

THE ART OF CYBERSECURITY



THROUGH THE EYES OF THE SECURITY MANAGER

TABLE OF CONTENTS

Embrace the Art of Cybersecurity to deliver more beautiful business outcomes	3
Out-manuever your flood of alerts	4
Rise above the skills shortage	6
Keep everyone fully in the picture	7
Deliver beautiful outcomes	8
Trend Micro has made cybersecurity an art form	9

EMBRACE THE ART OF CYBERSECURITY TO DELIVER MORE BEAUTIFUL BUSINESS OUTCOMES

How will you break free of your overwhelming workload and become part of valuable strategic security outcomes to your organization?

Every day you face spiraling numbers of increasingly sophisticated threats, security incidents, outages - and a relentless stream of alerts. There's constant stress over the time it takes to resolve them, and you're almost always under-staffed and forced to use disconnected tools. Business units are creating extra hassle by building systems without telling you. And your organization is full of people whose risky behavior suggests they're determined to become victims of cybercrime.

There's a constant nagging anxiety over whether you've actually already been hacked, and not yet discovered the breach. And your biggest fear is that the next alert will be something new and ruinously expensive.

You need time to educate users on best-practice behavior and compliance. You need more time to prepare management and compliance reports. And you need yet more time to be more strategic about your job instead of daily firefighting.

Indeed, you know you could achieve far more for your organization, if only you had a bit of breathing space. You could strengthen defenses, increase automation and improve resilience. Implement safer organizational processes to give everyone a common purpose. And improve visibility to ensure breaches are identified and acted on immediately.

Keeping business operations running, whatever the cybersecurity challenge, would enable you to build trust with your customers and suppliers. Business transformation initiatives would become far easier. Additionally, your whole organization could become more productive and competitive.

Delivering these strategically valuable outcomes is the Art of Cybersecurity, and achieving them can be much easier than you might think.



OUT-MANEUVER YOUR FLOOD OF ALERTS

Keeping up with security alerts is consistently raised as the number one challenge for IT security teams. With this reality, it's no surprise that alert fatigue is a major ongoing complaint.

Yes, there are other worries too: the constant stress of false positives and negatives; having to use legacy systems to solve modern problems; making do with security tools that are poorly integrated, and the huge amount of time spent on manual reporting. But the biggest problem, overall, is the volume of security alerts, and it's getting worse all the time.

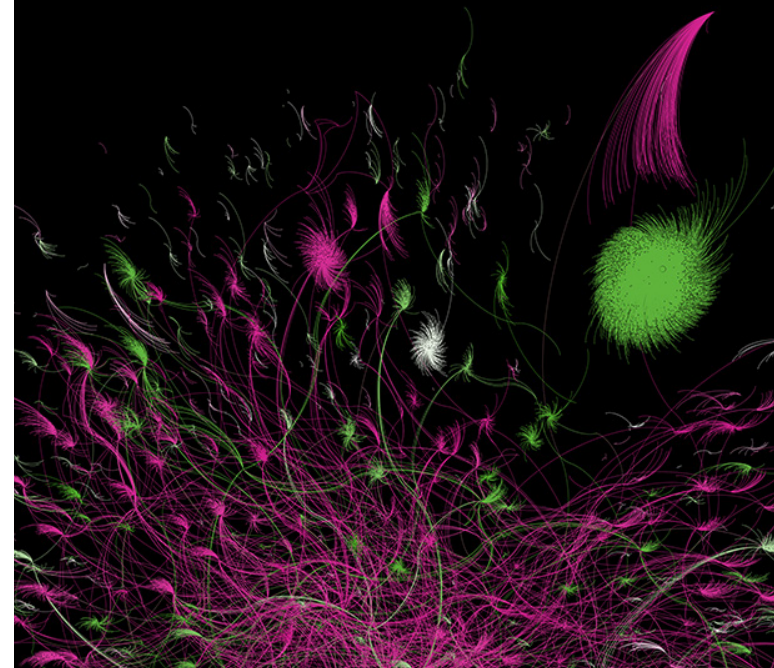
There are three reasons. Security technologies have become far better at identifying a wider and more up-to-date range of risks in recent times. Also, the number of tools has risen, with almost two-thirds of enterprises currently using at least 25 cybersecurity products¹. Finally, many solutions simply don't clearly differentiate between trivial and critical issues.

Enormous amounts of time are then typically wasted in performing a multitude of tedious, manual tasks to assess and validate the alerts. This often results in alerts either not being picked up, or those with more damaging consequences being overlooked and slipping through the net.

Indeed, a telling feature of some of the most high-profile data breaches is that security alerts were simply being ignored in the run-up to their taking place.

"Day-to-day alerts account for the vast majority of our time - it's constant. Five years ago, many of these incidents weren't recognized by security tools, so we weren't in a position to respond to them. It used to be set and forget. But now the security tools pick up so much more and, combined with the fact that there are more of them, it means it's an always-on task."

¹ 'Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms', Enterprise Strategy Group (ESG), October 2018



Your security team must have access to a wide range of threat defense techniques optimized for each of the environments you're protecting. You need a single platform that integrates and summarizes all the alerts as they happen across environments. And you need a single view of your overall security environment, so you can manage and monitor your operations, and also prioritize your incident responses more effectively.

Moreover, advances in artificial intelligence and data science are making it possible to automatically differentiate real threats from false alarms far more accurately. You can now detect patterns of behavior that depart from the norm - even subtle variations that might be difficult to describe in a rule - and narrow down anomalous events to a much smaller number of potential likely threats.

It's no surprise then that the use of automation combined with machine learning and other forms of human-augmented artificial intelligence are on the rise in cybersecurity. The enhanced ability to discern relevant issues across the entire threat landscape will give your security team sharper focus and the ability to respond to incidents faster.

Yet, it's also more than intelligence alone. You need a tool set that works across your multiple layers of security - tying together and making sense of seemingly unrelated events - to not only detect and respond to issues, but also enable rapid protection against newly discovered threats. That's what can enable a resilient business.

"We're constantly being reactive, not having the freedom to work in a more proactive, forward-thinking way."

SECURITY MANAGER WORKING IN THE PUBLIC SECTOR

RISE ABOVE THE SKILLS SHORTAGE

Maintaining a team big enough to cope with today's ever-increasing workloads and rapidly-evolving security threats is a major, ongoing challenge.

According to a recent ESG and ISSA study², the cybersecurity skills shortage worsened for the third year in a row in 2018, impacting nearly three-quarters (74%) of organizations. And that trend is set to continue.

These shortages are increasing risk and holding back productivity. Almost all (93%) of the study respondents believe that keeping their skills up to date is essential to maintain security, but 66% said it was hard to do that with current workloads. Two-thirds (66%) reported that their employees are already overworked; 47% reported an inability to learn about or use security technologies in the most effective way, and 40% reported limited time to work with business units.

Finding skilled and experienced people who are well versed in both security and the latest business technologies is therefore a critical objective. Yet, the market has become so competitive that it's difficult to find and retain the security talent you need on your teams.

Also, there is a strong trend for the best people to coalesce around the most challenging environments, such as dedicated centers of excellence for security. The opportunity for people to work alongside other highly-skilled security professionals, where they can learn and develop their skills from each other, appears to be a strong incentive in recruitment.

There is no easy solution to this problem specifically. So perhaps an alternative approach, of working on ways to reduce the overall workload of your security operations team, would be more effective. Adopting the right technologies across every layer, including human-augmented artificial intelligence and automation, is essential. And taking a balanced, strategic approach to the entire security lifecycle - protection, detection and response - can give your security team members some breathing space.

² 'The Life and Times of Cybersecurity Professionals 2018', Enterprise Strategy Group (ESG) and Information Systems Security Association (ISSA), 2019



KEEP EVERYONE FULLY IN THE PICTURE

The actions of your colleagues are a major, ever-present and relentless challenge to your organization's cybersecurity. Even if your policies are completely secure, nobody is infallible, people take shortcuts, and anyone can be duped.

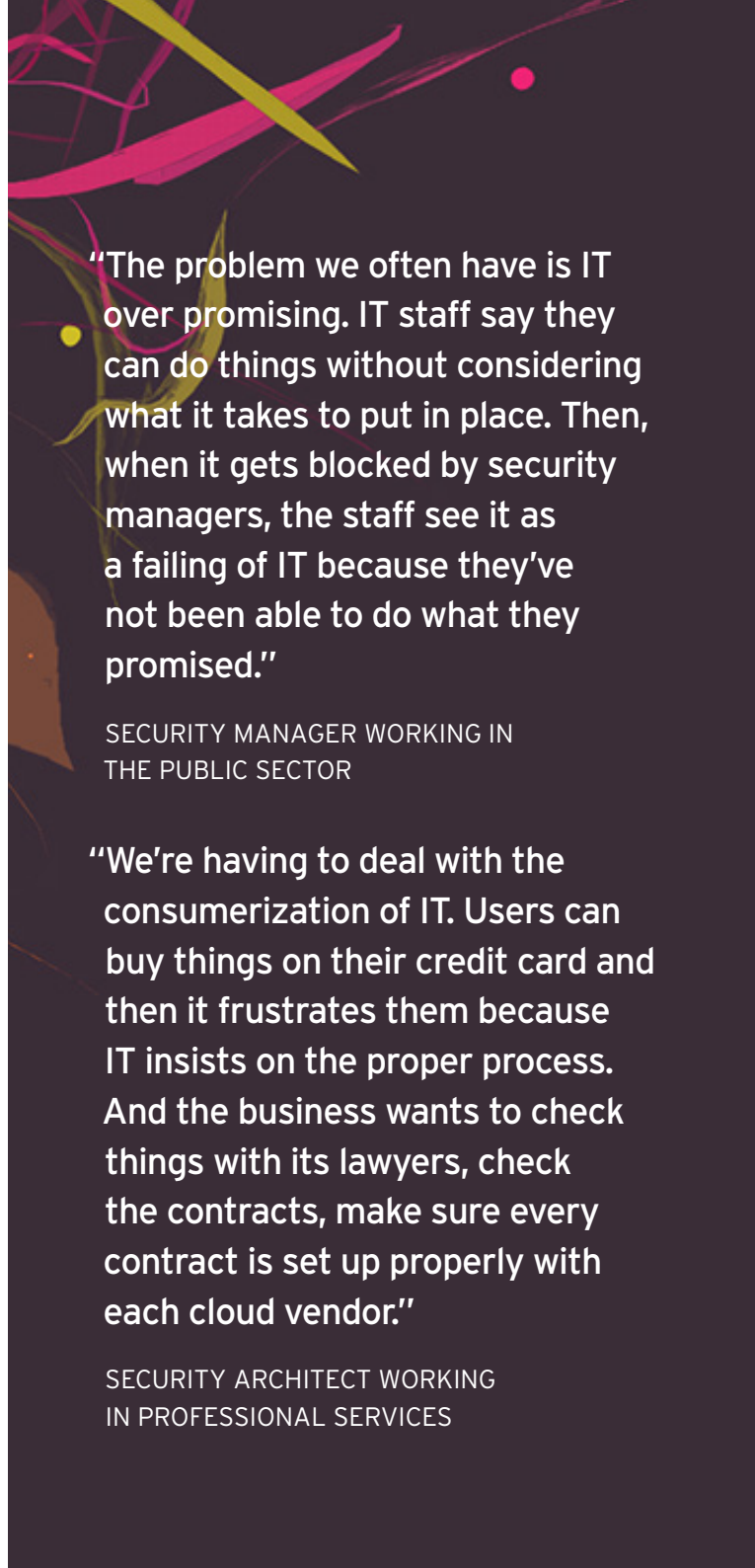
So your security procedures have to be created with people in mind. You have to provide flexible options that enable users to stay secure yet still work flexibly and autonomously. Above all, you need to keep your colleagues on-side, so that they are open about their actions and intentions. You can't protect what you don't know about, so it's essential that people choose to involve you in their projects from the start.

A key success factor is communication. Despite high-profile cases like WannaCry, there remains a lack of cybersecurity awareness across business. If end users don't know the risks and don't follow your policies, it's more likely they'll be caught out.

Engaging with line-of-business managers to understand each others' roles, objectives and challenges will enable you to help one another. Their success as business units is a critical factor in how your success will be measured.

You need to create clear, easy-to-follow processes on everything from connecting personal devices to the dos-and-don'ts of shadow IT. And providing regular awareness training to your colleagues will help create a sense of shared responsibility.

Ultimately, you need to safeguard your users' data across e-mail, web and SaaS applications regardless of device, application, network or location. You need to protect workloads and applications in the data center and across the multiple cloud providers you're using (AWS, Azure, Google). You need to ensure your networks are secure, able to not only deflect attacks, but also to understand when something does get through your defenses. And you need to do that with the maximum transparency, providing strong defenses seamlessly across multiple layers.



“The problem we often have is IT over promising. IT staff say they can do things without considering what it takes to put in place. Then, when it gets blocked by security managers, the staff see it as a failing of IT because they've not been able to do what they promised.”

SECURITY MANAGER WORKING IN
THE PUBLIC SECTOR

“We're having to deal with the consumerization of IT. Users can buy things on their credit card and then it frustrates them because IT insists on the proper process. And the business wants to check things with its lawyers, check the contracts, make sure every contract is set up properly with each cloud vendor.”

SECURITY ARCHITECT WORKING
IN PROFESSIONAL SERVICES

DELIVER BEAUTIFUL OUTCOMES

New technologies and more effective ways of working can help reduce your workload. That means you will have more freedom to think strategically and can play your part in delivering beautiful business outcomes.

With Trend Micro, you'll gain access to the key resources you need to make your business more resilient. You can...

- Dramatically reduce the number of security alerts to take the pressure off your team
- Respond faster to real security breaches while minimizing their impact
- Provide streamlined security and better support to your colleagues in different lines of business
- Become more strategic, deliver greater value to your business, and advance your career.

That means you can simplify the complexity of modern cybersecurity, which gives your business the beauty of...

- Trust - the most powerful currency in today's digital world, helping drive revenue and loyalty
- Transformation - so that growth initiatives can be safely executed with less fear of interruption
- Productivity - helping get more done each day, enabling consistent performance ahead of competitors.

Trend Micro's cybersecurity solutions will give you greater visibility and stronger protection of your organization, enabling you to work faster, smarter and more successfully.

“Trend is easy to use, integrates better and has better reporting. It saves us a lot of time, we don't have to feed and water it as much.”

SECURITY ARCHITECT WORKING IN PROFESSIONAL SERVICES

“By reducing the day-to-day fire-fighting, I have more time to work and think strategically, consulting on our five-year IT security plan, and working out which products and services I'll need over that time.”

SECURITY ARCHITECT WORKING
IN PROFESSIONAL SERVICES



TREND MICRO HAS MADE CYBERSECURITY AN ART FORM

Our X-Gen™ security strategy delivers a cross-generational blend of threat-defense techniques that give you the ability to apply the right technique at the right time. Everything's optimized for leading environments such as AWS, Azure and Google, as well as strategic applications like Office 365 and Dropbox. Our connected solutions - including the latest multi-layered detection and response capabilities - give you the very best protection for your organization.

Our foresight has been proven over three decades as we've successfully predicted and intercepted market-changing technology trends like virtualization and cloud. We've been able to proactively secure new environments that our customers can take full advantage of. And, along with our market-leading threat research, that means you get the solutions you need to continuously stay ahead.

Above all, however, we live and breathe cybersecurity at Trend Micro. Our passionate people are with you every step of the way, providing expertise, insights and creative thinking, so you can act with complete confidence.

You can protect every part of your technology footprint - your users, your network and your hybrid cloud - and bring clarity to the chaos of cybersecurity.

Because when you can prepare for, withstand, and rapidly recover from threats, you're free to go further and do more.

Discover how you can create beautiful outcomes by mastering the Art of Cybersecurity through;



Hybrid Cloud Security



Network Defense



User Protection

Talk to us today about how we can help you deliver beautiful outcomes at your organization - call us on +44 (0) 203 549 3300.

**THE ART OF
CYBERSECURITY**

