MANDIANT®

DEEP DIVE
INTO CYBER REALITY

SECURITY EFFECTIVENESS REPORT 2020

Deep Dive Into Cyber Reality

This report focuses on an analysis of security controls effectiveness across the multiple stages of attack lifecycles within 11 global industries. To gather data, our experts executed thousands of tests comprised of real attacks, specific malicious behaviors, and actor-attributed techniques and tactics. The report data provides measured evidence of leading enterprise production environments across network, email, endpoint and cloud-based security controls.

Our findings confirm the concern held by many security practitioners: Security controls are not performing as expected.

Mandiant Security Validation[1] experts generated evidence that current security control configurations cannot consistently protect enterprises from elevated cyber threat risks as previously assumed. This directly impacts core business objectives such as continuity of business operations, security of corporate assets, delivering evidence of regulatory compliance, and controls optimization.

1. Formerly Verodin Security Instrumentation Platform (SIP)

Table of Contents

This contents page is interactive. Click a section title to navigate straight to it.

Cyber Effectiveness as a Business Metric

Measuring the effectiveness of and justifying the investment in security controls has become a key performance metric for enterprises because boards of directors and CEOs are expected to provide verifiable proof that business assets are protected from the fallout of a potential breach. However, as organizations begin to address cyber risk as a business problem, they also continue to manage security as an IT function. This dynamic exposes the misalignment between IT, which owns infrastructure, and the security team, which owns the cyber security controls and processes that protect the business. Our experts have found that this disconnect increases the need for security teams to generate reliable evidence of effectiveness.

Security leaders report that they need to be able to confidently answer important questions, such as:

- **How effective are my security controls?**
- **How quickly can I assess the relevance of threat intelligence or my exposure to a likely attack?**
- **How well do I stop data leakage and protect data integrity?**
- **How can I simplify and standardize my security stack?**
- **What evidence can I provide with key security metrics for my executives?**

The Challenge of Measuring Security Effectiveness

CIOs and CISOs continue to report the importance of being vigilant as they validate and test security architectures. The challenges and complexities of having unique environments, multiple teams and constant change requires that their security programs evolve continuously. Security teams need a way to continuously measure and monitor controls to capture quantitative evidence of security gaps so they can demonstrate with evidence the ability to reduce risk and improve the organization's overall security posture.

The statistics outlined in this report were generated through careful analysis of thousands of attack behaviors. These attack behaviors were executed in enterprise production environments supporting over 900 million consumers, and against 123 market-leading security technologies, such as network, email, endpoint and cloud solutions.

ENTERPRISE PRODUCTION ENVIRONMENTS

11 INDUSTRY VERTICALS

123 MARKET-LEADING SECURITY TECHNOLOGIES

900M CONSUMERS AFFECTED

9%

IT IS ALARMING THAT ALERTS ARE ONLY GENERATED FOR 9% OF ATTACKS

Our experts discovered:

- Security tools perform differently from one environment to the next
- Size of an organization has not proven to correlate to security effectiveness
- There is a disconnect between security team assumptions, expectations and reality when we compare the effectiveness of organizations' ability to alert, block and detect threats

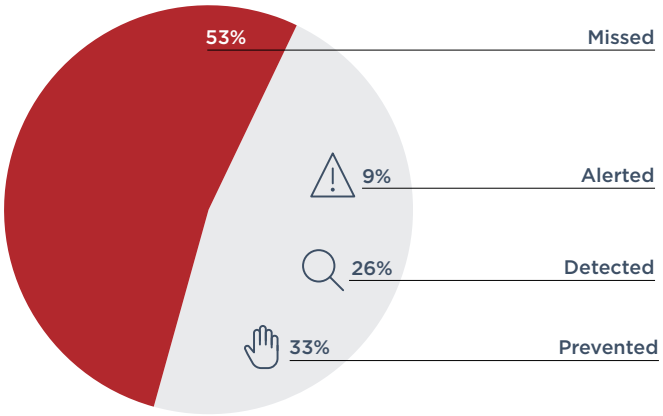


Figure 1. Aggregated data for attack interactions. Total is greater than 100% because alerted is a subset of detected and attacks *can be either or both detected and prevented.*

Many organizations are performing below their predicted levels of effectiveness. The data (Fig. 1) shows that many companies find a discrepancy between their expected capabilities and the measured results. On average, they detect only 26% of attacks and prevent 33% of them, which provides an opportunity to optimize their investments. It is alarming that alerts are only generated for 9% of attacks.

Altogether, this has a negative impact on incident response because SIEMs and other technologies responsible for triggering alerts cannot deliver a high level of fidelity to both prioritize and address security concerns.

Definitions of Attack Interactions

Missed An attack that was not prevented or detected.

Alerted Event raised to an analyst or response level, typically through a SIEM.

Detected Security control creates an event identifying an attack.

Prevented Security control successfully blocks an attack.

The Impact of Macro Trends on Security Effectiveness

Cloud
Moving workloads to cloud environments is commonplace today which introduces security risks to the enterprise. Organizations and experts alike have highlighted how this move complicates visibility and the ability to validate that controls such as network segmentation and credential management operate as intended in a hybrid model. Tests have shown that misconfigurations can expose data to the public when new instances are created and policies are set incorrectly. Corporate assets are also susceptible to risk when controls for specific business network zones are accidentally bypassed due to misconfigurations.

Disconnect Between IT and Security
While security teams are responsible for protecting organizational assets, they do not always have the corresponding operational authority or visibility into decisions or changes being made that impact the infrastructure. This disconnect results in "environmental drift," which causes the organization's risk posture to change unexpectedly. In the absence of continuous validation of controls, this can put the organization in a precarious position.

Technology Overload and Movement to Standardization of Controls
While our research suggests that on average, enterprises have 30-50 different security tools, data in this report comes from organizations that can exceed that number. This highlights the need to produce evidence of a specific tool's contribution to the overall security posture—evidence that supports standardization of security controls and divestiture of technologies that no longer add value.

Impact of Data Leakage
Organizations continue to highlight that protection of data and intellectual property has become central to business objectives. Corporate data protection, integrity and access are directly aligned with competitive advantage and valuation. Evidence of an organization's ability to protect data is a fundamental requirement of reporting to boards of directors and executives. The rise in activity from nation states, criminal actors and hacktivists, combined with the rapid growth of data and the complexities of corporate networks, reinforce the need to constantly test and validate specific controls and policies.

Host-based Controls
An over-reliance on host-based controls, which can be associated with a lack of visibility into status of security controls, may cause additional exposure for organizations.

Details on Seven Critical Security Challenges

From Reconnaissance to Lateral Movement

Several attacker techniques and tactics are associated with challenges most commonly found in enterprise environments when conducting testing through security validation. They are analyzed here, and include real-world examples.

Security tools are often configured to address such challenges but may be poorly optimized. The most common reasons for poor optimization include:

- Deployed under default "out-of-the-box" configurations
- Lack of resources to tune and tweak post-deployment
- Security events not making it to the SIEM
- Inability to force controls testing
- Unexpected changes or drift in the underlying infrastructure

When we asked security executives, "How do you believe your controls are performing in each focus area?" many found that after executing an initial iteration of testing, their production environments performed well below expectations against these challenges:

- **Reconnaissance**
- **Infiltrations and ransomware**
- **Policy evasion**
- **Malicious file transfer**
- **Command and control**
- **Data exfiltration**
- **Lateral movement**

ATT&CK

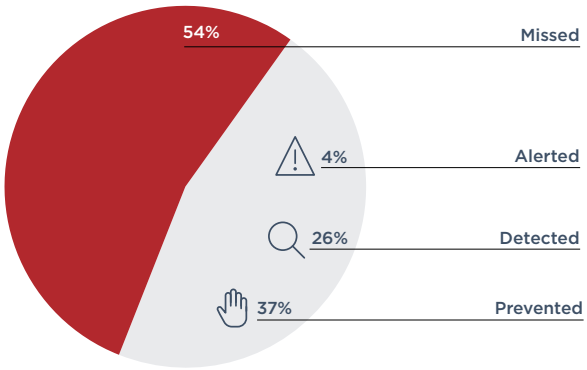
Operationalize Threat Intelligence

The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) framework has emerged as a key resource for security teams attempting the process of defending against threat actors. Technologies designed to test or validate security defenses offer new means to operationalize threat intelligence. Security teams can leverage ATT&CK to perform gap assessments on their defenses and discover what needs improvement.

4% OF RECONNAISSANCE ACTIVITY GENERATED AN ALERT.

RECONNAISSANCE

After testing network traffic, organizations reported only 4% of reconnaissance activity generated an alert. This exposes the risk associated with misconfigured controls, resulting in higher risks of successful scanning and profiling as well as a high percentage of missed early stage attack tactics.



Common Causes

- Network segmentation misconfiguration
- Lack of internal security control points—inside network traffic is not monitored the same way
- Inability to distinguish reconnaissance from normal network monitoring

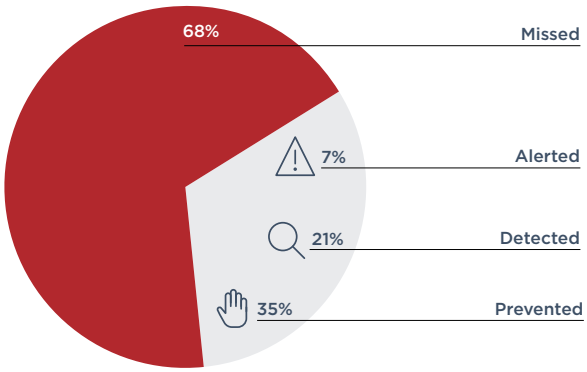
Example

A Fortune 500 company leveraging security validation discovered an inadvertently misconfigured proxy that was responsible for maintaining segmentation across two regulated systems. This misconfiguration enabled communications between networks and exposed a portion of the company's critical internal business network. With continuous validation in place, the security team was immediately alerted on this change and the company quickly restored segmentation and addressed exposure.

68% CONTROLS DID NOT PREVENT OR DETECT DETONATION WITHIN THEIR ENVIRONMENT **68% OF THE TIME.**

INFILTRATIONS AND RANSOMWARE

After testing against infiltration and ransomware tactics, organizations reported their controls did not prevent or detect detonation within their environment 68% of the time.



Common Causes

- Deployed under default "out-of-the-box" configurations
- Unknown fail-open conditions in security controls
- Outdated or poorly maintained signatures

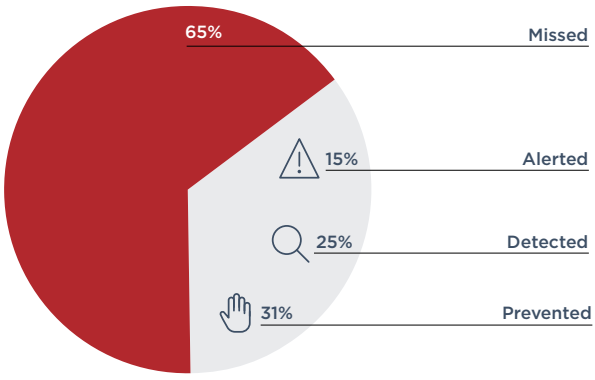
Example

During an initial testing period within a government entity, the security team identified that their network firewall blocked only 24% of executed attacks. Using detailed information that identified the attack patterns and behaviors, the security team was able to work with the client's vendor to optimize the firewall and increase attack blocking capability to 74%.

65% 65% OF THE TIME, SECURITY ENVIRONMENTS WERE NOT ABLE TO PREVENT OR DETECT THE APPROACHES BEING TESTED.

POLICY EVASION

When executing evasive focused attack techniques to bypass policies, 65% of the time, security environments were not able to prevent or detect the approaches being tested.



Common Causes

- Outdated classification categories
- Limited network monitoring on expected protocols
- Inadequate tracking and communication of changes for one-off exceptions

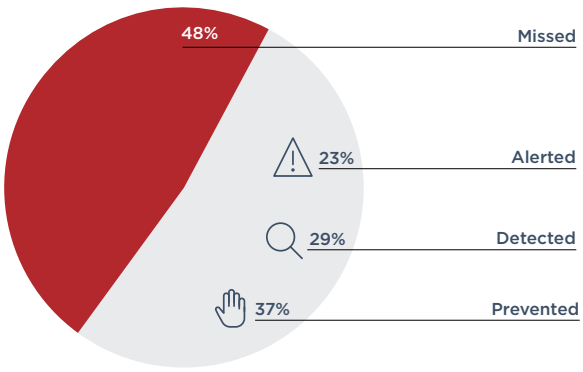
Example

A Fortune 500 company leveraged security validation to continuously monitor for changes causing environmental drift, and the investigating team discovered that data was not being delivered to the SIEM. After analyzing test results, they discovered that syslogs were being sent over UDP instead of TCP and a misconfigured load balancer was dropping all UDP traffic. As a result, events were not being sent to the SIEM and correlation rules did not trigger alerts to initiate the incident response process. The ability to test this with real attack actions exposed this scenario and allowed the company's security team to remove the risk.

48% OF THE TIME, CONTROLS IN PLACE COULD NOT PREVENT OR DETECT THIS STAGE OF THE ATTACK LIFECYCLE.

MALICIOUS FILE TRANSFER

When executing techniques and tactics associated with the delivery and movement of malicious files, 48% of the time, controls in place could not prevent or detect this stage of the attack lifecycle.



Common Causes

- Unaware of vendor removal of malware signatures
- Misconfiguration of existing security controls
- Under-resourced or aging sandboxing techniques and technologies

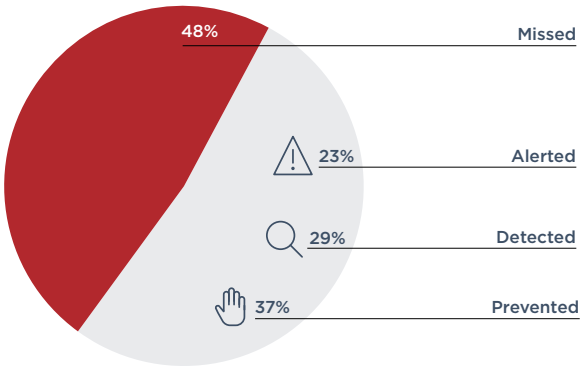
Example

An insurance provider leveraged security validation to test various network zones, including areas designated as hardened. Test results provided evidence that 35% of malicious file transfers attempted were allowed by the company's security tools and no alerts were generated in the SIEM for attempts that were detected and prevented. Continuous security validation identified misconfigurations, and this discovery resulted in the rapid optimization of security tools to minimize risk exposure going forward.

97% OF THE BEHAVIORS EXECUTED DID NOT HAVE A CORRESPONDING ALERT GENERATED IN THE SIEM.

COMMAND AND CONTROL

Of the tested command and control activities, 97% of the behaviors executed did not have a corresponding alert generated in the SIEM.



Common Causes

- Outdated or missing site classification
- Lack of SSL inspection
- Security events not making it to the SIEM

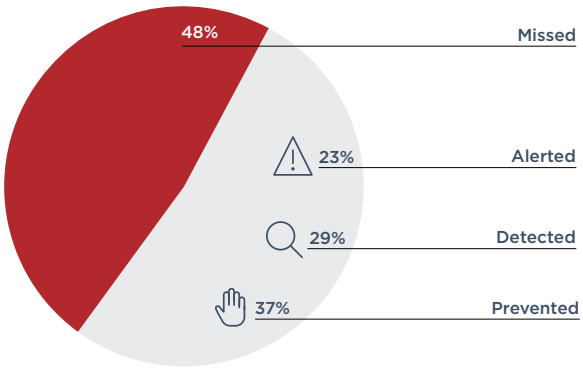
Example

To rationalize significant security investments and identify areas for divestiture, a critical infrastructure customer in the energy sector leveraged security validation. The team's testing efforts identified areas of overlap in capabilities, inefficiencies in product expectations and gaps in overall security posture. The findings provided evidence to support cost reductions in endpoint technologies, correct alerting gaps to the SIEM and deliver improved executive reporting through a third-party analytics platform.

67% EXFILTRATION TECHNIQUES AND TACTICS WERE SUCCESSFUL 67% OF THE TIME.

DATA EXFILTRATION

Data leakage and protection remains a top concern for CISOs, but exfiltration techniques and tactics were successful 67% of the time during initial testing.



Common Causes

- Unknown fail-open conditions in security controls
- Lack of SSL inspection
- Misconfiguration of existing security controls
- Under-resourced sandboxing technologies or outdated signatures

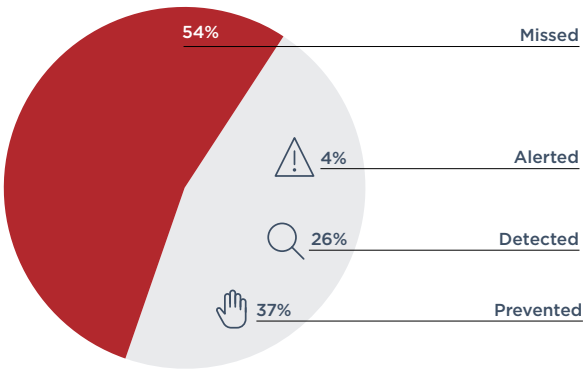
Example

A Fortune 1000 company testing data loss prevention (DLP) policies and the ability to stop data leakage observed that its next-generation firewall was not blocking techniques used to exfiltrate data. Security validation exposed the gap and identified the misconfigured device. Further analysis showed that the firewall vendor disabled detection capabilities in the latest release without making it widely known to customers. With this new awareness, the company reconfigured firewall policies and restored detection, prevention and alerting capabilities.

54% OF THE TECHNIQUES AND TACTICS USED TO EXECUTE TESTING OF LATERAL MOVEMENT ARE MISSED.

LATERAL MOVEMENT

Lateral movement is an essential tactic to infiltration of a network. Fifty-four percent of the techniques and tactics used to execute testing of lateral movement are missed, and 96% of the behaviors executed did not have a corresponding alert generated in the SIEM.



Common Causes

- Network segmentation misconfiguration
- Lack of internal security control points—inside network traffic is not monitored the same way
- Inability to distinguish administrative behaviors from malicious activities

Example

A large private healthcare provider had concerns about APT41, a specific actor reported to be actively targeting the healthcare industry. Leveraging security validation with integrated threat intelligence, the company discovered that its network security controls did not detect or prevent known techniques and tactics associated with attacks used by APT41. This exposed the company to dual espionage, criminal activity and over 46 different malware families. The testing results enabled the team to proactively optimize their controls and ensure they were prepared to defend against this adversary.

How to Improve Security Effectiveness

CONTINUOUS VALIDATION

PRIORITIZE
Prioritize what you are going to measure based on relevant and timely cyber threat intelligence

MEASURE
Measure where you are today

OPTIMIZE
Optimize your environment as informed by the identified gaps

RATIONALIZE
Rationalize your portfolio and processes to eliminate redundancies

MONITOR
Monitor your environment continuously against a known good baseline

Organizations often state that before using controls testing and configuration validation platforms, they had to answer these questions:

How effective are my security controls?

- How quickly can I assess the relevance of threat intelligence or my exposure to a likely attack?
- How well do I stop data leakage and protect data integrity?
- How can I simplify and standardize my security stack?
- What evidence can I provide with key security metrics for my executives?

Security validation can quantify the actual effectiveness of security controls because it provides continuous monitoring of unexpected changes or drift in underlying infrastructure that may impact the performance of security controls. As a result, you can gain the information you need to proactively outmaneuver attackers.

Effective cyber security requires implementing an enterprise platform that automates the key fundamentals of continuous security validation in order to maintain a strong defensive posture and proactively reduce risk.

To improve cyber security effectiveness we recommend the implementation of automated processes for continuous security validation.

Fundamentals of Security Validation

Adversary Coverage

- Tests on both adversary techniques and technical attacks
- New content delivered quickly as threat actors evolve
- Coverage across adversary attack vectors—email, endpoint, and network
- Customizable content to maximize test relevancy for your organization

Validation Automation and Outcomes

- Infrastructure discovery and visibility
- Continually tests efficacy at scale
- Ability to execute an attack once or on a periodic and continual basis
- Exercises external and internal security controls across all network paths and directions
- Graphical dashboards of the results of security effectiveness validation

Business Metrics

- Provides metrics to assess business risk and value of investments

Enterprise Readiness

- Proven in large complex environments
- Backed by a global support team and customer success program
- Deploys safely in live production environments
- Deploys on-premises or in the cloud and available as customer managed, co-managed, or fully managed

Conclusion

Companies are at much greater risk than they realize. As organizations—from the C-suite and board of directors down to those on the front lines of cyber defense—struggle to strengthen cyber hygiene and minimize risk, it has become imperative that organizations validate security effectiveness.

Organizations make significant investments in security infrastructure, hire and train teams and put processes in place to protect critical assets. But our research shows that without evidence of security performance, those organizations are operating on assumptions that don't match reality and leave them with significant risk.

The best way for your organization to combat this disconnect is to validate the effectiveness of your security program through ongoing, automated assessment, optimization and rationalization. This will enable you to minimize cyber risk across your entire organization by protecting not only critical assets but also brand reputation and economic value.

To learn more about Mandiant Solutions, visit: www.FireEye.com/mandiant

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®