SE Labs

INTELLIGENCE-LED TESTING

Annual Report 2021

GIGABYTE hit by RansomEXX
Only 13% cybercrime solved in two years
Cybercrime
Ransomware Attacks
of Ransomware
attack exploited Kaseya'
++ But why WERE warnings ignored?
DON'T BE HELD TO RANSOM
Crippling bug could be lurking in your inbox
CYBER HACKERS CRIPPLE THE NHS
No pedestrian access
rtment (A&E)
English hospitals divert ambulances 'ransomware' cyber attack
FBI warns ransomware assault threatens US healthcare system
Federal agencies say cybercriminals are unleashing a major ransomware
s dilemma
inst malwar
The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) linked roughly $5.2 billion worth of Bitcoin transactions to ransomware.
World > Americas
'Petya' cyber attack spreads to US pharma giant Merck after ransomware infects Ukrainian national bank
Spain's government said ye of companies, including telec Telefonica, had been attacked
Ransomware threat to UK
UK rail network
Crime syndicate
medical
Hackers

Contents

Document version 1.0 Written 17th November 2021

About SE Labs

The third SE Labs annual report charts the successes and failures of security companies, their customers and the criminals who keep relentless pressure on us all. Working from home is at its highest level in human history, which emphasises the need to secure all devices, everywhere.

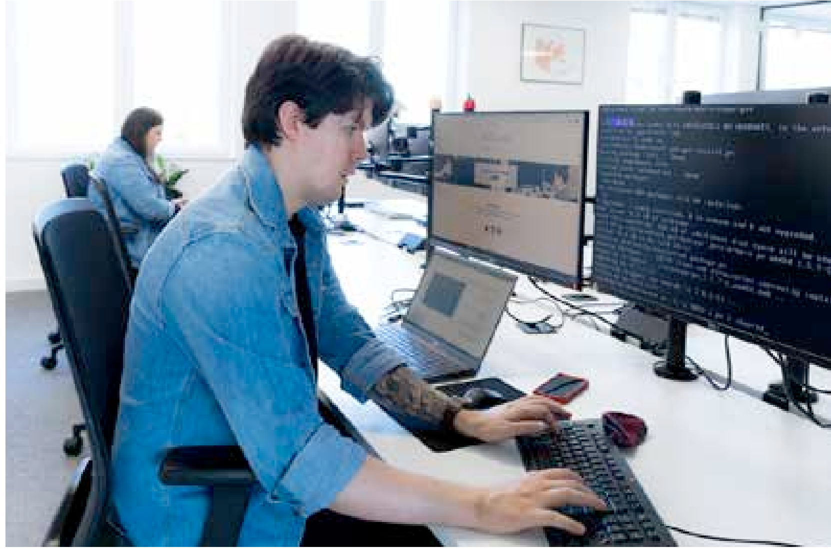
Not every company works the same way, though. And not every security product is suitable for all use cases. There are also many ways to use an individual product, which makes life interesting for customers and challenging for testers. How can you test an enterprise anti-malware product in a way that's directly relevant for all potential customers? We'll go over some of these challenges and see what useful testing can look like, and what to look out for in a bad test.

Six years of testing

After six solid years of testing endpoint protection, we've produced a review that examines some of the trends and data points we've identified. How did your favourite anti-virus behave over the last few years? Did any of the products face significant problems in that time? Are all products as good (or bad) as each other? We've dug into the data and produced a **two-page special review** on page 15.

We've expanded well beyond endpoint testing over the last 12 months and our Advanced Security tests cover next-generation firewalls, network detection and response products as well as the sort of Endpoint Detection and Response products we've been testing for some time. Of note this year was the publication of BlackBerry's results. This is the first official test of what used to be called CylancePROTECT. We've now published test results for all the major EDR products, including those from the 'next-gen' vendors.

The Advanced Email Security test continues in leaps and bounds and a public test is due early next year. Our annual conference focussed on email testing this year, with all major vendors joining us to discuss testing challenges and solutions.



Open, honest and useful

Since its inception, SE Labs has focussed on realistic and honest testing. One way we stay relevant and accurate is to rely on our highly skilled testers. We don't automate our tests: everything is done by a person, which means we can adjust to follow the behaviour of the criminals quickly.

We also pride ourselves on transparency, publishing everything we can think of to help people understand and trust our reports. As you'll see on page 9, we've launched a new initiative to bring even more value to security tests. The Security Testing DataBase provides low-level information on how tests are run by the best-known testers; how you can run your own tests; and configurations to help replicate systems for testing or even in real deployments.

We continue to follow the AMTSO testing Standard, which requires that we say what we're going to do, that we actually do it and are then prepared to be able to prove it. We encourage all testers to do the same.

Get involved

If we're guilty of one thing, it's in being too quiet about what we do and how we do it. Since the last annual report we've made significant changes to make ourselves more available to you. We now run an excellent monthly newsletter and our blog contains timely articles about current threats, testing news and the latest reports. The biggest change has been the launch of our very successful and award-winning podcast, DE:CODED. The first series is complete and available to download in full, from all the major platforms including Apple Podcasts, Spotify and YouTube. Series 2 is in production, scheduled for 'broadcast' in March 2022.

We strongly advise signing up to the newsletter, which is the primary way we communicate. We don't spam and we don't use your personal information for anything other than sending you the newsletter emails. We're largely ignoring Facebook because of its historical abuse of personal privacy, but if you like Twitter or LinkedIn you'll find regular updates from us there too.

Finally, in an effort to improve the personal security of our readers we bought and gave away 100 USB security keys and some very stylish SE Labs keyrings, worth $50 each. Find out if we'll do that again by (you guessed it) subscribing to our free newsletter!

The Team

Management

Simon Edwards
Chief Executive Officer

Marc Briggs
Chief Operations Officer

Magdalena Jurenko
Chief Human Resources Officer

Stefan Dumitrascu
Chief Technical Officer

SE Labs

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
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 NetSecOPEN.

Testing Team

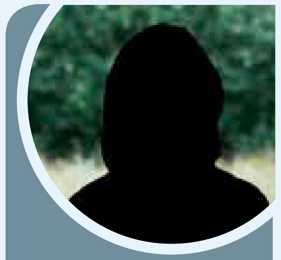
Nikki Albesa
Tester

Thomas Bean
Tester

Solandra Brewster
Tester

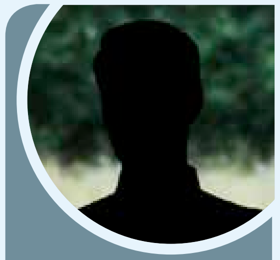
Rory Brown
Tester

Liam Fisher
Tester


Gia Gorbold
Tester

Erica Marotta
Tester

Jeremiah Morgan
Tester


Julian Owusu-Abrokwa
Tester

Joseph Pike
Tester

Testing Team

Dave Togneri
Network Appliance Testing Lead

Dimitrios Tsarouchas
Tester

Stephen Withey
Development Ops

Liangyi Zhen
Tester

Publication

Sara Claridge
Marketing

Colin Mackleworth
Design and Production

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
Next Generation Firewall
WINNER 2021

CISCO

SE Labs
INTELLIGENCE-LED TESTING
BEST
Enterprise Endpoint
WINNER 2021

Sophos

SE Labs
INTELLIGENCE-LED TESTING
BEST
New Endpoint
WINNER 2021

BlackBerry

SE Labs
INTELLIGENCE-LED TESTING
BEST
Endpoint Detection & Response
WINNER 2021

CrowdStrike

SE Labs
INTELLIGENCE-LED TESTING
BEST
Email Security Service
WINNER 2021

Barracuda

SE Labs
INTELLIGENCE-LED TESTING
BEST
Innovator
WINNER 2021

SentinelOne

SE Labs
INTELLIGENCE-LED TESTING
BEST
Product Development
WINNER 2021

FireEye

SE Labs
INTELLIGENCE-LED TESTING
BEST
Network Detection & Response
WINNER 2021

VMware

SE Labs
INTELLIGENCE-LED TESTING
BEST
Small Business Endpoint
WINNER 2021

Kaspersky

SE Labs
INTELLIGENCE-LED TESTING
BEST
Consumer Anti-Malware
WINNER 2021

NortonLifeLock

SE Labs
INTELLIGENCE-LED TESTING
BEST
Free Anti-Malware
WINNER 2021

Microsoft

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.

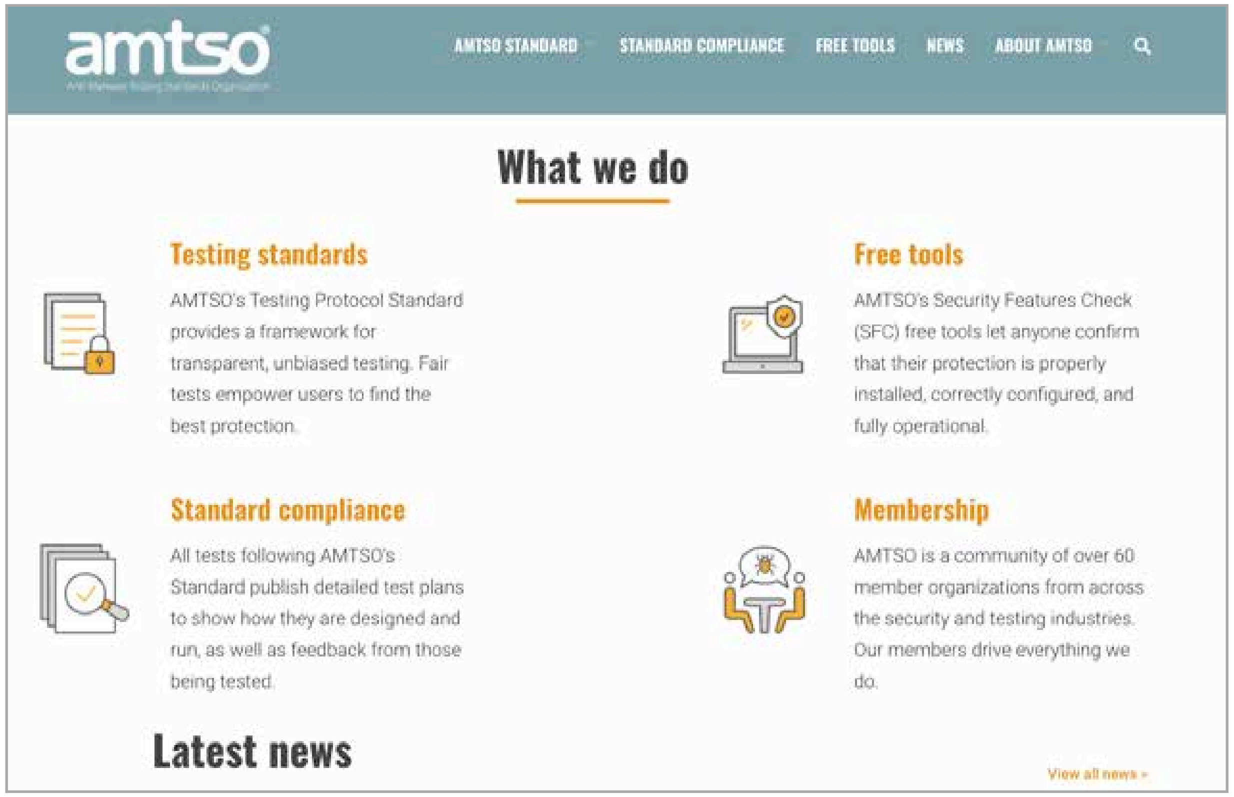
- Endpoint Security Software
- Network Security Appliances
- Email Security Services
- Web Security Gateway Services
- Content Disarm and Reconstruction
- Endpoint Detection and Response/Incident Response
- Artificial Intelligence/ Machine Learning

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.

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.



What we do

Testing standards

AMTSO's Testing Protocol Standard provides a framework for transparent, unbiased testing. Fair tests empower users to find the best protection.

Free tools

AMTSO's Security Features Check (SFC) free tools let anyone confirm that their protection is properly installed, correctly configured, and fully operational.

Standard compliance

All tests following AMTSO's Standard publish detailed test plans to show how they are designed and run, as well as feedback from those being tested.

Membership

AMTSO is a community of over 60 member organizations from across the security and testing industries. Our members drive everything we do.

Latest news

View all news »

The Anti-Malware Testing Standards Organization supports transparency in testing, which encourages more accurate reports.

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.

Say it! | **Do it!** | **Prove it!**

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.

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.

The Security Testing DataBase

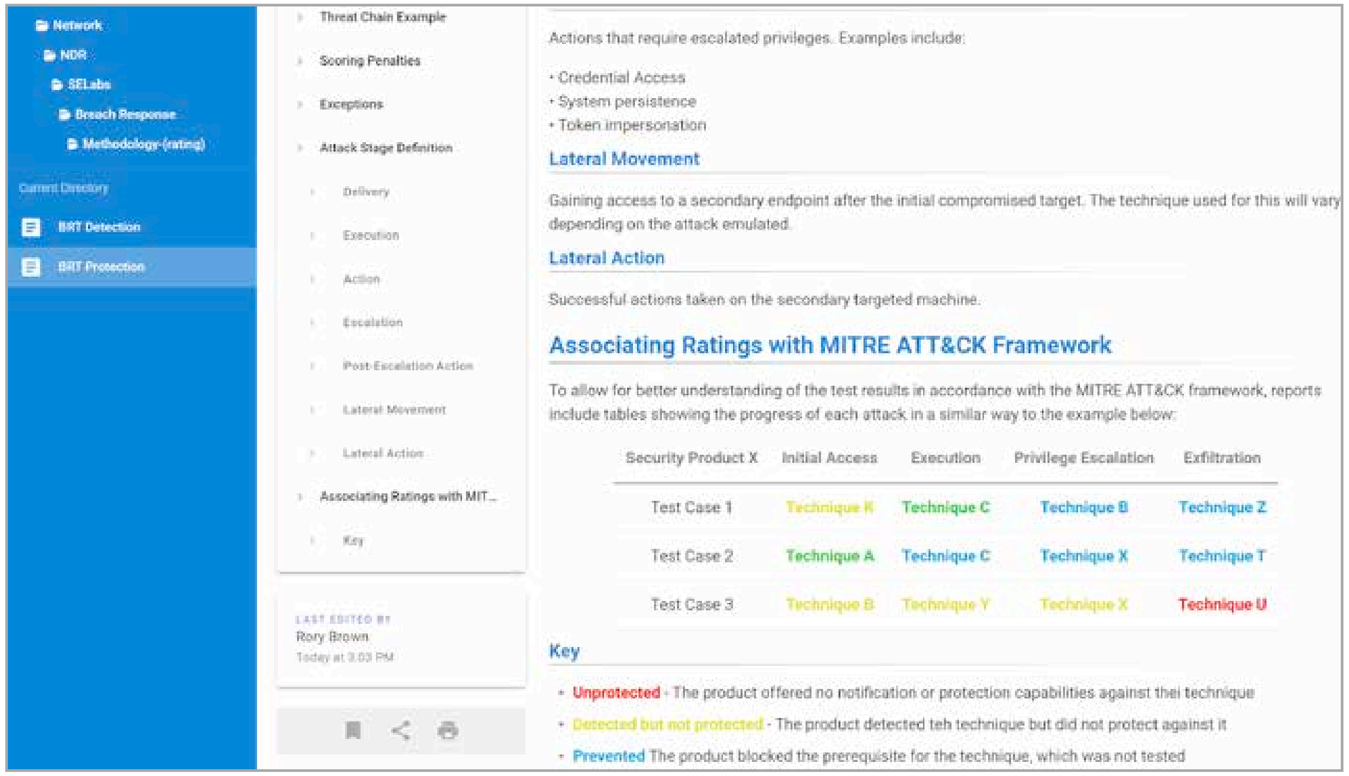
The Security Testing DataBase is the world's primary resource for companies and individuals interested in cybersecurity testing. Whether you are interested in endpoint security, network appliances or cloud services, its goal is to inform security professionals about how testing can be run; how past tests were executed; and provide high levels of detail about how the products and services were configured.

The Security Testing DataBase is owned by SE Labs but operates independently. It examines tests from other testing organisations too, and its guides are general purpose. Much of the material is not specific to SE Labs' testing.

If you are in the market for a new firewall, for example, you can use the Security Testing DataBase to better understand how testers assess these devices. In some cases, you will even be able to view and download the firewall's configuration files as used in a public test.

Similarly, if you are interested in email security testing the site contains general resources around testing these cloud-based services, as well as the configuration details used in public tests.

The site contains information about tests from a range of testing organisations. Potential customers of security products can gain a wide perspective on security testing, and be able to dig down into details that can help buying decisions.



Actions that require escalated privileges. Examples include:

- Credential Access
- System persistence
- Token impersonation

Lateral Movement

Gaining access to a secondary endpoint after the initial compromised target. The technique used for this will vary depending on the attack emulated.

Lateral Action

Successful actions taken on the secondary targeted machine.

Associating Ratings with MITRE ATT&CK Framework

To allow for better understanding of the test results in accordance with the MITRE ATT&CK framework, reports include tables showing the progress of each attack in a similar way to the example below:

Security Product X	Initial Access	Execution	Privilege Escalation	Exfiltration
Test Case 1	Technique K	Technique C	Technique B	Technique Z
Test Case 2	Technique A	Technique C	Technique X	Technique T
Test Case 3	Technique B	Technique Y	Technique X	Technique U

Key

- Unprotected - The product offered no notification or protection capabilities against thei technique
- Detected but not protected - The product detected teh technique but did not protect against it
- Prevented The product blocked the prerequisite for the technique, which was not tested

Gain deep understanding of how to test and rate security products

Most of the information is very technical, which makes it an ideal resource for in-house security testing teams. If you want to run your own test with cutting-edge techniques, the Security Testing DataBase can help.

How to use the database

Subscribers can access the following information:

1. Learn about general security testing principles
2. Browse guides on different ways to test, including how to use attack tools
3. Discover ways to approach different technologies
4. Compare how different testers work
5. Use test data and configurations to improve your own testing and security deployments

Apply

Anyone can apply to access the site. However, due to the sensitive nature of the content, we are currently processing applications on a case-by-case basis.

Two levels of subscription are available: User and Contributor. Applications are particularly welcome from internal security assessment teams working for large global organisations; security vendor third-party testing teams; and independent security researchers.

To apply to access the Security Testing DataBase please email sectestdb@selabs.uk

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 were the first testers to use machine learning to help power our tests.

Advanced Security Testing

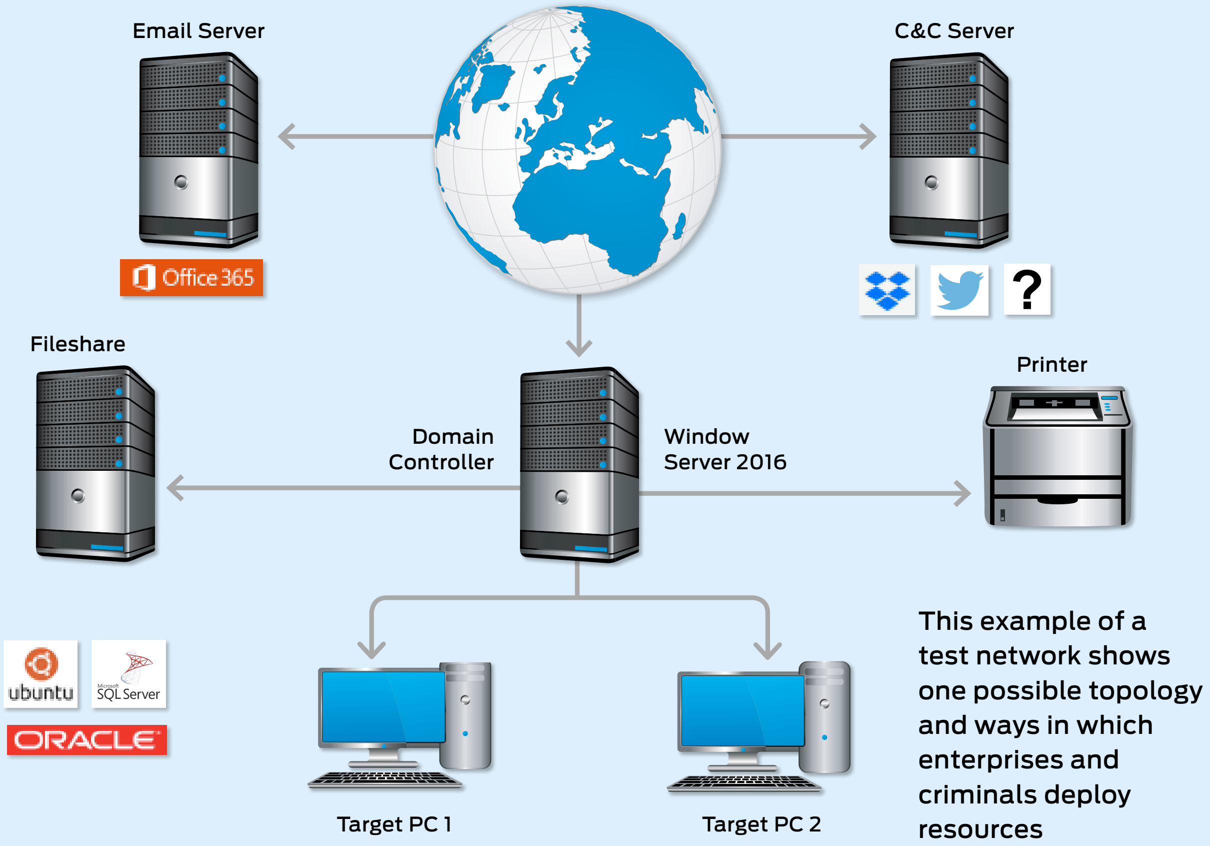
Over the course of 2021 we used our full attack chain testing on a range of products. The most common choice by the vendors was their endpoint protection products. This is why most of the 'breach response' reports on our website contain results for endpoint or 'EDR' products.

However, the way we test also works perfectly with firewalls, intrusion detection systems and cloud services. Starting in 2022, we've migrated our 'breach response' testing to the Advanced Security test programme. Advanced Security testing is available for endpoints; network appliances; and cloud services. This means that we're already producing Advanced Security reports for EDR, next-generation firewalls, network detection and response systems and email security services.

As before we have 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 Advanced Security test reports. Subsequently, it will also be simpler to assess which products you might choose to deploy.

Regardless of the product type, we can produce Advanced Security reports in one of two modes: Detection or Protection. 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

Advanced Security 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
Dragonfly & Dragonfly 2.0	✉ W	🏭	Phishing & supply chain methods used to gain access
APT34	✉ W <>	$ 🏭 🏛	Phishing with email and other services, combined with public tools
FIN7 & Carbanak	W	🛒	Documents containing scripts combined with public tools
APT29	✉ <>	🏛	Spear phishing emails containing scripts or links to malware

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

Key

✈ Aviation	🏦 Banking and ATMs	🏭 Energy	$ Financial
🃏 Gambling	🏛 Government Espionage	⛏ Natural Resources	🛒 US Retail, Restaurant and Hospitality

product can detect different elements of an attack. You can read about these reports on **page 14**.

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 2021 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 in the mail

Our Advanced Email Security test also reached new strengths in 2021. The way we test has expanded to include business email compromise threats, to the extent that our test framework includes the ability to replicate a real target organisation and its attackers and legitimate suppliers.

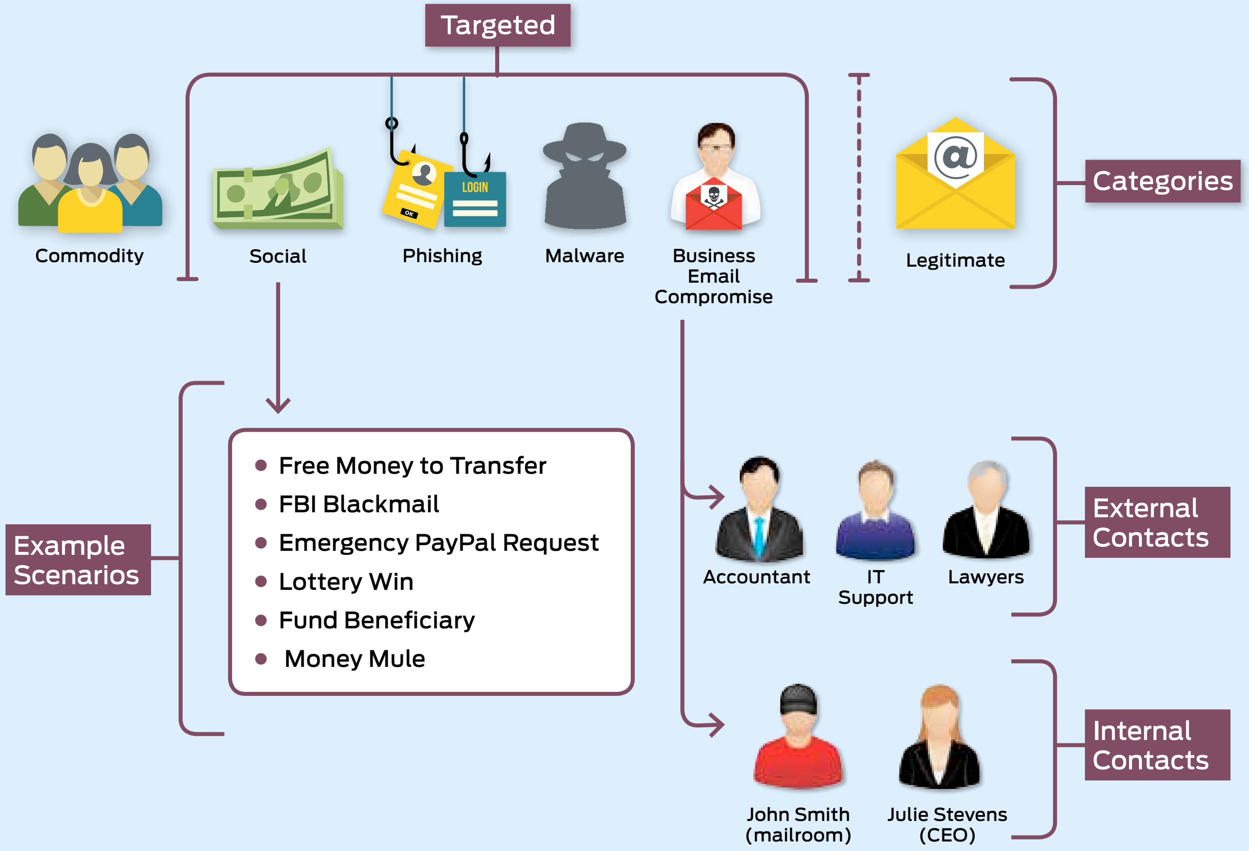
We also run a baselining process during which next-generation email security products can learn what a clean network looks like. This helps some technologies detect malicious anomalies.

The development of this test has attracted the attention of all the major email vendors, who are now testing privately with us on a regular basis. Public reports, along with important details of the configurations used, are available on our website.

Threats mobilise

Finally, we have created a new mobile security test that covers both Android and iOS. All of our testing must produce useful, meaningful data, which is why we have previously resisted running anti-malware tests for Android and iOS platforms – there isn't really much in the way of true malware in the wild. We are focussed on assessing mobile products' abilities to protect users from significant threats that pose real-world issues for users such as phishing.

Advanced Email Security Test Case Structure



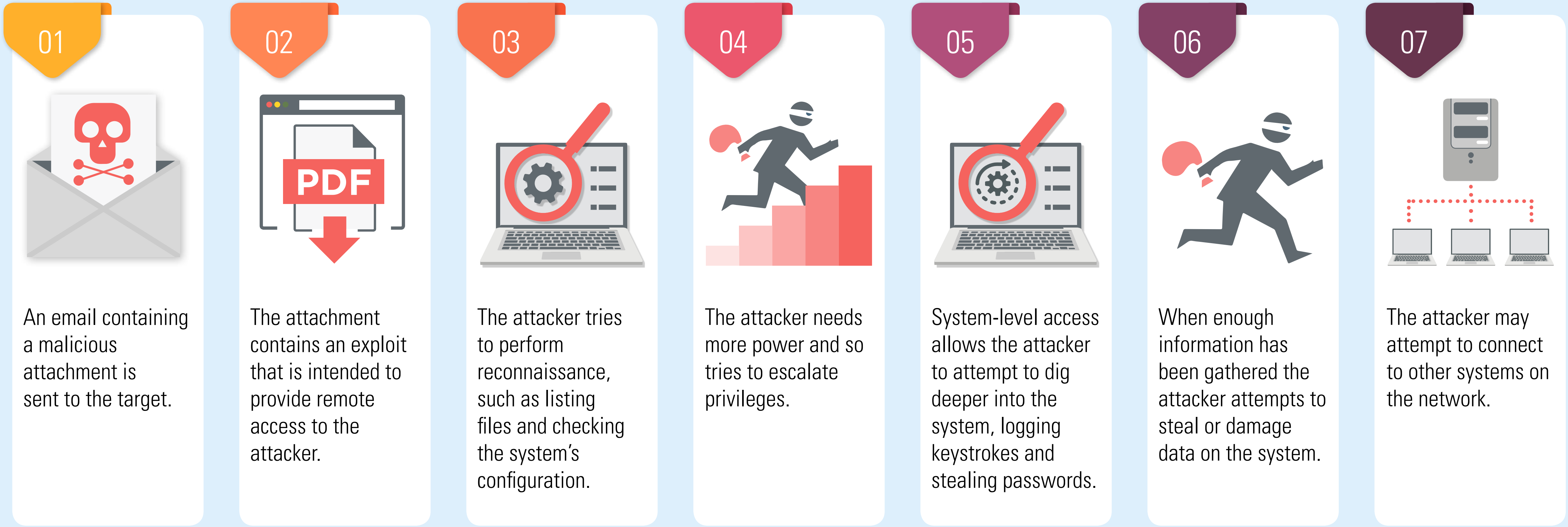
Threats used in the Advanced Email Security test vary in type and include targeted business attacks

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 An email containing a malicious attachment is sent to the target.

02 The attachment contains an exploit that is intended to provide remote access to the attacker.

03 The attacker tries to perform reconnaissance, such as listing files and checking the system's configuration.

04 The attacker needs more power and so tries to escalate privileges.

05 System-level access allows the attacker to attempt to dig deeper into the system, logging keystrokes and stealing passwords.

06 When enough information has been gathered the attacker attempts to steal or damage data on the system.

07 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 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.

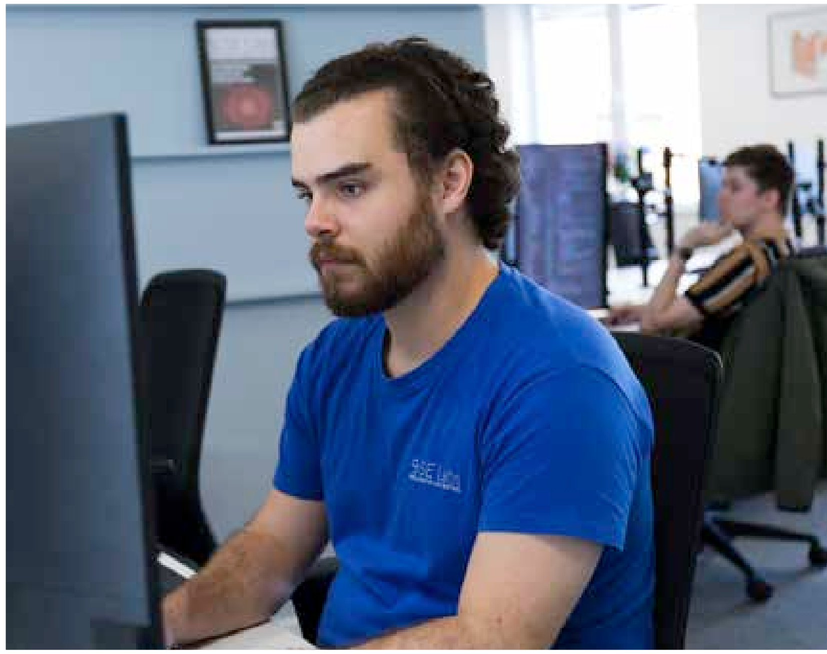
Venturing forward

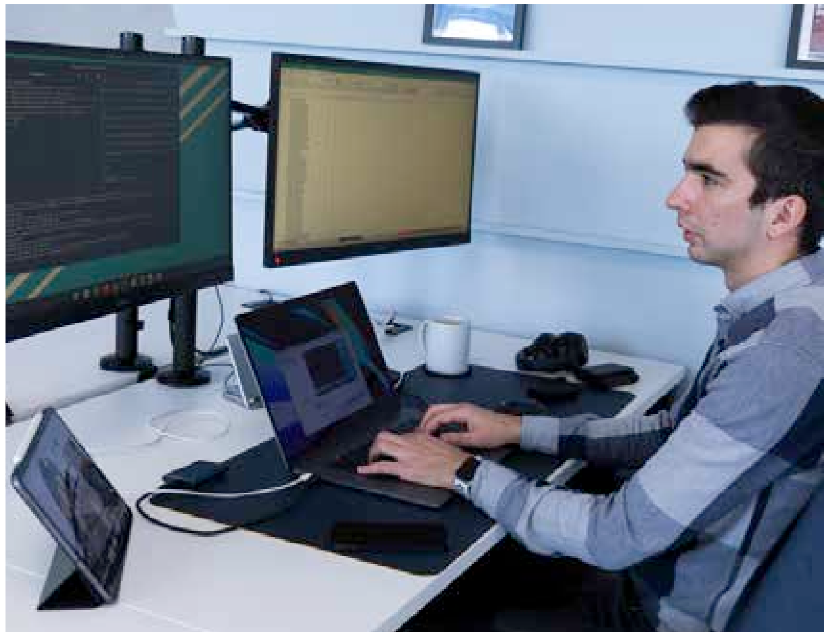
This knowledge is also useful to potential investors in cyber security, which is why our Investor Intelligence Insights (i3) programme is in such demand. Working with venture capital and other types of investors, we can lift the lid on the technology behind the sometimes very dubious pitch claims.

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 most standalone Advanced Security tests). In some very specific situations, a private test may be made public. To see the detailed options see the **flowchart** on page 14.





Testing with SE Labs

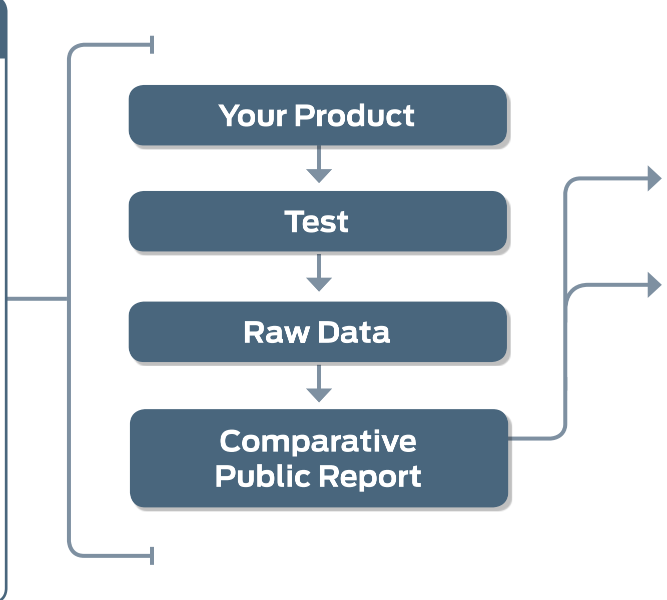
Our Advanced Security testing can be used for internal product development and public or private competitive comparisons.

PUBLIC

Outcome

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

- 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.



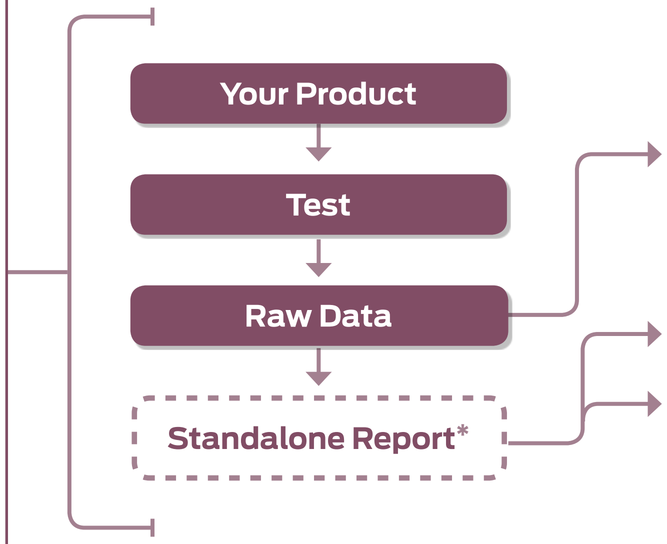
Testing Type	PDF Marketing Report Produced	Distribution Licence Ownership	Remarks
Public Test Option 1	✓	✗	The marketing report is produced as part of the public test. It is published and distributed by SE Labs.
Public Test Option 2	✓	✓	

PRIVATE

Outcome

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

- 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.



Testing Type	PDF Marketing Report Produced	Distribution Licence Ownership	Remarks
Private Test Option 1	✗	N/A	
Private Test Option 2	✓	✗	The report can be internally distributed and published on the SE Labs website.
Private Test Option 3	✓	✓	

* Optional

Endpoint Protection Review

What have we learned after six years of testing?
There are a lot of opinions about anti-malware products, with many being based on anger, frustration and bias. We've previously written about anti-virus bashing on our blog. We take an unbiased and practical, data-driven approach to endpoint security. We test it over a long period of time, consistently and using the threats of the day. After six years we have identified some interesting trends and other observations.

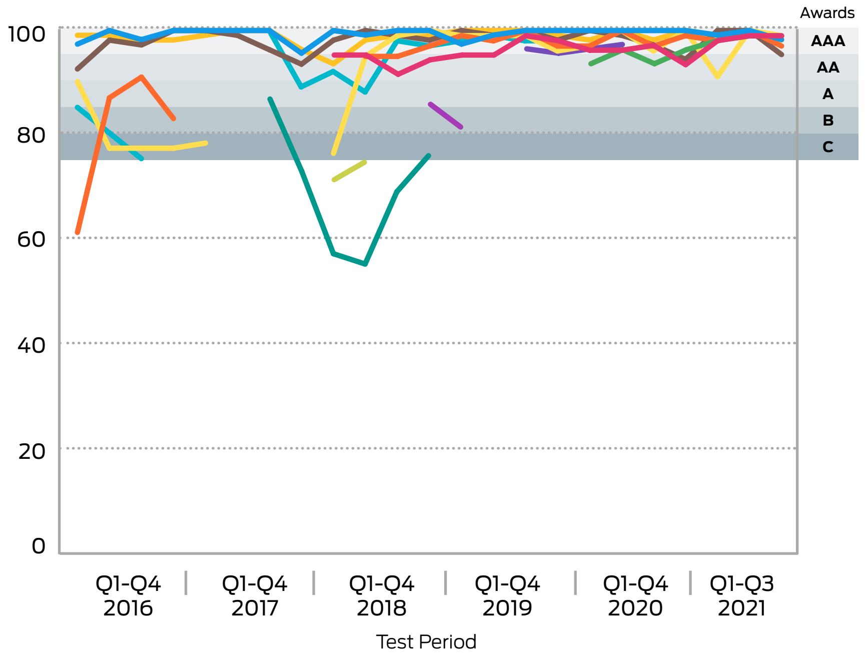
Firstly, and this should be no surprise to industry watchers, there are identifiable tiers of products. We're not talking about price or customer base, but effectiveness. Some vendors are capable of consistently providing reliable and wide-ranging anti-malware protection, while others are consistently less effective.

The best-known brands deserve their reputations. There will always be a little variation but the continued strong performance in the very challenging tests is a testament to their struggle against the malware threat. It's rare to see a good product drop its protection for long periods of time.

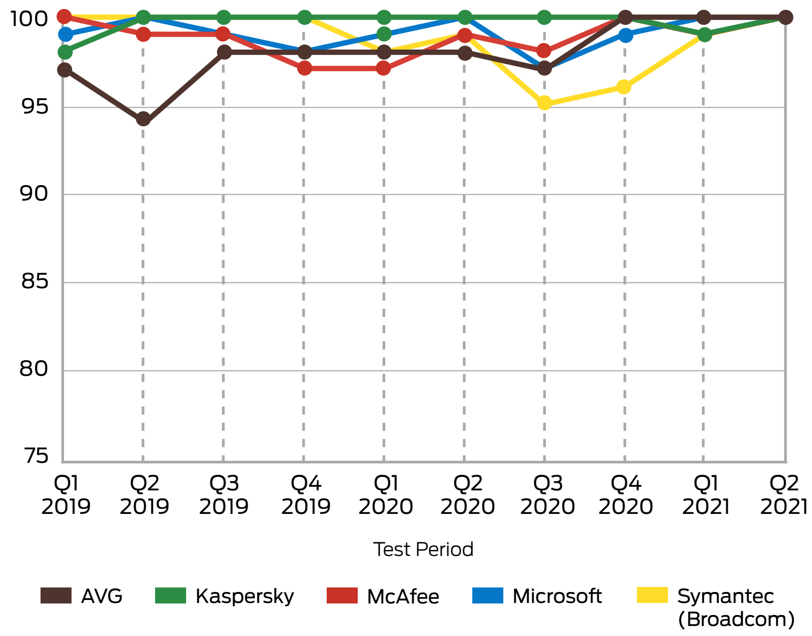
However, drops do happen and in 2017 we noticed that many products struggled with targeted attacks. We believe that they improved thanks in some part to our consulting services.

The best products have stayed strong, while technical investment has brought improvements to products that were lower scoring six years ago. This is an encouraging trend in a world where ransomware malware makes headlines regularly.

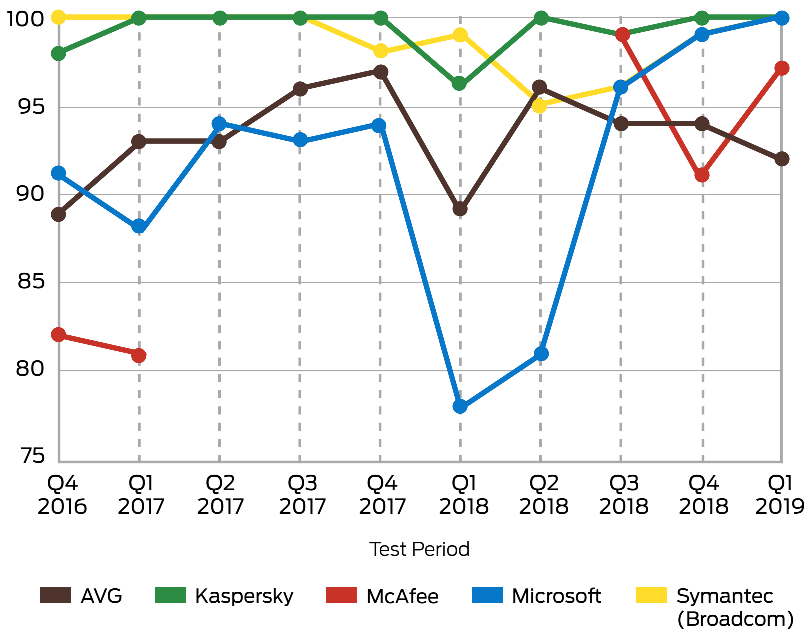
Top tier products win AAA awards



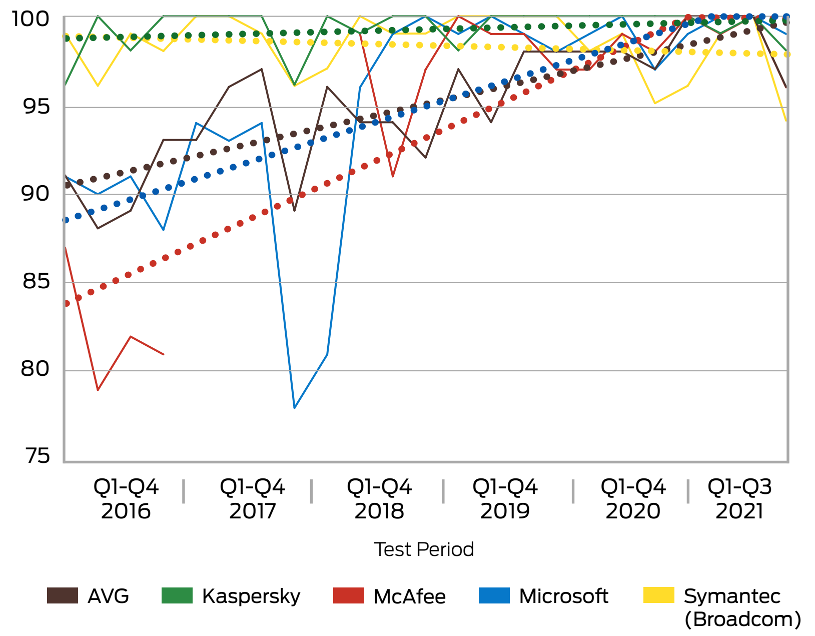
Best known brands consistency strong



Very challenging targeted attacks



Positive performance trends



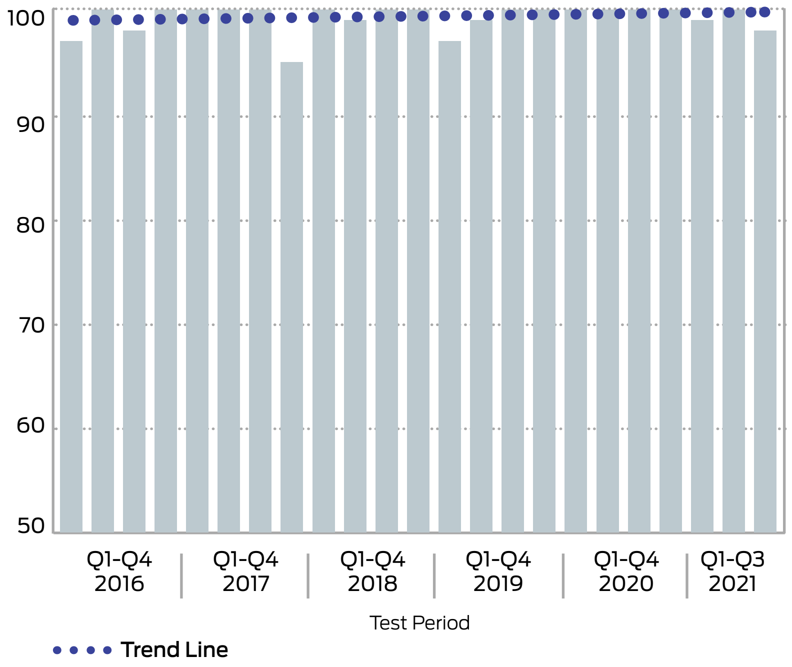
Endpoint Protection Focus

Top tier product improvement

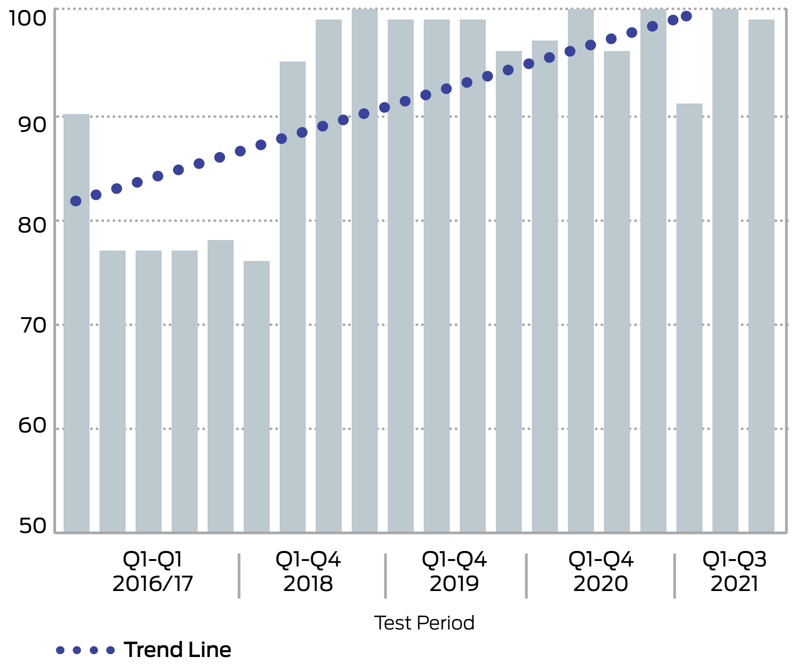
This summary of the performance of the top tier enterprise anti-malware products shows that there is variation even at the head of the pack. We've been watching them improve or remain solid since the start of 2016, when we started this testing project.

Kaspersky and **Symantec** (now **Broadcom**) have always performed very well, so there is not much improvement to be shown over the testing period. **Crowdstrike** started working with us in 2018 and a strong initial performance was followed by further improvement. **McAfee** and **Microsoft** have both demonstrated large improvements over the years.

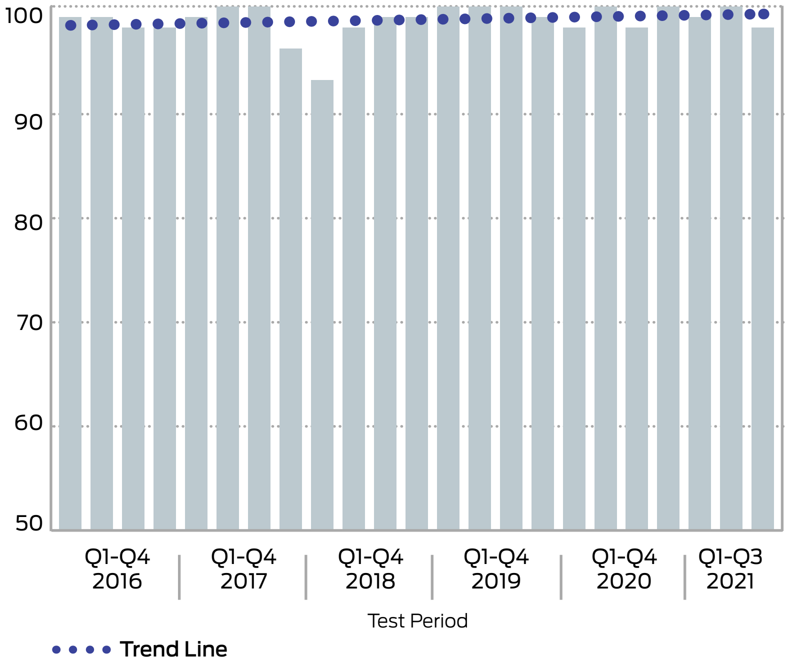
Kaspersky



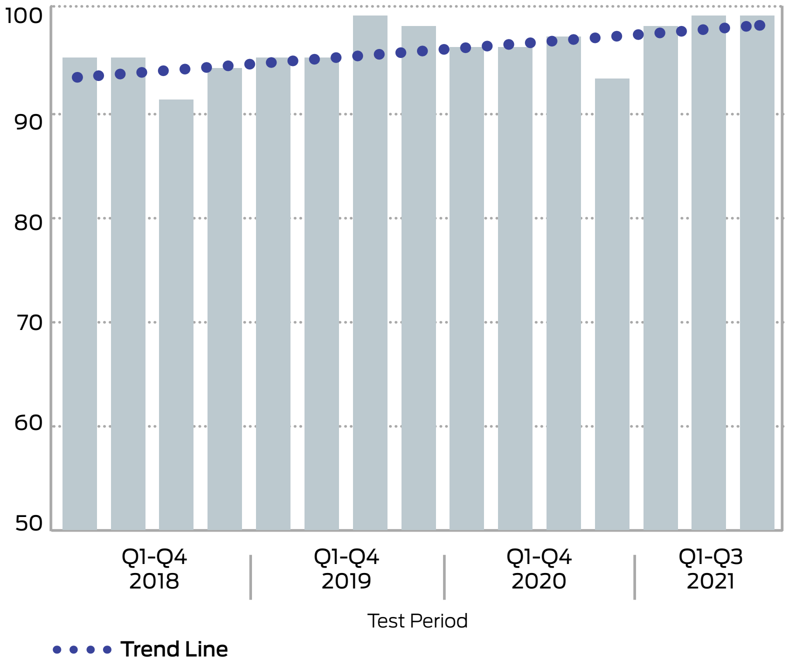
Microsoft



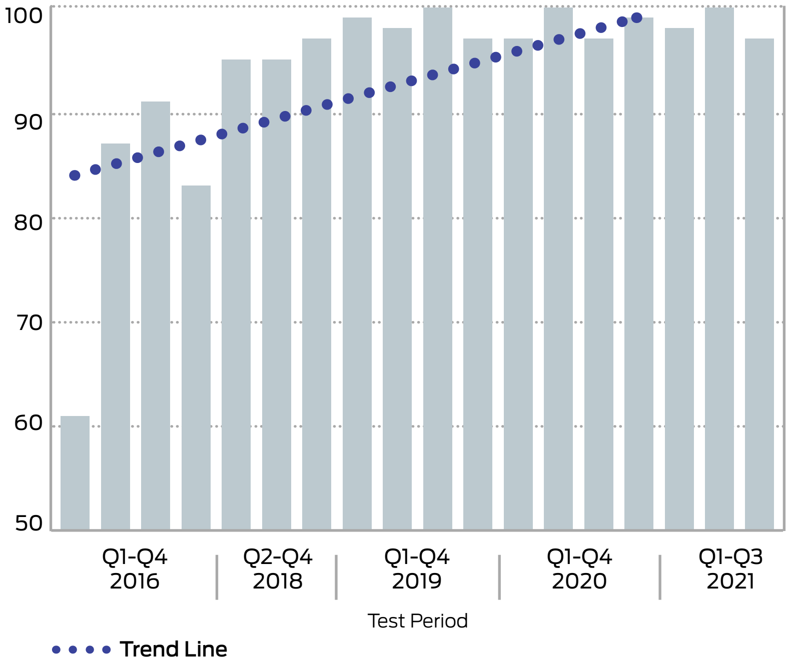
Symantec (Broadcom)



Crowdstrike



McAfee



A Word from Simon

Ransomware attacks aren't special

Ransomware is in the headlines. It makes for great copy because a typical ransomware attack involves hacking, an obvious impact on a business and large amounts of money. Even those with no computer knowledge can understand the basic concepts involved: criminals hack big companies and demand money in return for giving back the files they've 'stolen'.

But, as we'll discuss below, hacking doesn't need to involve super-secret programs and the kind of arcane knowledge known only to a handful of shadowy computer nerds. You can set yourself up as a pretty competent attacker with a handful of widely available books, some free software and access to YouTube. That sounds depressing and scary, but there is some good news in there too.

Let's look at Hacking Exposed, Second Edition. Published in 2000, this book explained in detail not only the principles behind computer exploitation but also the techniques. Simply scanning the main sections in the Contents page gives you the standard hacker playbook. You'd expect to run some reconnaissance, gain access, escalate privileges and steal or destroy information. Establishing persistent access is optional. This is all quite straight-forward and predictable. Which is good news for defenders.

In a ransomware attack the 'steal or destroy' stage above is where you would run the program that encrypts the victim's data. Everything up to that point is the same, whether your intent is to start a ransomware campaign, spy on the organisation silently or use the compromised system as a steppingstone to another network.

One positive thing that's come out of the prevalence of ransomware campaigns is that it's increased awareness of the hacker threat. We hope that defenders don't focus solely on anti-ransomware defences and recognise that general security measures help stop ransomware as well as many other flavours of attack. See ransomware as merely a payload in a regular attack. Defend against regular attacks and you stop ransomware, as well as other types of threats.

Enterprise security testing challenges

No test can completely represent all possible outcomes in the real-world. A good test will approximate real life as closely as possible. A good test can provide likely (but not guaranteed) predictions about future performance in various situations. A good test report will help you beat the odds because, over time, informed decision-making is better than doing things randomly.

All this is true, whether you are testing car tyres, trialling medicines or assessing school children with exams. Real life introduces variations that a test can't always copy or take into account, be they tyre performances in different weathers, different immune systems or teenage hormones.

Security vendors vs. hackers

Attackers behave in a number of ways, although they tend to follow basic principles and rely on well-known techniques. They don't use magic because they don't have to. Tried and trusted hacking methods rule the day, but hackers can adapt when they need to.

Similarly, security vendors produce products that they claim will stop these attackers. In many cases vendors use tried and trusted detection and protection methods because they work. Problems arise when a sufficiently motivated attacker learns to bypass the protection in place. It's then an arms race in which security products block attackers, who then learn how to progress, which then inspires the vendors to adapt. And so on. For decades.

It's about the settings.init

Security products are complex, with many options. IT teams can enable and disable certain features, for example. There are policies to create. Should suspicious files be blocked and deleted, or moved somewhere for analysis? Or allowed? Or allowed for some users but not others?

Other products can be added, too. You would not expect a Global 500 organisation to use just one security product and rely on its default settings.

So security testing has a challenge. What settings should a tester use? What type of organisation should it emulate when running a security assessment on, for example, an anti-virus endpoint product or an email security service?

Let's look at some extreme examples. An ATM is just a computer that spits money out at you on the street when you authenticate (and have sufficient funds). The ATM company would not expect to install software very often on such a device so it can lock it down and prevent any changes. This could be as simple as running the main operating system from a read-only disk. Or you could use an allowlisting product to monitor changes to the system and block new programs from running.

This approach would not work well when securing the laptops of your website developers, who need to have some level of creative freedom over the software they install on their systems. One security product would not work well for both the locked-down cash machine and an art director.

Insider testing

SE Labs works directly with large organisations that want to confirm or challenge the security of their environments and make decisions about changing products and services. This allows us to understand better how real companies work. This understanding feeds into how we test. We don't make wild assumptions about what clients need from their security purchases. And while we listen to vendors when they claim that customers want X or Y, we don't always believe them!

A typical question is, "We use products X, Y and Z. Can we replace all of these with Microsoft?" In some cases we build a test environment using those products to run a comparison, using advanced threats in a bake-off. In others, the client will provide virtual images or even real laptops configured with software and hardware security measures in place, exactly as used in real life.

Tests of business security products that use default settings can be useful as a baseline. However, there is so much more to buying, installing and using a security product than a single test's results can indicate usefully.

When you read an enterprise security test look for transparency in how the tester ran the test. What version of the product was used? What was its configuration? Does the configuration match the sort of setup your organisation requires? Did the tester follow the AMTSO testing Standard (see page 8)?

SE Labs publishes all of these details and more. And you can even download configuration files and read more about the threats used from the new Security Testing DataBase, which is available to all testers in the world. This way you can understand test results more clearly and learn the best ways to lock things down.

Stay in Touch

Don’t miss out on the latest in the world of cybersecurity testing

Newsletter

SE Labs

INTELLIGENCE-LED TESTING

News from the security lab

Our monthly newsletter provides a compact summary of all our reports, blog posts and other analysis that we provide publicly. Subscribe to this free newsletter and you won’t miss out on a thing.

Don’t rely on catching our social media posts as they fly by. All the best stuff ends up in the newsletter! We have options for enterprises, consumers and security vendors. Sign up now for free.

Link: https://selabs.uk/newsletter

Sign Up

Blog

SE Labs

Special Edition

Computer security testing comment and analysis from SE Labs

Ransomware Protection Tested

Red screens means red faces. Prevent, don’t pay!

Ransomware is causing all the rage right now. That’s why we’ve tested products that

Test results

Archive of security product and service test results

Subjects

Our blog gives a behind-the-scenes view on cybersecurity testing. Learn how we work and how you can improve your own personal and business security.

The blog adds extra context to all of our public reports. Understand what the security reports can mean to you, and how to use their results.

Our team monitors the threat landscape and writes about what we see. Stay informed about the latest attacks and learn how to stay safe.

Link: https://blog.selabs.uk/

Visit

Podcast

DE:CODED – Selling Security: The Insider’s Guide

“You’re thinking: How much truth is in that report?”

DE:CODED is the official podcast from SE Labs.

The security testers at SE Labs help decode the notoriously opaque world of cybersecurity. Practical and insightful, our experts have experience in attacking and defending in the physical and digital worlds.

In-depth discussions with expert guests will help you develop your own strategies for protecting yourself and your business. No marketing. Just solid, valuable advice from the best in the business.

Peek behind the curtain with DE:CODED, the award-winning cybersecurity podcast.

Link: http://decodedcyber.com/

Listen

Engineering firm Mitie hit by major ransomware attack
The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) linked roughly $5.2 billion worth of Bitcoin transactions to ransomware
Hackers
CYBER CRIME 'WE'RE ALL TARGETS'
Police warn everyone could be at risk
More crime is now online than offline
OAP robbed by hacker tells her story
Only 13% cybercrime solved in two years
held to ransom ++ Operations cancelled ++
A&E ++ But why WERE warnings ig
CYBER HACKERS CRIPPLE THE NHS
Cyber crime surges in Covid
Criminals also release new computer viruses
ransomware
English hospitals divert ambulances after 'ransomware' cyber attack
Protect
hacks 15,000 at Hospital, ransom
Three U.S. Hospitals Hit in String of Ransomware Attacks
flood cyber crime portal
highlights dilemma for fight against malware
Ransomware attack hits
CYBERSECURITY
INDIA'S DIGITAL
DON'T BE HELD TO RANSOM
UK rail network hit by multiple cyber attacks last
India lags in cyber s
Banks to face 100 million attacks experts warn
High alert over global cyber attacks

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.