understand and anticipate attacker behavior

Staying ahead of attackers is a constant concern—especially considering how quickly bad actors can morph and conceal their identities. The embedded intelligence you get with a smart, integrated security solution enables you to recognize threats you've never seen before. It also uses sophisticated analytics to model future attacker behavior. Through AI and machine learning, you can prioritize threats, isolate them, and choose the right remediation tactics.

Increase your readiness before the attack

You'll never entirely eliminate the threat of bad actors. But there is a simple way to defend against them—by always being prepared. By keeping your finger on the pulse of global cybersecurity trends and emerging threats, you're better equipped to deal with attacks that come your way. And with tactics, defensive playbooks, and recommended countermeasures built right into your integrated ecosystem, you'll have all the expert guidance you need to prevent attacks.

2. The Voice of the Analysts, IDC, 2021

> 287 days is the average time it takes to identify and contain a data breach.[3]

2. Accelerate your response

Every time you turn around, there's another major cyberattack in the news. We've reached a boiling point—one where even people who don't work in the security space know that responding to an incident is just as important as protecting against it.

To respond and safeguard against incidents, companies must make a well-functioning workflow a top priority. The most efficient and effective process consists of high-quality alerts, an orderly work queue, accurate analysis, and seamless case management.

Security product consolidation—combined with AI and machine learning—can help accelerate your response and equip you with the added ability to:

Integrate all the pieces of your security operations

A speedy response is typically a function of how quickly security teams can make sense of alerts. If alerts come from multiple sources without context or correlation, the log source has virtually no value. Consolidating log sources can improve your response time, and you can more easily overlay them with threat intelligence and analytics to surface new threats fast.

Enrich your response with intelligence

Intelligence is a key component of any mature security operations capability. But what good is it if it can't be applied directly to your operational environment? If you can't easily use your intelligence to defend your organization, it's useless. When your security products are integrated in a single smart solution, you get access to contextual, relevant intelligence that's specifically applicable to each breach and readily available to help your teams better investigate incidents.

Provide case management

Detecting and investigating an attack involves numerous team members and tasks. Unfortunately, traditional project management and communication tools often lack the qualities needed to coordinate these activities for security teams. A unified approach to SecOps makes it easier to equip your teams with simple tools to assign and track tasks, manage the work queue, and facilitate knowledge sharing for quick resolution.

Increase employee efficiency

As threats evolve, organizations are racing to fill cybersecurity jobs, with demand far outpacing supply. On top of short-staffed security teams, too many organizations rely on insufficient point products and siloed tools—ones that lead to inefficient, error-prone manual processes. With an intelligent, holistic security platform, your business can automate repetitive, time-consuming tasks, enabling your staff to be more engaged and efficient.

3. Cost of a Data Breach, IBM, 2021

3. Increase efficiency and cost savings

> Nearly 2/3 of survey respondents estimate saving more than $25,000 annually by having a single XDR vendor.[4]

What's the security of your business worth to you? That's a vital question to ask anytime you're considering a new security approach. Protecting your most valuable assets is of the utmost importance. And you need to know precisely what you're willing to spend to keep your company safe.

Oftentimes, organizations like to compare the price of products against one another—even if they're vastly different. But when it comes to total cost of ownership, businesses must think more broadly and strategically. It isn't enough to just consider financial costs. Companies must weigh the operational and impact costs, too.

An intelligent, integrated approach to SecOps can help:

Streamline financial costs

Hardware and software. Subscriptions and upgrades. Deployment and maintenance. The prices of these things may seem straightforward enough, but they often come with hidden costs—from overlap with existing solutions to a lack of integration with point products. Bringing together a broad portfolio of endpoint, cloud, and other security products in a single solution enables you to cut costs.

Minimize impact costs

Cybersecurity is risky business. An organization that's unable to protect itself from attacks increases its exposure to risk and loss. Loss in productivity. Loss in reputation. And more. Integrating your security operations offers you the chance to stay safe and rise above the risk. With increased visibility and control, you can minimize disruptions in your operations and reduce the likelihood of an event that negatively impacts the opinion of your customers.

Control operational costs

Time is money. Every minute you spend hiring top talent, training staff, or supporting ongoing security operations—it all adds up. The right unified platform can help keep operational expenses down in a number of ways. It offers broader capabilities, so you can reduce the time you spend training employees to use multiple tools. It automates workflows, so staff can focus more on impactful activities rather than menial tasks. And it equips team members with the right tasks for their skill levels, so you can keep employee churn to a minimum.

4. Future of Extended Detection and Response (XDR), Cisco, 2021

WHITE PAPER

Presenting the next evolution in SecOps

As a business, you should always strive to grow smarter. Stronger. More agile.

One surefire way to do that is by bringing all your security products together in a single intelligent solution. Only then can you truly bring your security to life.

With the right integrated platform, you can harness the power of artificial intelligence, machine learning, and automation to unlock insights and streamline workflows. This gives your organization the ability to not only increase employee efficiencies but constantly learn and adapt to new and evolving threats.

An integrated ecosystem also benefits your business by offering a more unified approach to protection—integrating both native and open tools, so you can configure your security setup to meet your customized needs.

And by firmly embedding a smart, holistic platform into your operations, you can reap the rewards of having security in your DNA. Real-time detection, response, and remediation are all second nature to you now.

Want to learn more about bringing your products together and bringing your security to life? Visit trellix.com today.

Trellix
6000 Headquarters Drive
Plano, TX 75024
www.trellix.com

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.

032023-14