This whitepaper has been prepared in consultation with Technology Law Firm, Fieldfisher.

It is intended to provide helpful and informative material but should not be relied upon as constituting legal advice on the part of Trend Micro or Fieldfisher. You should always seek your own, independent legal advice where necessary.
Trend Micro SaaS Security Solutions for GDPR Compliance:

Deep Security as a Service White Paper

Introduction

As a leader in security, Trend Micro has always taken data privacy and protection very seriously. Trend Micro operates in over 50 countries around the world and it works diligently to ensure compliance with regional data protection regulations. Trend Micro solutions are also used by organizations around the world - including Trend Micro’s own infrastructure - to protect sensitive user and corporate information from the escalating number and sophistication of attacks happening today.

Trend Micro Deep Security™ as a Service, a software-as-a-service (SaaS) offering, provides a single platform for server security to protect physical, virtual and cloud servers, as well as hypervisors and virtual desktops.

This white paper outlines how Deep Security as a Service can be used to help with our customers’ compliance with the EU General Data Protection Regulation (GDPR) and how it should be used in a compliant manner with the GDPR. The document also details how Deep Security as a Service itself adheres to the GDPR principles.

The GDPR

The GDPR took effect throughout the European Union on 25 May 2018. It changes the privacy and security landscape not only in the EU but also globally, as it seeks to extend its extra-territorial reach outside the EU.

The GDPR regulates the "processing" of "personal data":

- "Processing" means any activities performed on personal data and includes storing or receiving personal data, such as, in emails identifying security threats.

- "Personal data” means any information relating to an identified or identifiable living individual, such as contact information.

  Note: "personal data" is much wider than the US concept of "PII" or "personally identifiable information". Data that would not be considered PII could be considered personal data, such as IP addresses or device identifiers.

The GDPR applies to both:

- controllers, who decide the "why and how" of processing personal data; and

- processors, who are engaged by controllers to host, analyze or process personal data for them.

Under the GDPR:

- Security – organizations must implement appropriate technical and organizational measures to protect personal data, including appropriate security measures. Breach of these security requirements could subject controllers to regulatory fines of up to 4% of total annual turnover.
or (if higher) €20 million, and for processors, up to 2% of total annual turnover or (if higher) €10 million.

- **Data protection by design and by default** – controllers must build data protection, including security, both when designing and implementing their systems and processes and when processing personal data. Infringement of this requirement could expose the organization to a fine of up to 2% of total annual turnover or (if higher) €10 million.

- **Personal data breach notification** – controllers must notify personal data breaches to regulators without undue delay and within 72 hours where feasible, while processors must notify their controllers without undue delay. Controllers must also notify the affected individuals of "high risk" personal data breaches. Fines for non-notification could reach 2% of total annual turnover or (if higher) €10 million.

State of the art security and the ability to **detect and report on threats** are therefore important factors for data protection under the GDPR.

**What is Deep Security as a Service?**

Deep Security as a Service secures servers (physical, virtual, or cloud workloads), as well as hypervisors and virtual desktops and helps protect what customers put in the cloud (operating systems, applications and data) through a wide range of host-based security controls. It provides a complete suite of security capabilities including:

- malware prevention with web reputation, predictive machine learning and optional sandbox analysis;
- network security with intrusion detection and prevention (IDS/IPS) and firewall; and
- system security with integrity monitoring, log inspection and multi-platform application control.

Deep Security as a Service is hosted in the cloud, leveraging Amazon Web Services highly secure infrastructure.

Deep Security as a Service enables the protection of all workloads with a single, multifunction agent (the "Deep Security Agent") that both secures the workload and communicates information to a central dashboard for each customer. The Deep Security Agent is responsible for enforcing policies for all capabilities and is controlled by the central Deep Security Management Console.

Deep Security administrators log into the central dashboard on the Deep Security Management Console to manage all aspects of the services including policy management, incident management, enforcement point (Deep Security Agent) deployment and reporting.

Deep Security as a Service is a fully segmented multi-tenant offering, allowing each customer to have a separate management environment for policies and events.
How does Deep Security as a Service work?

As it is a SaaS application, Deep Security as a Service is configured and managed through a secure web console. It has been optimized for use with VMware, AWS and Microsoft Azure but also works with a number of other cloud providers and can protect physical workloads.

When a customer signs up and creates their own account, seamless integration with the customer's cloud provider(s) is achieved by creating new permissions to give Deep Security as a Service access to see the customer's instances, images and tags. Protection of workloads in the data center is simply achieved by the deployment of Deep Security Agents to servers (physical, virtual or cloud workloads) as well as hypervisors and virtual desktops.

On logging into their own account, customer administrators can view a comprehensive overview of their security status and events across all workloads and environments. In the central dashboard, administrators can also implement and manage policies to replicate security settings (e.g. firewall rules, vulnerability shielding, system integrity and alert generation) to workloads that share similar security requirements (example groupings include, by operating system, server function or application installed/version).

Deep Security as a Service uses a single Deep Security Agent that is installed on each workload to enforce security settings based on policies set via the dashboard in the Deep Security Management Console. Deploying the Deep Security Agents on a customer's instance is easy; they are either baked into the customer's cloud provider template or can be launched dynamically using a deployment script. If the customer has configuration management tools, these scripts can be added to the deployment(s) or by using the built-in tools provided by the cloud provider platform.

A recommendation scan can also be performed on a workload, enabling the application of contextual policy within the bounds of group policy or individually.

Leveraging XGen™ security to deliver a cross-generational blend of advanced threat defense techniques, Deep Security as a Service can deliver the following capabilities:

Anti-malware

- Filters and blocks all known malware with information from the Trend Micro™ Smart Protection Network™ (SPN), Trend Micro's cloud-based threat intelligence network. The SPN uses a global network of millions of threat intelligence sensors to identify threats before they reach the customer and blocks them with Deep Security as a Service.
• Deep Security as a Service uses advanced machine learning and behavioural analysis techniques to discover unknown threats and block them. Newly discovered threats are shared with the SPN in an anonymized or pseudonymized way.

• If Deep Security as a Service detects a suspicious or unknown file it will record related information in an anti-malware event log.

• If a customer has purchased Trend Micro™ Deep Discovery™ (Deep Discovery) and configured Deep Security as a Service to use it as a sandbox:
  o the suspicious or unknown file will be downloaded to the customer’s data center and analyzed in the sandboxed environment. Again, using advanced techniques like machine learning and behavioural analysis techniques, the sandbox can analyze against multiple customized environments designed to match the real operating environments;
  o to ensure the malware detonates in the sandbox, the product uses industry-leading anti-evasion techniques such as mouse movements and accelerated time environments; and
  o once the risk of the detected file has been assessed, Deep Discovery then passes the information back to Deep Security as a Service for action: allow, isolate (quarantine), clean, deny access or delete, if appropriate.

Web Reputation

• URL filtration capability used to help detect botnet command and control traffic or lock down access to approved sites only.

Bidirectional Firewall

• Decreases the attack’s surface by creating a firewall perimeter to block attacks.

• Limits communication to the necessary ports and protocols only.

• Centrally manages server firewall policy, including templates for common server types.

• The customer can control traffic access (and block attacks) through the creation of firewall rule actions. Other functions available include using the stateful filtering engine to inspect and validate each packet on an individual basis (enabling protection against attacks such as denial of service) or using interface isolation to force a computer to use only one interface at a time (preventing attackers from bridging across two interfaces).

Intrusion Detection System / Intrusion Prevention System (IDS/IPS)

• Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack.

• Includes a collection of rules that can be applied to stop threats, shield systems from vulnerabilities, and detect suspicious behaviour that may indicate an attack.

• Uses protocol enforcement technologies to protect against a wide range of attacks including web application attacks (e.g. sequel injection and cross-site sequencing).
Integrity Monitoring

- Provides the ability to track both authorized and unauthorized changes made to a protected workload (files, registries, ports) and enables the customer to receive alerts about unplanned or malicious changes, which can be a good indicator that something suspicious has occurred and should be investigated.

- Customers can easily configure what they want to monitor, leveraging included rules or creating custom rules that use event tagging to replicate actions automatically for similar events.

Log Inspection

- This automated tool collects, analyzes and reports on the operating system and application logs for cases of serious security risk.

- Assists with compliance (e.g. PCI DSS) by providing audit trails of security events across multiple products and systems.

Application Control

- Monitors changes to a computer's original software and gives administrators the ability to lock down systems to run approved applications only or ensure no new applications can run without first being whitelisted.

- If enabled, all software changes are logged and events are created when changes in software are detected.

Events and Reports

- Rich reporting features are embedded in the Deep Security Management Console with the ability to report on security modules as well as security and system events.

Deep Security as a Service Communication and Data Access

Customers connect to Deep Security as a Service via HTTPS connections. Generally, communications between Deep Security as a Service and other internal and external components are achieved via HTTPS connections and TLS.

Anti-malware

- If an infected file is discovered (one that has been found to be, or to contain, malware), specific actions are taken based on customer-configured policy. For example, if the anti-malware policy dictates that the next action is to quarantine the file, the file is encrypted and moved to the quarantine directory on the customer's computer. Once quarantined, the file can be downloaded to a location of the customer's choice.

- For the optional use of an on-customer-premise Deep Discovery sandbox, files for evaluation are sent over HTTPS to the sandbox for analysis. Results from the analysis are shared with Deep Security as a Service via HTTPS for policy-based action.
IDS/IPS

- If configured by the customer in the Deep Security Management Console, this module can send IP information to a Whois service to look up the domain name associated with an IP address tied to an intrusion prevent or firewall event. However, Trend Micro has no access to this data processing activity as the data is sent directly from the customer's network to a configured Whois server.

Web Reputation

- The web reputation module uses the SPN to determine whether URLs are malicious. Information is sent in anonymized or pseudonymized form.

Log inspection

- The log inspection module can be configured to forward suspicious events to the Deep Security as a Service SIEM system or centralized logging server for correlation, reporting and archiving.

Email alerts

- Email alerts and reports sent from Trend Micro to customers are sent encrypted with TLS via the AWS e-mail service to the customer e-mail infrastructure. Customers also have the option to encrypt reports generated by the service with a chosen password.

Security events

- Generally, when a security module is enabled and a rule or condition is triggered (a "security event") occurs, information about the event is recorded in the service and available to the customer for access. Security event information can include intrusion prevention packets, URL reputation, firewall packets, log entry, malware file and IP addresses. Security event information is retained in Deep Security as a Service for 32 days and a back-up is retained for a further 35 days. If the customer requires a longer retention period, it can export events to an external SIEM using a communication channel secured with TLS via syslog protocol or AWS SNS. Please see Appendix 1 for more details.

Customer Tenant System events

- Deep Security as a Service records when administrative or system-related events occur (a "system event"), such as, software updates. System event information is retained in the service’s audit information for 13 weeks and a back-up is retained for a further 35 days. If the customer requires a longer retention period, it can export events to an external SIEM or syslog.

- Access to the service’s system events is restricted to the Deep Security as a Service operations team, using 2-factor authorization and such access is reviewed on a periodic basis. A System event log records general logging data and can be viewed by the Deep Security as a Service operations team for troubleshooting for 13 weeks, after which time it is stored in Amazon S3 for a minimum 1 year period to satisfy compliance requirements.

Audit information

- A range of other audit information can be maintained by Deep Security as a Service to record security and system events. The information is stored in the Deep Security as a Service SIEM
and is used for troubleshooting, monitoring and overall protection of the system. Access to tenant specific and environment auditing information is available to the Deep Security as a Service operations team. For more information about the data retained and accessed in the audit information, please see Appendix 1.

**Trend Micro team communication and data access**

- In addition to involvement with email alerts and access to system and security events and audit information described above, Deep Security as a Service support staff may sign into tenant accounts in response to a support case, with the customer being aware that support access is required.

- The Deep Security as a Service operations team may also access customer databases hosted in AWS RDS or sign into tenants’ accounts, in order to perform maintenance operations, without requiring customer consent. Such access activities are logged and formally reviewed by Trend Micro.

- Tenant access by Deep Security as a Service operations and support staff is logged into the tenant system event log.

- Trend Micro does not have access to data on workloads protected by Deep Security as a Service.

**Caches**

- Caches do not store customer information. They store heartbeat requests coming from the Deep Security Agents, which only contain agent identifiers.

**What personal data may be involved when using Deep Security as a Service, and how?**

In the activities described above, Deep Security as a Service may process personal data. For example, when a security or system event takes place, some of the information processed will constitute personal data such as IP addresses. The logging data created by Deep Security as a Service may also contain personal data such as administrator names and IDs.

**Data processing roles**

The customer is the controller, and Trend Micro is the processor, of personal data processed using Deep Security as a Service.

The reason why the customer is acting as the controller is that they are able to retain control over what Deep Security as a Service can access and how; the personal data processed by Trend Micro in or from Deep Security as a Service is strictly performed in accordance with the instructions the customer provides using the service system settings. For example, the customer:

- is able to enable or disable security modules and consequently, a security event will/will not be generated; or

- decides which of their users can access the Deep Security Management Console as administrators or otherwise and determines what rules and policies to apply, includinghow the service enforces policies for specific groupings.
See the Deep Security as a Service Data Collection Notice for further details about the Deep Security as a Service features which collect and transmit data and how the customer can control these features https://success.trendmicro.com/solution/1119904.

Trend Micro’s role

As a processor for customers, Trend Micro is required by the GDPR to maintain appropriate security for the personal data processed for its customers. Trend Micro has other obligations, such as, including certain minimum terms in customer contracts and in relation to the use of subcontractors/subprocessors.

Security

Trend Micro maintains strong physical, organizational and technical security measures, and ensures segregation and isolation of different customers' data:

- Deep Security as a Service is certified as ISO 27001:2013 compliant.
- The Deep Security as a Service operations team undertakes regular scans of the service to identify any vulnerable components and install updates. Members of the team are also on call 24x7 to respond to alarms set by the system.
- Trend Micro's InfoSec team also conducts system scans and continuous monitoring of audit events.
- Databases are backed up daily using AWS RDS snapshots for both security and continuity.
- Annual penetration testing is conducted by third party companies specializing in security audits.
- Deep Security as a Service is a certified PCI DSS Level 1 service provider.
- Certifications and security for the AWS hosting platform are relevant and available at https://aws.amazon.com/compliance/.
- All Trend Micro administrators who work with Deep Security as a Service are Trend Micro employees who have signed confidentiality agreements as a part of their employment contracts. For more information about employees' screening and security awareness, see https://www.trendmicro.com/en_us/about/legal/product-certifications.html.

Contract terms

- Trend Micro offers customers GDPR terms as a standard part of doing business, see https://www.trendmicro.com/en_us/about/legal.html. Trend Micro also has a process for implementing GDPR terms with relevant subcontractors.

Deletion of data

- If a customer terminates their Deep Security as a Service account, the database schema that contains their account information containing all the customer's account data is subsequently deleted as part of Trend Micro's maintenance operations. Inactive database pruning is scheduled on the last day of each month when databases for accounts that have been cancelled for more than 30 days are deleted.
• If the account database schema is not yet deleted a customer may restore a cancelled tenant by raising a support request with Trend Micro.

• Customers can remove protected workloads from Deep Security as a Service, as well as uninstall a Deep Security Agent, and thus stop generating events. Security events that have been generated by workloads up to the point of their removal will be purged after 32 days.

• Tenant administrator accounts, contact information and policies will be deleted from the active tenant database as soon as the customer removes them.

• Backups of the tenant databases are kept for 35 days and any data removed from the active database schemas will be completely deleted from Deep Security as a Service on expiry of this period.

Breach management

• Although Trend Micro has designed Deep Security as a Service not to collect personal data, if a personal data breach does happen, Trend Micro has a breach reporting plan to notify customers as necessary to meet breach reporting obligations under the GDPR and has also implemented 24x7 monitoring and incident response.

How can a customer use Deep Security as a Service compliantly with the GDPR?

The customer, as the controller, remains responsible for its obligations under the GDPR in relation to the personal data processed in Deep Security as a Service.

This includes:

• having a "legal basis" for the processing activities;

• complying with core GDPR principles;

• meeting transparency requirements incumbent on controllers;

• addressing individuals’ requests to exercise their GDPR rights; and

• complying with other obligations under the GDPR regarding security, data protection by design and by default and international transfers.

Establishing a legal basis for using Deep Security as a Service

Personal data cannot be processed without a recognized legal basis. Article 6 of the GDPR recognizes several legal bases one of which is legitimate interests (Article 6(1)(f)): "the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

Furthermore, Recital 49 of the GDPR explicitly acknowledges that the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, constitutes a legitimate interest of the controller concerned. It cites as examples, preventing unauthorized access to electronic...
communications networks, malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

In addition, EU privacy regulators have also noted, in a pre-GDPR opinion that still largely holds true today, that legitimate interests can extend to processing for physical security, IT and network security purposes (WP217 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf).

However, regulators (WP217) expect a "balancing test" to be conducted by the controller, to confirm that the processing is indeed necessary and proportionate for that legitimate interest, and is not overridden by individuals’ rights (i.e. not too privacy-intrusive). In this day and age, security services such as those provided by Deep Security as a Service are necessary, given the prevalent and increasing use of different channels for threats. The UK Information Commissioner has provided a "legitimate interests assessment" sample template at https://ico.org.uk/media/organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx which can be used by customers to perform and document the balancing test. To meet the balancing test, customers should carefully consider the policies, rules and controls they implement when configuring and using Deep Security as a Service, as well as the scope of their monitoring and security services, limiting the extent of the processing activities to what is necessary for security purposes and providing appropriate transparency to their end users.

Regulators recommend (WP249 http://ec.europa.eu/newsroom/document.cfm?doc_id=45631) considering mitigating actions to reduce the scale and impact of the scanning on end users, including undertaking a data protection impact assessment (DPIA) and implementing and communicating to end users appropriate monitoring policies as well as privacy notices. In some EU countries, employee works councils may have to be involved in relation to the policies.

Customers should also involve their data protection officer (if appointed) in their legitimate interest assessment and any DPIA.

Deep Security as a Service has been designed to incorporate safeguards that will assist in any legitimate interest assessment, such as ensuring that logs are only accessible to authenticated individuals over a secure connection and retention is for a defined, relatively short period of time.

Special categories of personal data

For processing "special category" personal data, further conditions beyond legitimate interests must be satisfied. However, EU data protection regulators have acknowledged in an opinion (WP55 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf), an opinion which has been endorsed by the more recent WP249, that as long as the scanning is not specifically aimed at special category data, they do not consider it unacceptable if in practice it is collected.

Complying with core GDPR principles

The customer is responsible for complying with core principles such as fairness, purpose limitation, data accuracy, and storage limitation/deletion (Article 5 GDPR).

"Integrity and confidentiality" is another core GDPR principle (Article 5(1)(f)) and customers may use a security service like Deep Security as a Service to help meet their obligation to protect the integrity and confidentiality of the personal data of which they are controller.
Transparency and privacy notices

Transparency is also a core GDPR principle and controllers are specifically required to give privacy notices to individuals with certain minimum information.

Customers may comply with this requirement by giving their end users notice of the automated and non automated event collection for security and auditing, such as through implementing and communicating a monitoring policy.

Individuals’ rights

A customer may receive a request from an individual (including, employees and any consumers of the customer’s business, if security events have been configured to collect security event information from end users that are consumers of the customer’s business) exercising their rights under the GDPR. As the customer retains original copy personal data processed by Deep Security as a Service and Deep Security as a Service deletes any personal data it processes in accordance with customer instructions (as described above) the customer is best placed to deal with individuals’ rights requests.

Security and data protection by design and by default

Given the prevalence of security threats, employing the security modules in Deep Security as a Service will assist customers to comply with their security and data protection by design and by default obligations under the GDPR.


International transfers

- **Hosting:** all customers are hosted in AWS\(^1\) data centers: AWS-East-1 (North Virginia) with the exception of data back-ups, which are hosted in AWS-West-1 (North California).

- **Trend Micro team:** Deep Security as a Service operation, InfoSec and support team members who provide support and troubleshooting are Trend Micro employees based in Ottawa, Taiwan and Austin, Texas.

Trend Micro relies on EU Commission approved model clauses to transfer personal data out of the EEA.

\(^1\) The contracts with AWS are held by Trend Micro Taiwan.
Additional Resources

- More information on how Trend Micro can help with GDPR compliance: www.trendmicro.com/gdpr
- More information about different types of deep security products available and which one is right for you: https://help.deepsecurity.trendmicro.com/decision-tree.html
- Information on Trend Micro’s product and service approach to data collection: https://success.trendmicro.com/data-collection-disclosure
- Trend Micro data privacy policies: https://www.trendmicro.com/privacy
# Appendix 1: Audit Information

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Information Stored</th>
<th>Where Stored (location of log hosting)</th>
<th>Retention Period</th>
<th>Who Can Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenant specific information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System events</td>
<td>- User Name</td>
<td>All customers – AWS US</td>
<td>13 weeks + 35 days for back-ups</td>
<td>Customer tenant administrators Deep Security as a Service operation team</td>
</tr>
<tr>
<td></td>
<td>- Console Action</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Computer name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Computer IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Tenant Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Policy name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-malware events</td>
<td>- File name and path</td>
<td></td>
<td>32 days + 35 days for back-ups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- File contents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- File hash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Computer/Container Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-reputation events</td>
<td>- Computer name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- URL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall events</td>
<td>- Computer name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Source IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Source MAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Destination IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Destination MAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Packet header</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Type</td>
<td>Key Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Integrity monitoring events   | - Computer name  
- User ID  
- Process name |
| Intrusion prevention events   | - Computer name  
- Source IP  
- Source MAC  
- Destination IP  
- Destination MAC  
- Relevant packet data |
| Log inspection events         | - Computer name  
- Host name  
- System name  
- Program name  
- Source IP  
- Destination IP  
- User names and IDs  
- URL  
- Command  
- Relevant data extracted from the event |
| Application control events    | - Computer name  
- User ID  
- File name |

**Deep Security as a Service environment auditing information**

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Key Information</th>
</tr>
</thead>
</table>
| AWS ELB Logs (access logs)   | - Source IP  
- Deep Security as a Service HTTP Request  
- All customers – AWS US  
- Indeterminate  
- Deep Security as a Service operation team |
| DSM Node System Logs (server0.log) | - Deep Security as a Service user names  
- Pseudonymized e-mails (j****t@company.com)  
- Exception data  
- Error messages  
- Tenant names  
- Session IDs  
- Integration URLs  
- Host Names |