SE Labs
INTELLIGENCE-LED TESTING

Annual Report
2020

Contents

Document version 1.0 Written 30 September 2020

About
SE Labs

In our second annual report we review the unprecedented year of 2020, in which major security companies were bought and sold, hackers battered down the virtual doors of major companies and a biological virus brought the world to its knees.

We will explain who we work with, to try and improve everyone's security in this time of uncertainty. We'll also explore how security testing has improved (or not) over the last 12 months and suggest ways in which you can use us better to help you personally or your organisation.

WHO WE WORK WITH

We've always worked with the largest security organisations to try and help improve products and provide recognition when strong security is available. Since our last report we have extended our reach to work with those companies and organisations that actually create and operate the internet, collaborating with the likes of the Internet Engineering Task Force (IETF), Microsoft, Google and the UK's National Cyber Security Centre (NCSA).

Although our programmes of social responsibility have been impacted by the COVID-19 pandemic, we continue to support those who need access to computer equipment and now donate equipment to the Computer Aid charity. Its CEO Keith Sonnet said, "The computers and equipment SE Labs provides goes a long way to empowering the lives of individuals in the developing world. Without companies like SE Labs we would not be able to help bridge the digital divide and create long-term, measurable improvements in these lives of people who need it most."

OUR TESTING

Always accurate, transparent and based on real-world threat intelligence, our testing has continued to evolve, taking into account the way bad guys behave and providing results in ways that are most easily interpreted.

The Breach Response test now comes in two flavours: Protection and Detection modes, which is ideal if you want to find a product that keeps hackers out, or which tracks them when they break in.

Our Email Security Services Protection (ESSP) test has also been renewed, producing one of our most successful reports to date.

Throughout the development of all these tests we have been exploring the potential of machine learning (ML) for use in powering tests. In the latter part of this year we have been

using ML in a number of ways to make testing more relevant, consistent and accurate. Well, if the security vendors use it and the bad guys use it, probably testers should use ML too!

ARE TESTS TRUSTWORTHY?

How can you trust a security test? And why is it important to do so? If you are in charge of protecting an organisation, you need good data to help make buying decisions. The consequences of simply trusting internet reviews, vendor sales pitches and instinct are extremely serious. So which tests are the best?

There are lots of published tests available on the internet and we'd advise looking beyond the headline and the summary before deciding on which to trust. The best way to tell a good test from bad is to see how transparent it is and a shortcut to that is to check that it follows the Anti-Malware Testing Standards Organization's testing Standard. More of that in Testing Standards on page 8.

Our unique Email Security Services Protection test took the security world by storm.
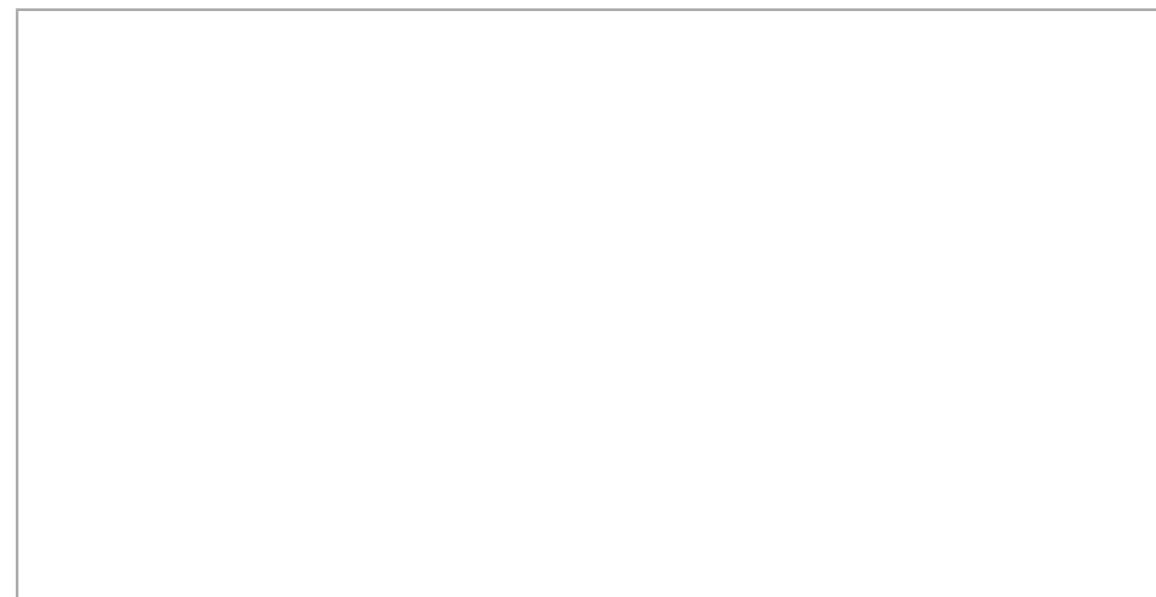
Our team works closely together to ensure only the most accurate and useful test results leave the lab.

WE'RE HERE TO HELP

Our role in 2020, and in all previous years, is to be a partner to you (the reader), the companies that create the security products you need and to the wider community of organisations that are trying to create a more secure internet and computing environment for businesses and consumers globally. We want to fix things, not just give out awards. And the feedback we've had from all of our clients is that we are refreshingly honest, produce in-depth but easy to understand work and have a direct impact on how security products are developed.
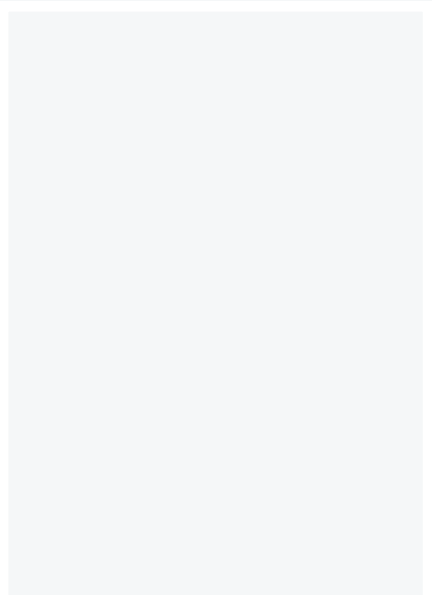
Our new website (also launched this year) is free of registration, provides access to reports that can be read online or downloaded for free, contains detailed information for security testing nerds and is a gateway to a portal of threat intelligence for close partners.

The Team

Management
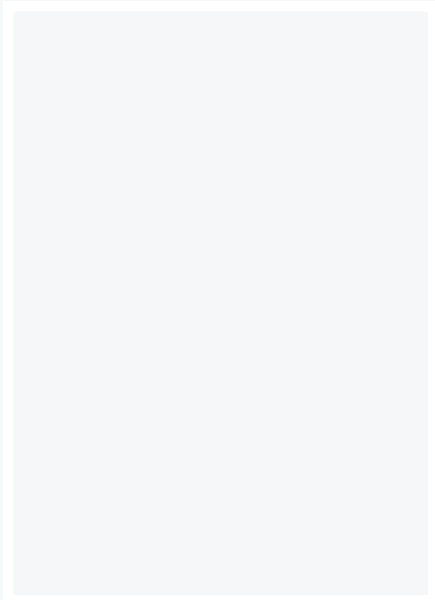
Simon Edwards
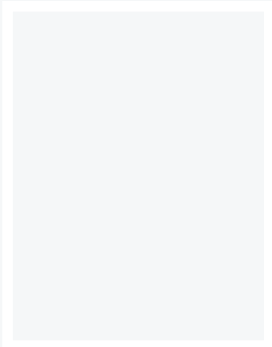Chief Executive Officer

Marc Briggs
Chief Operations Officer

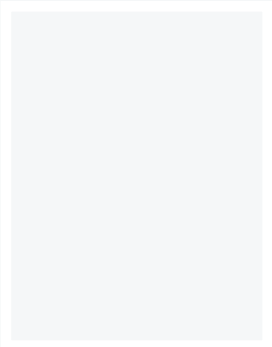Magdalena Jurenko
Chief Human Resources Officer
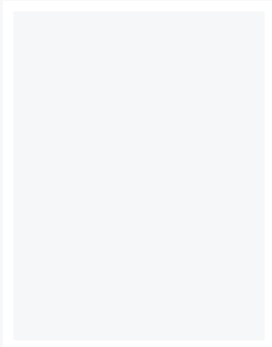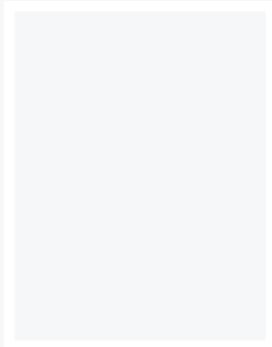
Stefan Dumitrascu
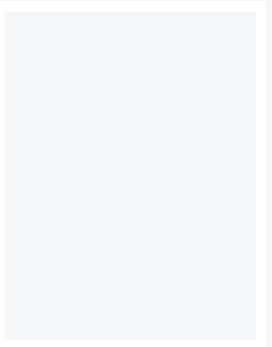Chief Technical Officer

Testing Team
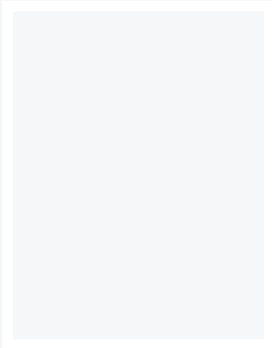
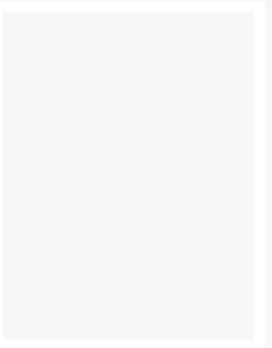Nikki Albesa
Tester

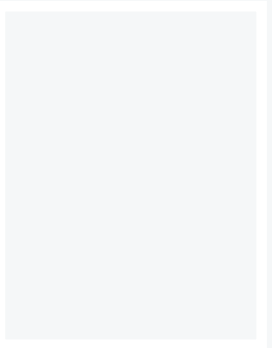Thomas Bean
Tester

Solandra Brewster
Tester

Liam Fisher
Tester

Gia Gorbold
Tester

Joseph Pike
Tester

Dave Togneri
Network Appliance
Testing Lead

Jake Warren
Tester
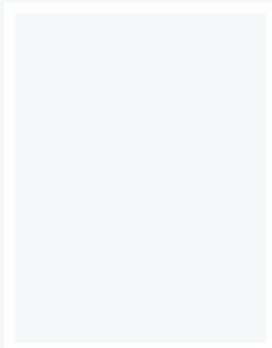
Zaynab Bawa
Development Ops
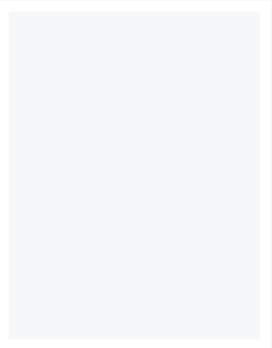
Stephen Withey
Development Ops

IT Support
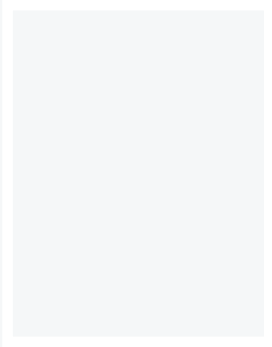
Danny King-Smith
IT Support Manager

Publication
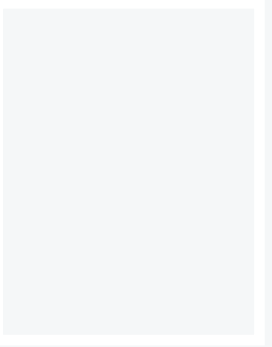
Sara Claridge
Marketing
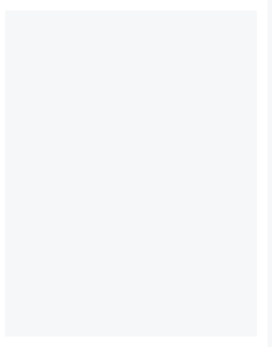
Colin Mackleworth
Design and Production

SE Labs

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Blog blog.selabs.uk
Phone +44 (0)203 875 5000

Post
SE Labs Ltd,
55A High Street,
Wimbledon,
SW19 5BA,
UK

SE Labs is ISO/IEC 27001 : 2013
certified and BS EN ISO 9001 : 2015
certified for the Provision of IT
Security Product Testing.

SE Labs is a member of the Microsoft
Virus Information Alliance (VIA);
the Anti-Malware Testing Standards
Organization (AMTSO); and the
Messaging, Malware and Mobile
Anti-Abuse Working Group (M3AAWG).

© 2020 SE Labs Ltd

Annual Awards Winners

After months of in-depth testing we are proud to announce this year's Annual Awards winners. Each of the following companies or products has demonstrated to SE Labs its excellence in its category. We've based our conclusions on a combination of continual public testing, private assessments and feedback from corporate clients who use SE Labs to help choose security products and services.

SE Labs INTELLIGENCE-LED TESTING
BEST New Endpoint
WINNER 2020
SentinelOne

SE Labs INTELLIGENCE-LED TESTING
BEST Innovator
WINNER 2020
Deep Instinct
D-Client
deepinstinct

SE Labs INTELLIGENCE-LED TESTING
BEST Enterprise Endpoint
WINNER 2020
Kaspersky
Endpoint Security
kaspersky

SE Labs INTELLIGENCE-LED TESTING
BEST Small Business Endpoint
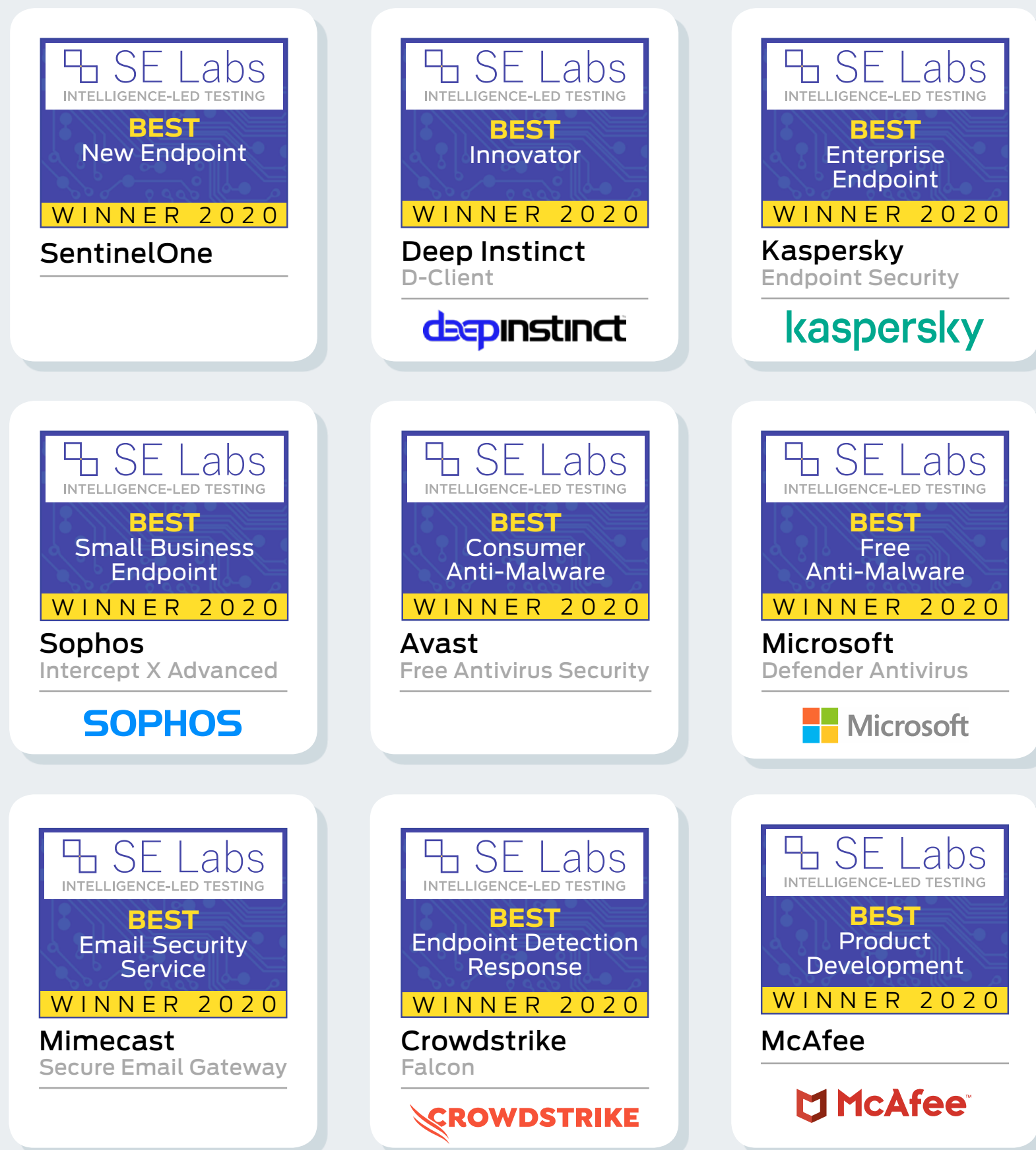**WINNER 2020**
Sophos
Intercept X Advanced
SOPHOS

SE Labs INTELLIGENCE-LED TESTING
BEST Consumer Anti-Malware
WINNER 2020
Avast
Free Antivirus Security

SE Labs INTELLIGENCE-LED TESTING
BEST Free Anti-Malware
WINNER 2020
Microsoft
Defender Antivirus
Microsoft

SE Labs INTELLIGENCE-LED TESTING
BEST Email Security Service
WINNER 2020
Mimecast
Secure Email Gateway

SE Labs INTELLIGENCE-LED TESTING
BEST Endpoint Detection Response
WINNER 2020
Crowdstrike
Falcon
CROWDSTRIKE

SE Labs INTELLIGENCE-LED TESTING
BEST Product Development
WINNER 2020
McAfee
McAfee

Our Tests

Many of SE Labs' test reports are available for free from our website. We test a wide range of software, hardware and cloud-based services. The following list provides a few examples of our areas of expertise. In most cases we use both attacks found in the wild along with targeted attacks created in the lab. These targeted attacks can represent similar attacks that have occurred against real victims or may be more theoretical (but likely future) attacks.

- Endpoint Security Software

- Network Security Appliances

- Email Security Services

- Web Security Gateway Services

- Content Disarm and Reconstruction

- Endpoint Detection and Response/Incident Response

- Artificial Intelligence/ Machine Learning

Testing Standards

Security testing organisations make judgments on products and services, but how do you know if the tester is competent?

Testing computer security products and services comes with its own unique challenges and it is hard to assess the assessments. The industry is not known for its transparency in product effectiveness, and that extends to some testing. SE Labs has always prided itself on its ethical behaviour in terms of testing and business practices. That behaviour extends to maximum amounts of transparency. Unfortunately, until recently, there was no official way in which to demonstrate that we do what we say and are prepared to prove it to both validate test results and to help improve products.

In mid-2018 the Anti-Malware Standards Organization approved and adopted the AMTSO Testing Protocol Standard. A test that complies to this Standard has demonstrated that the testing has been conducted fairly and transparently. The Standard means, say what you're going to do. Do it! Then be prepared to prove it.

SE Labs was the first testing lab to engage with the Standard, running private and public pilots, before complying with the official Standard immediately. No other testing organisation has engaged so thoroughly and successfully with the AMTSO Standard.

A reliable tester states in advance what it's going to do; follows its own rules; and then has the data to prove it has done what it said it would.
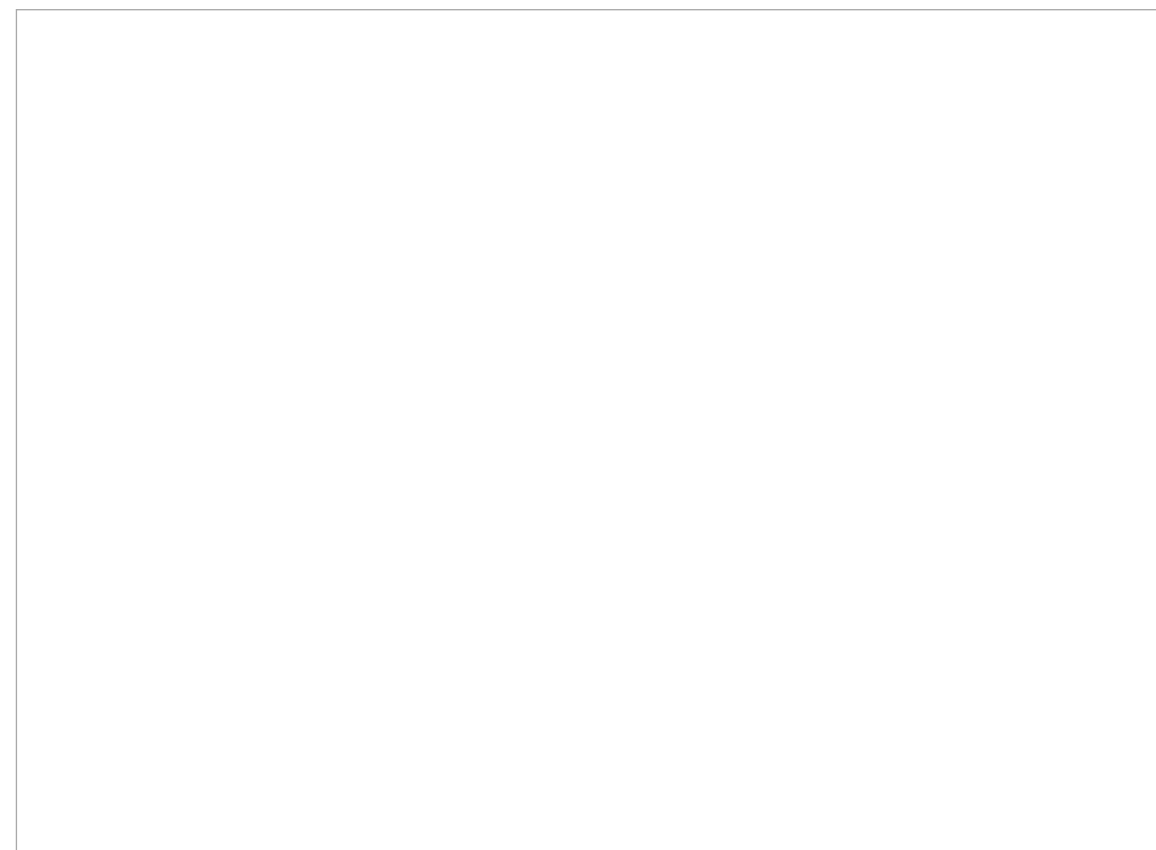
The Anti-Malware Testing Standards Organization supports transparency in testing, which encourages more accurate reports.

To date all of SE Labs' public endpoint testing has complied with the AMTSO Standard, since its inception in 2018. We are committed to following the Standard so that readers of our reports can be assured that we've tested the way we said we did and that the results were checked by third parties.

Additionally, SE labs complies with the ISO 9001 : 2015 Standard for Quality Management Systems, specifically relating to the Provision of IT Security Product Testing. We are also ISO/IEC 27001 : 2013 certified.
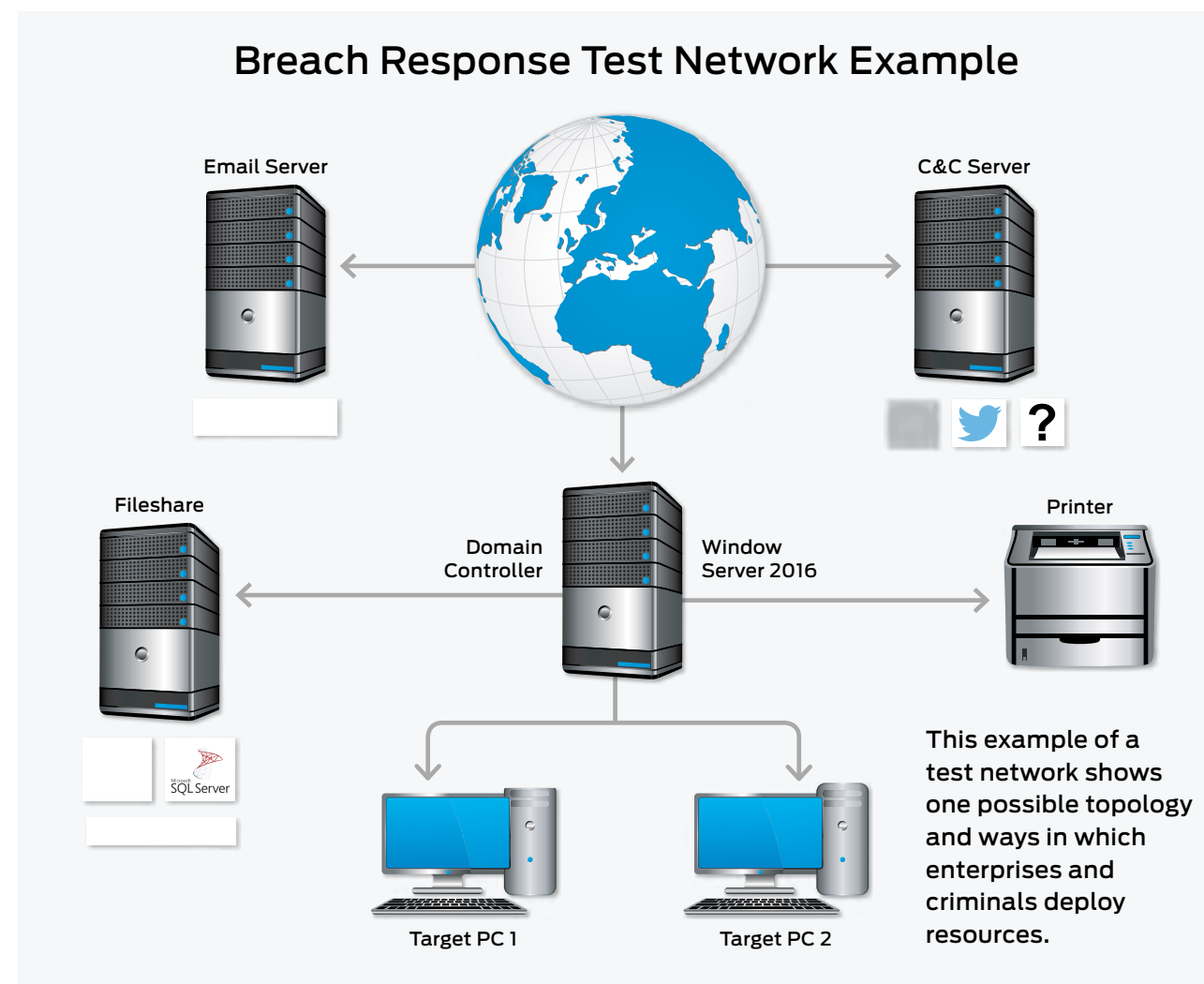
Testing Like Hackers

To test a security product properly, you have to behave like a real attacker. There are countless clever ways to simulate attacks, automate testing and so on, but at the end of the day nothing beats sitting down and manually hacking away at a target for realism, which is why we do it that way. That said, to ensure that testing keeps abreast of the latest developments, we have now started using machine learning to help power our tests. We believe this is a world first in security testing.

BREACH! BREACH! BREACH!

2020 was the year that our Breach Response (BR) test came of age. We'd always planned a full end-to-end hacking-based test, capable of testing any type of product, or combination of products. But this year we really cracked it, delivering advanced and evolved public and private testing services to security companies dedicated to producing the finest products.

We worked with The MITRE Corporation and others on how to score products in a way that is compatible with the MITRE ATT&CK framework so, if you're familiar with that system, you'll find it extremely easy to understand our BR test reports. Subsequently, it will also be simpler to assess which products you might choose to deploy.

We now produce two types of Breach Response test reports. The Protection mode reports look at how fully a product (or combination of products) can protect the target, while the Detection mode approach assesses how thoroughly a product can detect different elements of an attack. You can read about these reports on

Breach Response Test Network Example

This example of a test network shows one possible topology and ways in which enterprises and criminals deploy resources.

Hackers vs. Targets			
Attacker/APT Group	Method	Target	Details
APT3	📧 ‹›	🏛	Spear phishing emails containing scripts
APT29	📧 ‹›	🏛	Spear phishing emails containing scripts or links to malware
APT33	📄 ‹›	✈ 🏭	Documents containing scripts combined with public tools
APT34	📧 📄 ‹›	💲 🏛 🏭	Phishing with email and other services, combined with public tools

Key							
✈ Aviation	🏛 Banking and ATMs	🏭 Energy	💲 Financial	🃏 Gambling	🏛 Government Espionage	🛢 Natural Resources	🛒 US Retail, Restaurant and Hospitality

We describe the attacks and attackers emulated in our advanced tests.

COMPUTER VIRUSES ARE STILL A THING?

SE Labs is probably best known for its world-leading anti-malware testing, in the shape of our Endpoint Protection (EPP) test. In 2020 we tested more products than ever before and have welcomed some of the best-known products from the newer, so-called 'next-gen' companies like SentinelOne, FireEye and Crowdstrike. Our EPP reports are the best place to find such a wide variety of business and consumer products tested to such an in-depth degree.

THREATS COME THROUGH EMAIL. MOSTLY...

Our Email Security Services Protection (ESSP) test also reached new strengths, with more products tested, a wider range of attack types and clear descriptions about why you should care about those types of attack! Although it did compare services, such as those from Microsoft, Google and Mimecast, it also made it very clear that the real battle is between these services and the bad guys, rather than between themselves as competitors.

By highlighting the threats clearly, according to their specific threat actor groups (e.g. APT 33), the test data became alive for readers, who understand that these relevant threats evolve and don't just disappear. There is clearly room for improvement in this industry and the interest shown from the email vendors for future development of this test has been enormous. We expect to publish even larger ESSP reports in 2021.

THREATS MOBILISE

Finally, we are working on a new mobile security test that should produce some amazing results. We insist that all of our testing has to produce useful, meaningful data, which is why we have always resisted running anti-malware tests for Android and iOS

Email Security Services Protection Test Case Structure

Targeted

Commodity | Social | Phishing | Malware | Business Email Compromise | Legitimate

Categories

Example Scenarios
- Free Money to Transfer
- FBI Blackmail
- Emergency PayPal Request
- Lottery Win
- Fund Beneficiary
- Money Mule

Example Test Cases

1 — 10

Basic — Sophisticated

Basic examples might include plain text, poor spelling and grammar alongside obviously unsuitable email addresses (e.g. an FBI scam sent from a Gmail account). More advanced options can include message re-coding, more believable email addresses and malware equipped with anti-virus evasion abilities.

The threats used in the ESSP test vary in type and sophistication.

platforms – there isn't really much in the way of true malware in the wild. We have now identified a way to test any mobile product's abilities to protect its user(s) from significant threats that pose real-world issues.

Full Attack Chain Testing Every Layer of Protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack Chain Stages

01	02	03	04	05	06	07
An email containing a malicious attachment is sent to the target.	The attachment contains an exploit that is intended to provide remote access to the attacker.	The attacker tries to perform reconnaissance, such as listing files and checking the system's configuration.	The attacker needs more power and so tries to escalate privileges.	System-level access allows the attacker to attempt to dig deeper into the system, logging keystrokes and stealing passwords.	When enough information has been gathered the attacker attempts to steal or damage data on the system.	The attacker may attempt to connect to other systems on the network.

A realistic test contains all of the major stages of an attack.

How we Work

SE Labs works with a range of clients. Our main focus is on helping security vendors improve their products, and helping large companies make the best buying decisions when changing their IT security.

For both sets of clients we perform both private and public testing, and we'll go into detail about what that means here.

INCORPORATING OUR ANALYSIS

When considering a change in anti-malware, EDR or other security product, companies generally require private testing. Usually the company will engage with a few competing vendors that run 'proof of concept' (POC) tests to show their strengths in the hope of winning the contract. Even the largest of companies, with their own internal test labs, use SE Labs as a credible second opinion to these POC tests. Our reports are useful when making proposals for change to the Board.

With corporate engagements we produce detailed technical reports and executive-level presentations, engage in conference calls and even make in-person presentations from time to time. For corporate clients, SE Labs is the consultancy with the widest range of knowledge about what products are available, how they work and how well they work. We don't just have the figures – we do the analysis.

VENTURING FORWARD

This knowledge is also useful to potential investors in cyber security, which is why our Investor Intelligence Insights (i3) programme is in such demand. Working with venture capital and other types of investors, we can lift the lid on the technology behind the sometimes very dubious pitch claims.
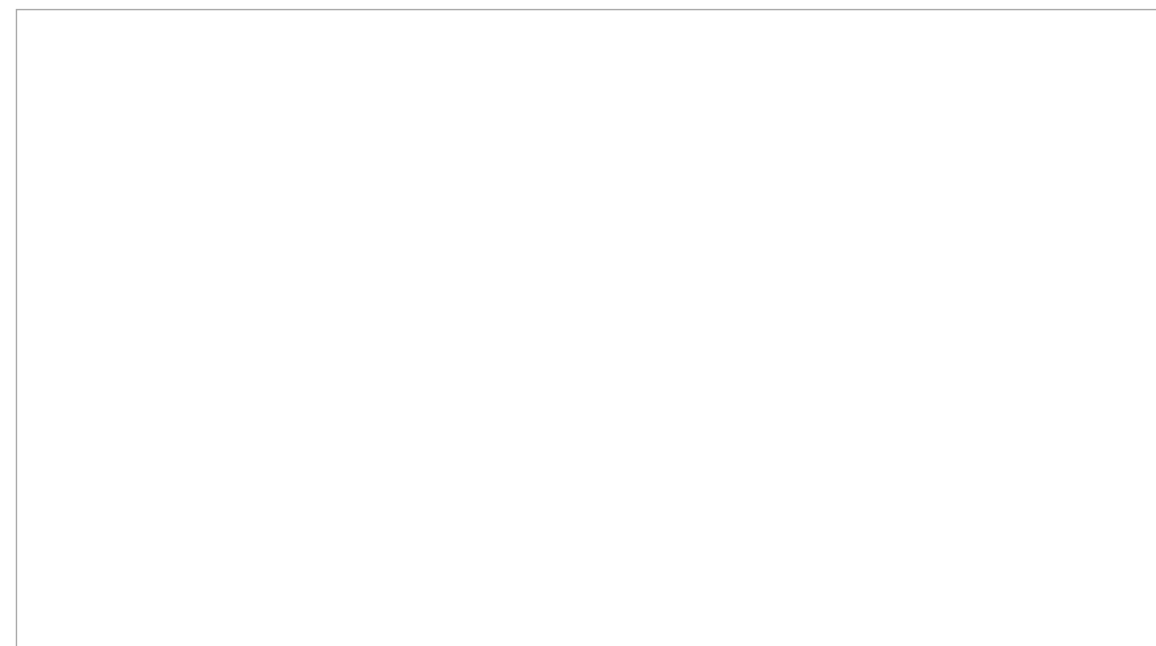
Even the largest of companies, with their own internal test labs, use SE Labs as a credible second opinion to these POC tests.

But there are some great, new products out there and our reports often help cyber security start-ups gain funding beyond the very initial stages.

GOING PUBLIC (WITH RESULTS)

Test reports can be published or kept private. Most security vendors start with private testing and move into public testing after a short period of orientation. We have some rules about what can and can't be public, though. When we test a range of products for a single report, for comparison purposes, each vendor must commit to having its results published before the test starts. This commitment is not required for standalone tests, in which one product is pitted against a suite of threats (such as in the Breach Response test). In some very specific situations, a private test may be made public. To see the detailed options see the flowchart on page 13.

Your Route Through Public and Private Testing

Our Endpoint Protection, Email Security Services Protection and Breach Response testing can be used for internal product development and public or private competitive comparisons

Endpoint Protection and Email Security Services Protection Testing

PUBLIC

Outcome

- Your report appears in a public comparative report.
- Product improvement.

Your Product
↓
EPP or ESSP Test
↓
Raw Data
↓
Comparative Public Report

- Your test is run alongside other products in the same test.
- Awards and comparative ranking between products are published in the report.
- There is no option to keep your results private once this test has started.

PRIVATE

Outcome

- Prepare your product for public comparative testing.
- Product improvement.
- Public standalone report, if requested.

Your Product
↓
EPP or ESSP Test
↓
Raw Data
↓
Standalone Report*

- Your product is tested against threats only - no comparisons to other products are made.
- At the end of testing you have the option to publish the results in a standalone report (at an additional cost).
- This test could be compared to the public report when run at the same time and against the same threats.

* Extra cost

Breach Response Testing

PRIVATE

Outcome

- Product improvement.
- Public standalone report, if requested.

Your Product
↓
Breach Response Test
↓
Raw Data
↓
Standalone Report*

- Your product is tested against threats only.
- At the end of testing you have the option to keep the results private or for us to create and publish a report (at no extra cost).

* If requested

A Word from Simon

Last year we produced the first fully featured test for 'anti-hacker' products. Businesses that buy these products, and even the security companies that make them, loved it for the depth of detail and the fairness of the scoring system. This year we made it even greater.

Our Breach Response test essentially involves hacking targets that are monitored by one or more security products. It doesn't matter if the product is a box on the network, a cloud service or some software running on a Windows PC – or is made up of a combination of those things. If it can be deployed in the real world we can test it realistically.

Built to be compatible with the popular ATT&CK framework from MITRE, the Breach Response test uses the same tactics as real attackers the world over. Not only that, but we report results in a similar way to MITRE's own tests and provide plenty of threat intelligence to help report readers understand what's really going on – and where the strengths and weaknesses lie.

Some clients want an Endpoint Detection and Response (EDR) product to spot hacking attempts and provide useful information about them, similar to a CCTV system but on a computer network. For these people, we have the Breach Response test running in Detection mode. The results are provided in a similar way to MITRE's and you can see how a product can handle different parts of an attack. For example, one might be great at noticing malware executing, but not spot the hacker moving into other parts of the network. Other products might focus more on this lateral movement or other suspicious behaviour and be less concerned with specific scripts and executable files.

Of course, if a product can detect a threat you might also want it to protect against it! Increasingly we're seeing demand for the Breach Response test in Protection mode, which measures how well a product can protect against threats.

In all cases we explain about the attacks, and who we are emulating (as far as it's possible to attribute attacks to attackers...) We use multiple APTs in each report and create variations of each of them, producing results that indicate very clearly how well you might expect a product to perform in the real world against real attackers who won't give up on their first failed attempt to breach a network.

We do the same in our brand new Email Security Services Protection (ESSP) test, in which we run real attacks through email services as if we were real customers/ targets. The reports explain the tactics of the attackers and the types of industries that they target. We can look at how the products combat the attacks – batting them away, putting them in quarantine or removing malicious content. Or not, as the case often is! We're expecting a lot of improvement in the email security space next year.

WHO DO WE WORK WITH?

The Breach Response and other tests that we run benefit lots of people. The readers of the public and free reports gain a previously unprecedented insight into how well these expensive products work. However, the companies that make the products are also able to use our expertise to identify issues that they can fix and make their products stronger. And, if they have a great product, we can give them the recognition they deserve with an award.

But we don't just help those who make security products or browse our site for the free reports. We also provide guidance directly to those who buy security products, specifically Global 500 companies for which changing an anti-virus or hacker hunting solution is a decision worth millions of any major global currency. We also talk to well-known analysts to help build and support their opinions with real-world lab data.

TRYING TO BE TRENDY
We're often asked about the latest trends in the threat landscape. The boring answer is that it's business as usual, much of the time. We see new approaches appear every so often, such as the increasing use of scripts. It's hard to tell the difference between a user running a Powershell script for good and one with an evil intent, for example. So hackers can behave much like administrators to hide their actions. Similarly, malicious Macros, Master Boot Record infectors and application exploits come and go, and come back again.

It should be of no surprise to anyone that mobile attacks are increasing but you may be surprised to learn that they do not fully replicate the way that we've seen attacks via personal computers. Social engineering is far more prevalent because of the inherently better technical security built into mobile platforms. When you're busy and on the run, a phishing SMS is far more likely to trick you than a poorly formatted email or attached PDF that doesn't show properly on your smartphone.

With this is mind, we have finally decided to test mobile security. For years we've been asked to test Android and iOS anti-malware products and we've consistently refused because we don't see the threat level being at all significant, in direct contrast to the dozens of companies willing to sell or give away products that claim to solve this virtually non-existent problem.

Combining our approach of detailed manual testing and analysis with, for the very first time, machine learning, SE Labs is now testing mobile security against the kinds of threats that affect real people in the real world, and not theoretical problems or using annoying adware software often wrongly described as 'malware' or 'viruses'.

TALK TO US
This year we upgraded our website and paid more attention to social media. We have never been more accessible to you. Please follow us on Twitter for technical news and link up with us on LinkedIn for business insights. Do you wish we had an email list, or paid more attention to Facebook or Instagram? Let us know. We're only one email away (info@selabs.uk).

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an "AS IS" basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.