Positive Technologies MultiScanner

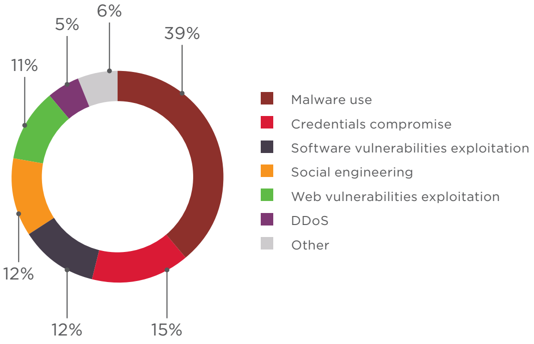
DATA SHEET

POSITIVE TECHNOLOGIES

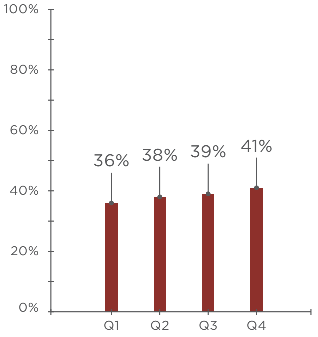
Damage from malware attacks in 2017 exceeded USD $1.5 billion.[1]

MALWARE: THREATS AND CHALLENGES FOR BUSINESS

Attacks using malware top the list of common cyberthreats, accounting for 39 percent of all attacks in 2017.



Methods used in 2017 attacks



Percentage of attacks featuring use of malware in 2017, by quarter

According to Positive Technologies estimates, one out of ten organizations was hit by ransomware in 2017.

Attackers are increasingly aggressive and indiscriminate in their targets. Malware tends to strike as many systems as possible and inflict maximum damage, as happened with NotPetya and WannaCry ransomware. The malware often does not even have the ability to decrypt the victim's data. Even worse, it can spread around the world in hours.

Under the growing "ransomware as a service" model, anyone willing to pay can obtain access to professionally written ransomware. As a result, the barrier to entry for cybercriminals has dropped dramatically. Now attackers without technical skills can find what they need on the dark web to start shaking down victims.

Why are these attacks so common and so destructive? Based on years of experience in investigating security incidents, we have identified a few of the key factors in why companies are unable to defeat malware.

Vendor delays in updating antivirus knowledge bases.

Approximately 250,000 samples of malware are generated every day. But how long does it take for a new threat to be recognized by antivirus products? This process can take from a few days to several weeks, during which the consequences could be catastrophic. Depending on a single antivirus vendor is risky: how do you know that your antivirus vendor will be the first to react to every new threat?

Incomplete antivirus coverage of corporate endpoints.

In penetration testing and incident investigation in 2017, our experts found that antivirus coverage at large companies hovers around 85 percent of systems, on average. Major contributors to the problem include company size and remoteness: security may be strictly enforced at headquarters, but conditions and budgets tend to be worse out in the field. In addition, only a few companies regularly check their workstations to make sure that antivirus protection is running on them. Companies usually don't even own software that can automatically check whether antivirus protection is installed on a particular computer.

[1] "Cybersecurity threatscape 2017: trends and forecasts" (Positive Technologies report)

Gaps in antivirus coverage are one of the key factors that enabled the ransomware rampage of 2017.

According to Positive Technologies estimates, one out of ten organizations was hit by ransomware in 2017.[2]

Migration to the cloud.

Finance, insurance, and telecom companies, as well as governments, increasingly offer services online: clients can fill out forms and request services via the web or email. By the same token, these services make companies vulnerable. After all, the same forms that allow clients to upload files can also be used by attackers to upload malware.

Advanced persistent threats specially designed to evade specific antivirus products.

Even good antivirus protection may not be enough to stop a determined attacker. For example, government agencies must publish procurement records online, making it easy to figure out which antivirus software they use. Attackers then develop malware that is designed to evade detection by that particular product. These attacks can remain unnoticed for a very long time. This threat is becoming increasingly acute, with half of major companies falling victim to targeted attacks in 2017.[2]

No visibility on cross-network malware movement.

Reacting to a threat or investigating an incident requires reconstructing how malware has spread on the victim's infrastructure. This information can be obtained partially from the IPS, IDS, or DLP systems in place at most companies. But these systems are being asked to perform a job they are not designed to do, in a way that requires meticulous configuration and excessive effort.

Reckless use, or underuse, of cloud scanners.

Cloud-based cross-scanning services are convenient, offering a free way to scan suspicious files with dozens of antivirus engines. But carelessness can have dangerous consequences. Unaware employees often upload confidential data to these external sites for scanning. As a result, such data may even end up in the hands of attackers, who can use this information for planning and preparing hacks (including with malware).

On the other hand, banning use of such services has a big downside. If the company does not have antivirus protection, or protection is poor, employees are less likely to detect malware before it infects company infrastructure.

Difficulty of juggling diverse protection solutions.

When different anti-malware solutions are in use, the difficulty of managing them rises exponentially. Manually going through scan reports in different formats creates busywork for security staff and impedes timely, targeted threat response.

Low security awareness by employees.

As shown by our research,[2] only 25 percent of companies train and test their employees in security. Yet humans are often the weakest link in the security chain. Just one click on a suspicious link or boobytrapped attachment can mean a compromise of the entire network.

The solution to these problems starts with PT MultiScanner, which offers centralized protection from malware and full-infrastructure data coverage.

[2] Positive Research 2018 (Positive Technologies report)

PT MULTISCANNER: KEY FEATURES

PT MultiScanner is a multilevel system for protection from malware that detects and blocks threats across the data flows of a company's infrastructure.

PT MultiScanner advantages

Security expertise in practice

PT MultiScanner scans objects by combining the strengths of multiple methods: multiple antivirus engines by different AV vendors, static analysis and reputation lists from the Positive Technologies Expert Security Center (PT ESC), which regularly investigates critical security incidents at major companies. The solution supports scaninng for both files and archives, including recursively compressed.

Full coverage of all data flows

PT MultiScanner can identify and block malware threats across connection types: web portals, file storage, network traffic, web traffic, and email (with an attachment sanitizing for most common file extensions, such as .docx, .xlsx, .rtf, .pptx, .pdf, .html, .jpg, .zip, etc.).

Retrospective analysis

PT MultiScanner detects the latest threats and signs of hidden malware with the help of retrospective analysis. Previously scanned objects are rescanned automatically after updates to the knowledge base or when resources are available, without any performance hit to ongoing scanning.

Expert tool for incident investigation

Security operations center (SOC) and security staff will find PT MultiScanner an effective tool for investigating incidents: it can detect malware points of entry into infrastructure, pinpoint relevant users, and identify all stages of malware spread.

Ease and convenience

Centralized monitoring of malicious activity across all data flows makes it easy to track and localize threats on corporate infrastructure. Similar attack elements across diverse data flows are linked into a single threat chain, helping security staff to react more quickly and precisely.

Intuitive interface makes all information readily available to security staff in at-a-glance dashboard form.

PT MultiScanner deploys in less than one hour. Adding scan sources (mail services, proxy servers, file storage, network sensors) takes just a few clicks.

More benefits

+ PT MultiScanner supports all the important standard interfaces (SPAN, MTA, BCC, ICAP, REST API).
+ Scale-as-you-go by adding components.
+ All files are scanned within the system on local storage; files never leave the company perimeter (on-premise scanning).
+ PT MultiScanner fits perfectly into the ecosystem of Positive Technologies products.

"Now that policyholders themselves can upload documents to our online service, the odds of encountering malicious files have risen enormously. So one of our team's jobs is to quickly detect and block any such viruses. That is why we chose PT MultiScanner from Positive Technologies."

Andrei Polomoshnov,
Head of Information Security Operations at Ingosstrakh insurance company

"We know how high the risk of malware is at a large company like VGTRK. To meet this threat, we needed a reliable, yet very flexible, solution that could be adapted to our needs. These qualities drew us to PT MultiScanner, a product that combines the deep expertise of Positive Technologies with the experience offered by antivirus vendors. With PT MultiScanner, we've finally solved the problem of antivirus protection at our company."

Dmitry Safronov,
Head of Information Security, VGTRK

PT MULTISCANNER DEPLOYMENT: GOALS AND METHODS

Goals

- Protect from malware across all data flows on company infrastructure.
- Better investigate malware incidents.
- Strengthen company security stance.
- Promote security awareness by users.

Methods for accomplishing these goals

- Monitor malicious activity at the network level.
- Scan objects with multiple antivirus engines, static analysis, and reputation lists.
- Inform users and security staff of threats as they are detected.
- Block malicious content.
- Maintain a knowledge base of all downloaded objects, metadata, and verdicts, plus history of network movements.
- Perform retrospective analysis and notify if malware is detected in previously downloaded objects.
- Analyze scan results, generate statistics, and provide reporting.

Integration

The system supports standard interfaces: SPAN, MTA, BCC, ICAP, and REST API.

SPAN

PT MultiScanner has built-in support for integration with network devices supporting traffic mirroring (SPAN) and can analyze objects sent over the HTTP, SMTP, POP3, IMAP, FTP, and SMB protocols.

MTA

PT MultiScanner can identify and block malware in email traffic. To do this, a lightweight mail transfer agent (MTA) is installed on the company's mail server to pass messages and their attachments to PT MultiScanner for scanning. PT MultiScanner gives its verdict, which is implemented as a decision to allow or block the message.

BCC

PT MultiScanner can scan emails and attachments by means of BCC integration with the company email server. In this case, the mail server sends a copy of incoming messages to PT MultiScanner while simultaneously delivering the messages to their recipients. This option does not enable blocking malicious messages, unlike MTA integration.

ICAP

PT MultiScanner can scan all files passing through proxy servers, web application firewalls (WAF), intrusion detection and prevention systems (IDS/IPS), and any other products with ICAP support.

REST API

PT MultiScanner integrates with network devices, protection solutions, and internal corporate systems via the standard HTTP REST API.

Scalability and high availability

The architecture of PT MultiScanner is perfect for scaling both vertically and horizontally. It is fully fit for cluster deployment in active–active configuration with one central management console.

Form factors

PT MultiScanner can be installed on a physical server or virtual machine.

HOW IT WORKS: PT MULTISCANNER SUBSYSTEMS

Scanning subsystem

Scans objects received from various sources.

Sources of objects:

- Mail servers
- Proxy servers
- File storage via NFS, FTP, SMB
- Mirrored network traffic
- On-demand verification services (via web portal or email)
- Other sources (via API requests)

Each file is scanned with several antivirus engines. These results are combined with information from the Positive Technologies knowledge base to make an overall verdict.

After scanning is finished, the object, its metadata, and information about scanning is passed to the Management and Storage subsystems. If a threat is found, information is also sent to the Threat Management subsystem.

Storage subsystem

Stores files and their metadata. This information is needed when rescanning objects after an update of antivirus signature databases or reputation lists.

All objects are stored locally with reversible encryption. The subsystem supports wiping such objects based on data rotation settings.

Data collected by the Storage subsystem:

- Date and time of scanning
- Object metadata (size, name, and MIME type)
- Hash value
- Object source (type, address, protocol, message, ICAP request, API request parameters, network node, User-Agent/Referer header, etc.)
- Antivirus engines used for scanning (name, engine version, signature database version, scanning result)

The Storage subsystem allows performing the following actions with scanned objects:

- Search by name, source, and malware type
- Filter results by one or more object attributes
- Download objects from storage
- Add comments and tags
- View general information (hash sums, size, MIME type, source, and download date)
- Add to whitelist or blacklist
- View full scanning history and statistics of retrospective scanning

Retrospective Analysis subsystem

Rescans previously scanned objects after antivirus signatures or reputation lists have been updated. If the verdict for an object changes based on retrospective analysis, the threat is flagged and notification is sent to security and IT staff.

Threat Management subsystem

Aggregates threats and allows managing their lifecycle. Close and reopen threats or groups of threats. Navigate and filter threats based on attributes of threats and relevant objects.

Monitoring subsystem

Monitors the state of all subsystems, informs the user of current functioning of the system via the web interface, and restarts subsystems if errors arise. It also checks for updates from Positive Technologies and, if they are found, initiates the update process.

Management subsystem

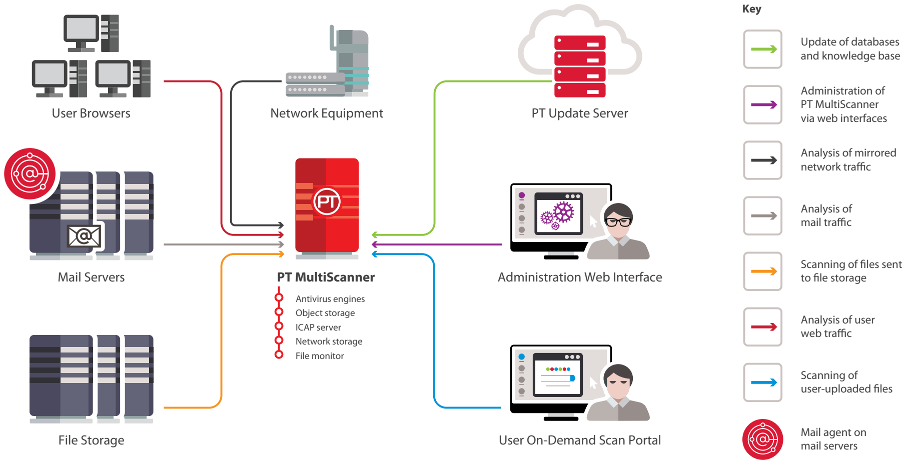
Manages user access and roles in the system with identification and authentication based on username and password.

Add, change, and remove sources of objects for scanning. View and manage threats, objects, and reputation lists. Adjust system settings.

PT MULTISCANNER MODES

Mode	Purpose	Object sources
Manual (on-demand) uploading	Scan suspicious objects flagged by users	+ User web portal + Dedicated email address
Traffic scanning	Find malware and notify security staff of any threats in traffic	+ Corporate traffic mirrored from network equipment (SMTP, HTTP, POP3, IMAP, FTP, and SMB protocols) + Mail agent (installed on the corporate mail server) passes on messages for scanning + Corporate mail server sends message copies for scanning + WAF, IDS, IPS, and proxy servers + File storage (NFS, FTP, SMB)
Traffic scanning and blocking	Find malware and stop its spread on infrastructure; notify security staff of any threats in traffic	+ Mail agent (installed on the corporate mail server) passes on messages for scanning and blocks malicious messages + WAF, IDS, IPS, and proxy servers + File storage (NFS, FTP, SMB)

USAGE SCENARIOS


User Browsers
Network Equipment
PT Update Server
Mail Servers
PT MultiScanner
Antivirus engines
Object storage
ICAP server
Network storage
File monitor
Administration Web Interface
File Storage
User On-Demand Scan Portal
Key
Update of databases and knowledge base
Administration of PT MultiScanner via web interfaces
Analysis of mirrored network traffic
Analysis of mail traffic
Scanning of files sent to file storage
Analysis of user web traffic
Scanning of user-uploaded files
Mail agent on mail servers

PT MultiScanner illustration

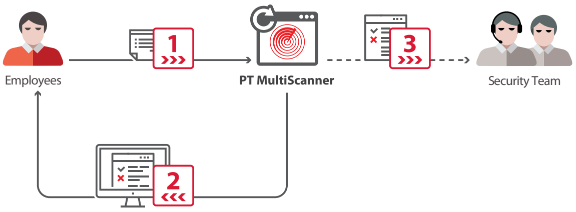
In this scenario, threats trigger notifications but are not blocked.

User web portal (on-demand)

PT MultiScanner can be used to create a local user service (web portal). Users manually upload files for scanning and view the verdict via a web portal.

What happens:

1. An employee uploads a file or archive, whether downloaded online or from an external disk, to PT MultiScanner via a web portal.
2. PT MultiScanner runs an antivirus scan and checks reputation lists. The verdict is given to the user directly on the web portal.
3. If malware is detected, PT MultiScanner automatically informs security staff.



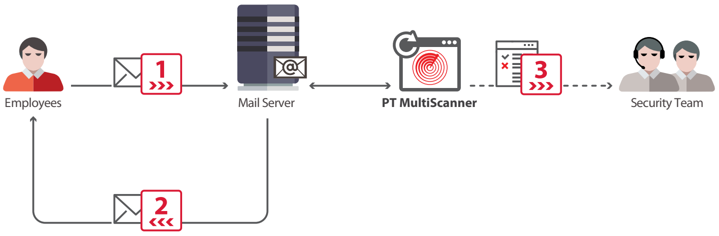
User email scanning (on-demand)

In case of a suspicious file, users can manually forward the message to a special PT MultiScanner email address at the client company.

In this scenario, threats trigger notifications but are not blocked.

What happens:

1. An employee sends a file or archive, whether downloaded from the Internet or copied from an external disk, for scanning by PT MultiScanner at a special email address.
2. PT MultiScanner scans for viruses and checks reputation lists. The verdict is returned to the user as an email reply.
3. If malware is detected, PT MultiScanner automatically informs security staff.

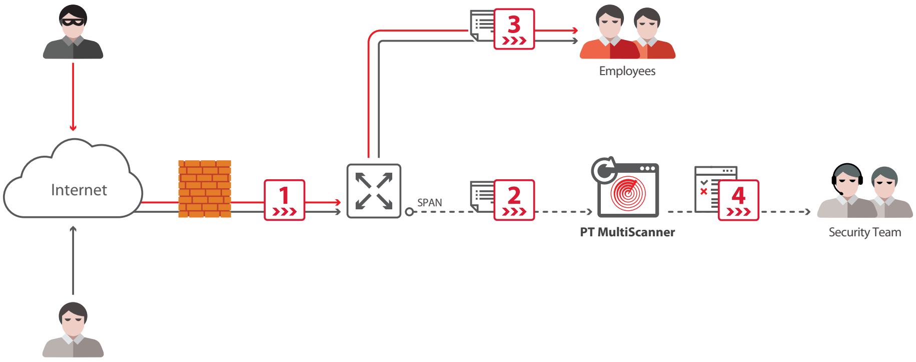


Traffic monitoring

In this scenario, threats trigger notifications but are not blocked.

What happens:

1. PT MultiScanner scans mirrored traffic routed through SPAN-enabled network equipment. With no network performance penalty, objects are checked with antivirus scanning and reputation lists. Protocols supported: SMTP, HTTP, POP3, IMAP, FTP, SMB.
2. If malware is detected, PT MultiScanner automatically informs security staff.



This scenario can be implemented in two ways: with or without blocking of malware.

In this scenario, PT MultiScanner is integrated with PT Application Firewall from Positive Technologies.

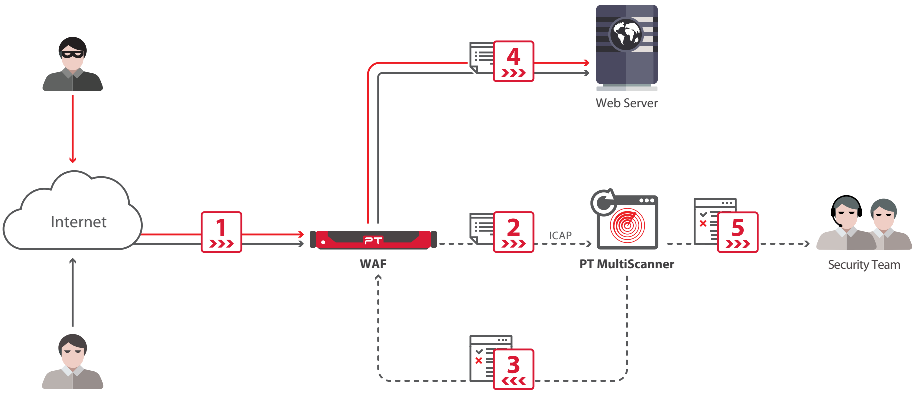
Protection of web applications and portals

PT MultiScanner can be used to protect web applications and portals from malware attacks, when used in tandem with a web application firewall (WAF). Integration is achieved using the ICAP protocol.

What happens:

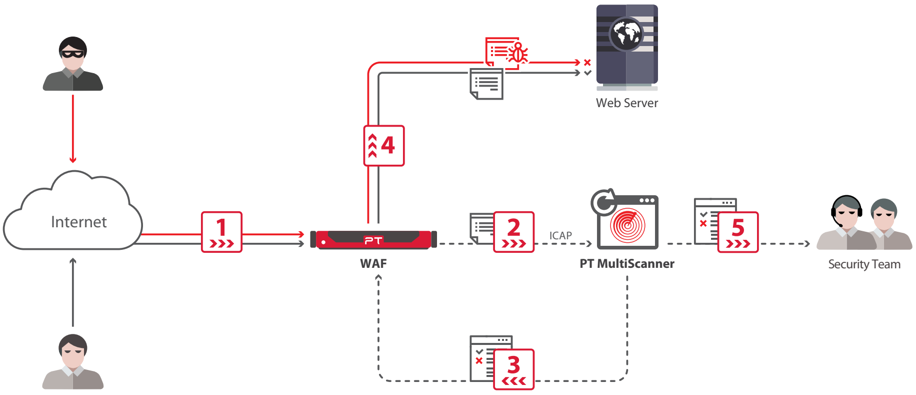
1. All incoming traffic to the web server is checked by the WAF.
2. Attachments contained in this traffic, together with information about their source, are passed by the WAF to PT MultiScanner.
3. After scanning, PT MultiScanner returns the verdict to the WAF.

…if blocking is disabled



- Traffic is received by the web server from the WAF.
- If malware is detected, PT MultiScanner automatically informs security staff.

…if blocking is enabled



- If no threat is present, traffic is passed by the WAF to the web server. If a threat is found, the malware is blocked and PT MultiScanner automatically informs security staff.

User web traffic scanning

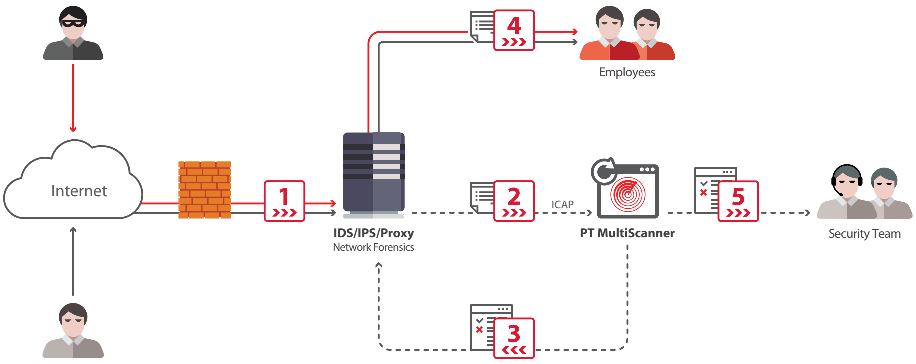
PT MultiScanner offers a way to boost the security of the network perimeter by means of integration with traffic monitoring and analysis tools, such as intrusion detection and prevention systems (IDS/IPS), proxy servers, and other ICAP-compatible solutions.

This scenario can be implemented in two ways: with or without blocking of malware.

What happens (with proxy server):

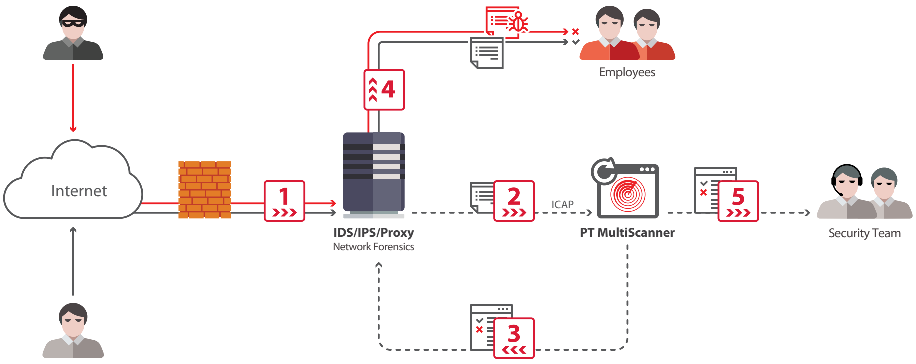
1. A user downloads an object from the Internet and, in so doing, initiates the download via a proxy server.
2. After the object is downloaded, the proxy server passes a copy to PT MultiScanner, together with information about the user and download source.

…if blocking is disabled



- After scanning, the verdict is returned to the proxy server, which delivers the object to the user.
- If malware is detected, PT MultiScanner automatically informs security staff.

…if blocking is enabled



- If no threat is present, the object is delivered to the user. If a threat is found, the malware is blocked and PT MultiScanner automatically informs security staff.

This scenario can be implemented in two ways: with or without blocking of malware.

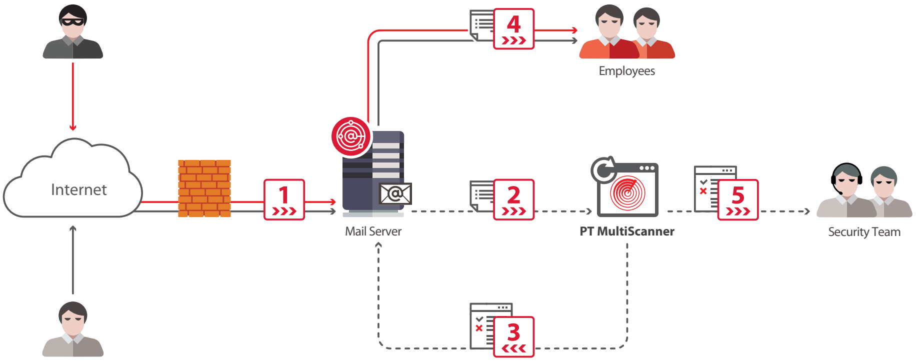
Attachment scanning

PT MultiScanner can be integrated with mail servers to identify and block malware in email attachments.

What happens:

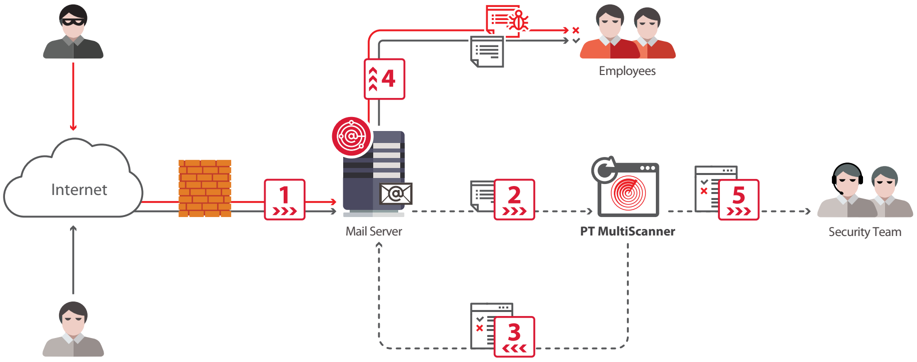
1. A message with an attachment is received by the mail server.
2. PT MultiScanner receives the attachment plus information about the message (From, To, CC, and Subject fields).
3. PT MultiScanner scans the object and returns a verdict.

…if blocking is disabled



+ The mail server delivers the email and attachment to the recipient.
+ If malware is detected, PT MultiScanner automatically informs security staff.

…if blocking is enabled



+ If no threat is present, the message is delivered to the recipient. If a threat is found, the malware is blocked and PT MultiScanner automatically informs security staff.

File storage scanning

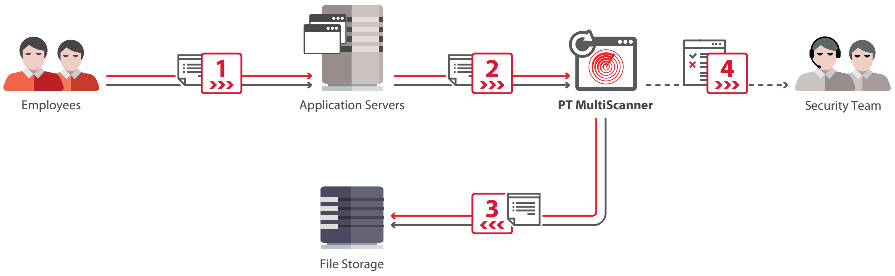
PT MultiScanner can be used to detect and block malware on corporate file storage.

This scenario can be implemented in two ways: with or without blocking of malware.

What happens:

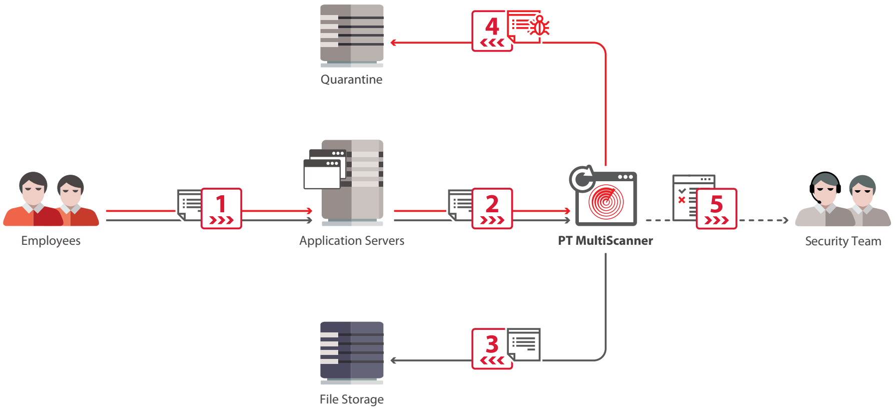
1. A user places an object on a corporate network resource.
2. PT MultiScanner, monitoring the resource in question, initiates scanning of the new object and identifies any malware.

…if blocking is disabled



- The object is saved to the corporate network resource.
- If malware is detected, PT MultiScanner automatically informs security staff.

…if blocking is enabled



- If no threat is present, the object is placed in the user-specified folder. If malware is found, the object is placed in quarantine and PT MultiScanner automatically informs security staff.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com