

# 奇安信网神数据防泄漏系统 V6.0

## 产品彩页

奇安信集团

# 1 产品简介

奇安信网神数据防泄漏系统 V6.0（简称“奇安信 DLP 系统”）遵循以数据为中心的安全架构设计，使用先进分类分级数据内容识别引擎，结合用户行为分析技术，完美解决用户数据防泄漏的难题。通过奇安信 DLP 系统，数据管理部门能够借助产品中数据分类能力，实时梳理不同业务类别数据，实现可视化展现和差异化分类保护策略。

# 2 产品规格

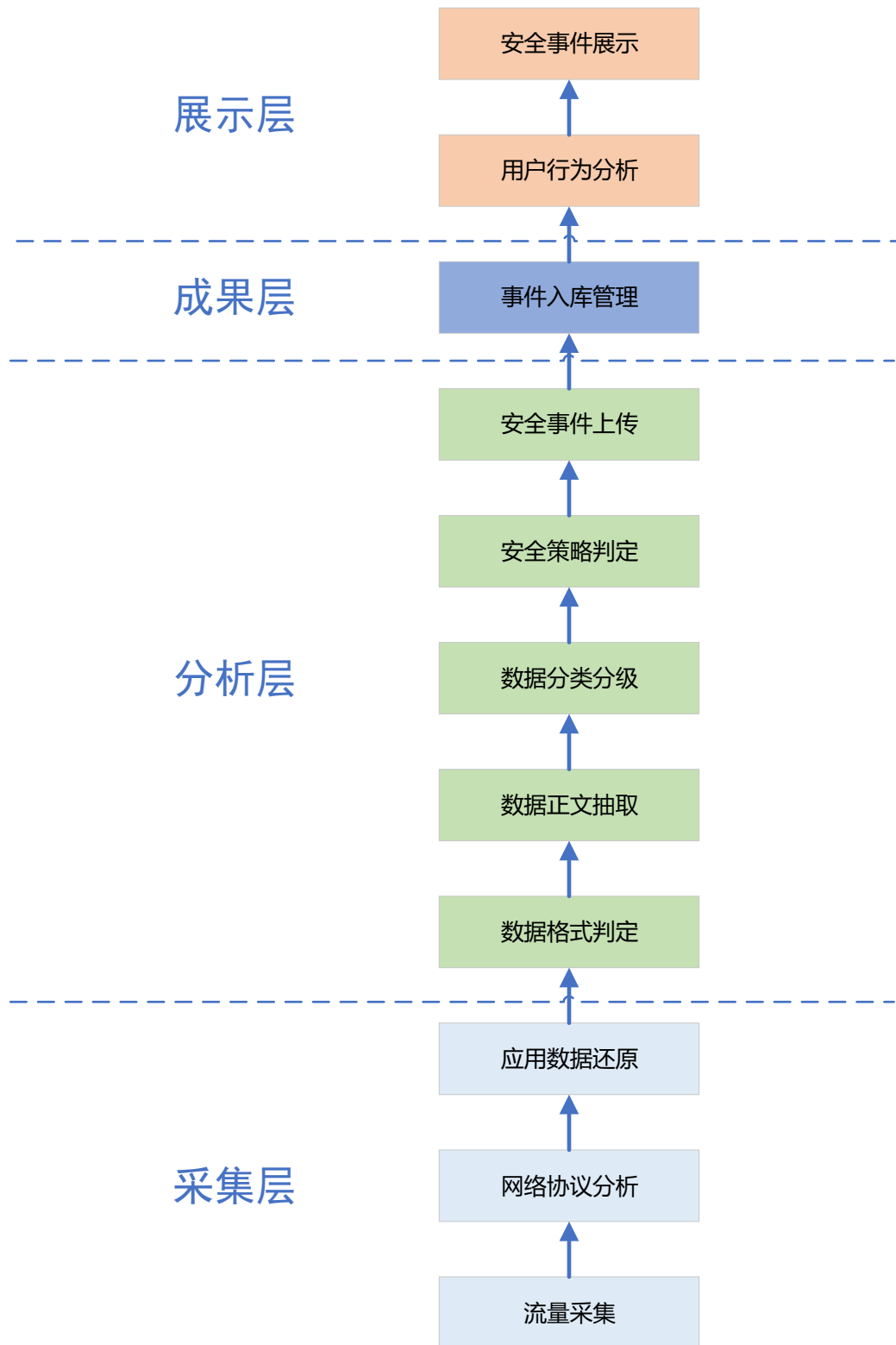
型号	功能项	网络数据泄露防护一体机		
		NDLP-M-YJ-M500	NDLP-M-YJ-M1500	NDLP-M-YJ-M3000
指标				
硬件信息	CPU	国产化 CPU 16 核	国产化 CPU 16 核*2	国产化 CPU16 核*2
	内存	32G	64G	128G
	硬盘	4TB*1	4TB*1	4TB*1
接口	扩展网卡 1	4GE	4GE	4GE
	扩展网卡 2	双口万兆光网卡(不含光纤模块)	双口万兆光网卡(不含光纤模块)	四光万兆扩展网卡(含 4 个光模块)
	接口扩展槽数	扩展卡槽总数: 2 默认已占用数: 2 剩余可使用数: 0	扩展卡槽总数: 6 默认已占用数: 2 剩余可使用数: 4	扩展卡槽总数: 6 默认已占用数: 2 剩余可使用数: 4
	其他接口	板载一个串口、2 个 USB 接口、一个 VGA 接口、一个 BMC 管理网口	板载一个串口、2 个 USB 接口、一个 VGA 接口、一个 BMC 管理网口	板载一个串口、4 个 USB 接口、一个 VGA 接口、一个 RJ45 BMC 管理网口
功能	功能描述	文件扫描识别能力 ≥10G/小时 数据库扫描识别能力 ≥100 万条/小时	文件扫描识别能力 ≥50G/小时 数据库扫描识别能力 ≥500 万条/小时	文件扫描识别能力 ≥100G/小时 数据库扫描识别能力 ≥1000 万条/小时

性能	网络带宽	1.5G	3G	5G
	电源规格	冗余电源	冗余电源	冗余电源
	机身	2U	2U	2U
其他	机箱尺寸 (宽、深、高, mm)	宽(447mm)/高 (86.1mm)/长 (748mm)	宽(447mm)/高 (86.1mm)/长 (748mm)	宽(447mm)/高 (86.1mm)/长 (748mm)
	操作系统	采用国产化操作系统	采用国产化操作系统	采用国产化操作系统

## 3 产品功能

### 3.1. 网络协议解析还原

网络数据防泄露（简称“网络 DLP”）通过旁路部署或配合网络代理服务器串联部署的模式，对员工将关键文档外传至文库、邮箱、网盘等行为实施有效监控。其中，如果客户是通过 https 等 ssl 或 tls 加密协议外发，需要配合网络代理设备进行监测，支持 IPv4 和 IPv6 协议。数据流示意图如下：



- 采集层完成镜像流量的采集，通过网络协议分析并还原网络应用中传输的数据
- 分析层分析网络中传输数据的格式，提取格式中的文本，根据分类分级规则对传输的数据设置分类分级标签，然后根据安全策略判定此数据的传输动作是否涉及安全事件，最后将涉及的安全事件上传

- 还原出的文档进行整理归档存储，以供后期的审计和溯源
- 成果层存储并管理分析层发现的安全事件
- 展示层除了安全事件展示，还支持用户行为分析及分析结果的展示
- 支持协议类型

本产品可以对不同网络传输协议所传输的数据进行监控，包括：

- 电子邮件（SMTP、POP3、IMAP），可支持对邮件标题、正文、附件进行敏感内容识别
- Web（HTTP、HTTPS）
- 文件传输（FTP）
- 共享协议 SMB（Samba）
- DNS 异常检测（监测通过 DNS 回传敏感数据）
- 在流量获取和解析时可自定义端口设置、更改、添加端口设置。

## 3.2. 网络监控策略

网络策略中，支持对部门、用户组、用户、源 IP、IP 段、目的地 IP、域名、URL 等进行针对性监控。设定相同敏感数据字段搬移次数阈值，超出阈值阻断发送，保证数据安全。

## 3.3. 网络风险监控响应

提供对违规操作进行记录、审计以及全流量数据审计，执行网络策略时，本产品不但支持放行、审计、阻断等相应动作，还支持修改严重度、指定处理人、邮件告警等后续操作。

## 3.4. 数据分类分级

奇安信网神数据防泄露系统贯彻数据分类分级治理理念，在制定数据防泄漏策略之前先进行数据分类的治理工作，再通过对分类（分级）类别的价值差异决定对数据的具体保护方式。通过数据分类的治理功能一方面实现了对不同价值数据的区别保护；同时，系统数据保护策略依据的也是基于数据分类分级的场景保护，实现了对不同风险事件的差异识别。

### 3.4.1. 数据分类

在企业实际的业务中，通常是按照数据在企业运转中的作用对数据进行划分（例如：个

人信息、隐私信息、账户信息、财务数据、采购信息、合同信息等等), 这种划分方式我们称之为“数据分类”。

#### 某银行部分数据分类实例

##### 小企业管理部

- 零售信贷业务管理文档
- 个人征信管理文档
- 零售信贷业务系统客户信息

##### 资产保全部

- 不良贷款清收数据
- 不良贷款定期分析报告
- 不良贷款清收计划

##### 风险管理部

- 内部自查质量月度分析报告
- 操作风险事件
- 风险计量模型验证
- 内评体系建模、校验和维护等

##### 运营管理部

- 核心账务系统基础数据
- 核心账务系统各类会计报表
- 会计操作风险监控

##### 监察室

- 未公开的涉及到领导的举报材料
- 反欺诈预警及核查信息
- 员工失范行为信息

##### 私人银行业务

- 向银监局统计局上报监管类报表
- 专营机构报表
- 私人银行业务培训计划、方案、课件
- 私人银行客户数据统计和分析信息

#### 3.4.2. 数据分级

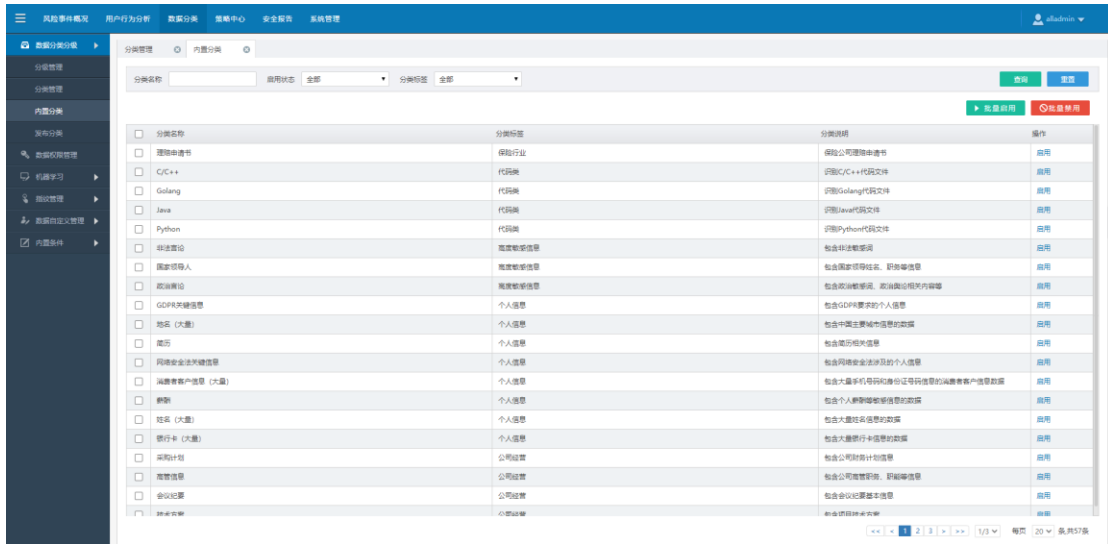
如果按照企业特有的价值评价方式将数据规划为不同的“级别”(例如: 普通商密、核心商密、秘密、机密、绝密等等), 这种从价值角度看待数据划分的规则体系通常被称为“数据分级”。

### 数据分类分级

分类	分级					
	机密	秘密	核心商密	普通商密	内部	公开
重要客户信息	✓					
专利申请	✓					
人民银行公文		✓				
经营分析会报告			✓			
干部考察材料			✓			
民主生活会纪要	✓					
内部审计报告		✓				
重要业务系统账号列表			✓			
管理层薪酬福利			✓			
渠道管理政策				✓		
一般合同				✓		
市场调研					✓	
产品市场报价						✓

#### 3.4.3. 内置分类

系统预置多种数据分类模板，包括 GDPR-个人信息类、代码类、行业信息类、合同类、密钥类等。



### 3.5. 人工智能内容识别

#### 3.5.1. 机器学习

系统在文本内容认知方面独创性地引入了中文自然语言处理方法,应用机器学习和文本聚类分类技术,对数据进行基于内容的实时精准分类。通过集成到系统平台的机器学习引擎,实现有监督机器学习,提取短句或长组合词作为语义特征,自动生成分类规则库,解决内容识别分类的难题。在机器学习过程中,用户亦可人工干预特征选择。

#### 3.5.2. 持续优化学习

为了能有效解决数据内容识别的准确率,在机器学习过程中可使用对照样本(例如:误报样本组、漏报样本组)加强训练,可以极大提高数据梳理及在线机器学习效率及准确率。

### 3.6. 常规内容识别规则

- 支持关键字、关键字排除、关键字对、词典模式检测
- 支持对正则表达式、关键字、文档指纹、确切数据匹配、分类、文档属性(文档名称、文档大小、文档类型)进行敏感数据识别与检测
- 支持结构化数据指纹,支持指纹库管理
- 支持非结构化数据指纹,非结构化数据指纹识别依据指纹匹配的百分比(相似度)进行响应,匹配百分比可设置
- 支持各种识别技术任意组合方式。如文档中必须有手机号、关键字为指导书且文件

属性为 word 文档

- 办公类类型文件支持 DOC、DOCX、PPT、PPTX、XLS、XLSX、TXT、PDF、WPS、ET、DPS，支持识别文件嵌套
- 压缩包类型文件支持 RAR、ZIP、7Z，支持对压缩文件进行识别，支持文件多层压缩识别

### 3.7. 图像文件内容识别

OCR 是英文 Optical Character Recognition 的缩写，意思是光学字符识别，也可简单地称为文字识别。它通过扫描和摄像等光学输入方式获取纸张上的文字图像信息，利用各种模式识别算法分析文字形态特征，DLP 通过配合 OCR 服务器，将图片传输给 OCR 服务器进行识别，可识别图像文件的文字内容，支持通用图片格式敏感内容识别。

### 3.8. 内置数据规则

本系统预置多种数据规则模板，包括手机号码、身份证号码、港澳通行证号、统一社会信用代码、银行卡号、车牌号（包括新能源车牌）、车辆 VIN 码、IP、邮件地址、通信地址、开发代码等等内置规则条件，并可根据行业特性自主添加。

条件名称	启用状态	条件标签	来源	是否启用	操作
<input type="checkbox"/> 条件名称	全部	全部	全部		
<input type="checkbox"/> 车辆VIN码		车牌类	来源	启用	禁用
<input type="checkbox"/> 普通车牌号		车牌类	来源	启用	禁用
<input type="checkbox"/> 新能源车牌号		车牌类	来源	启用	禁用
<input type="checkbox"/> Master卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> VISA卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 常见银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 工商银行		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 光大银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 广发银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 华夏银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 建设银行		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 交通银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 民生银行		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 宁波银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 农业银行		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 平安银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 浦发银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 深发银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 兴业银行卡		银行卡号类	来源	启用	禁用
<input type="checkbox"/> 银联卡		银行卡号类	来源	启用	禁用

条件名称	启用状态	条件标签	来源	是否启用	操作
<input type="checkbox"/> 银行卡-壳	<input type="checkbox"/>	银行卡号类	来源	启用	禁用
<input type="checkbox"/> 招商银行	<input type="checkbox"/>	银行卡号类	来源	启用	禁用
<input type="checkbox"/> 中国银行	<input type="checkbox"/>	银行卡号类	来源	启用	禁用
<input type="checkbox"/> 中信银行	<input type="checkbox"/>	银行卡号类	来源	启用	禁用
<input type="checkbox"/> JCB卡	<input type="checkbox"/>	国外银行卡号	来源	启用	禁用
<input type="checkbox"/> 美国运通卡	<input type="checkbox"/>	国外银行卡号	来源	启用	禁用
<input type="checkbox"/> IP地址	<input type="checkbox"/>	IT类	来源	启用	禁用
<input type="checkbox"/> JDBC连接串	<input type="checkbox"/>	IT类	来源	启用	禁用
<input type="checkbox"/> MAC地址	<input type="checkbox"/>	IT类	来源	启用	禁用
<input type="checkbox"/> URL	<input type="checkbox"/>	IT类	来源	启用	禁用
<input type="checkbox"/> 大陆护照号	<input type="checkbox"/>	证件类	来源	启用	禁用
<input type="checkbox"/> 港澳通行证号	<input type="checkbox"/>	证件类	来源	启用	禁用
<input type="checkbox"/> 美国护照号	<input type="checkbox"/>	证件类	来源	启用	禁用
<input type="checkbox"/> 美国社保号	<input type="checkbox"/>	证件类	来源	启用	禁用
<input type="checkbox"/> 身份证号	<input type="checkbox"/>	证件类	来源	启用	禁用
<input type="checkbox"/> 统一社会信用代码	<input type="checkbox"/>	证件类	来源	启用	禁用
<input type="checkbox"/> 通讯地址	<input type="checkbox"/>	个人信息类	来源	启用	禁用
<input type="checkbox"/> 邮件地址	<input type="checkbox"/>	个人信息类	来源	启用	禁用
<input type="checkbox"/> 手机号码 (东南亚)	<input type="checkbox"/>	电话号码类	来源	启用	禁用
<input type="checkbox"/> 手机号码 (韩国)	<input type="checkbox"/>	电话号码类	来源	启用	禁用

### 3.9. 特殊泄露方式保护

奇安信 DLP 系统除了可以对常规的泄露途径进行防护外，还可以针对一些特殊的泄露方式进行防控。比如 DLP 系统能准确识别通过修改文件名，更改文件后缀，或转换文件类型等规避手段处理过的，企图逃逸检查的敏感数据内容。同时，也能检测到通过多层压缩、分卷压缩、多层嵌套等试图规避检查的方式外发敏感文件的行为。

#### 3.9.1. 点滴式泄露方式

点滴式泄露是指在指定的间隔时间内敏感信息命中的次数达到了指定的次数即可视为风险。在策略设置中，可以通过设置高级条件，来监控这种特殊的数据泄露方式，保护敏感数据。例如，员工 A 在一小时内发送的邮件内容中手机号的数量累计达到 50 个，就会命中策略产生事件，但是他若在 1 小时内第一次发送了 20 个手机号，第二次发送了 15 个手机号，手机号累计数量小于 50 就不会命中策略。

#### 3.9.2. 修改文件后缀名方式

支持对更改文件名、更改文件后缀、更改压缩包后缀、转换文件类型或不带文件扩展名等常见规避手段处理过的敏感文件内容进行检查。

### 3.9.3. 多层嵌套方式

包含敏感信息的文件经过多层嵌套后，也能被 DLP 系统识别到。识别引擎对嵌套层数无限制，可检测到将敏感文件通过数层嵌套以逃逸检测的行为。

### 3.9.4. 多层压缩方式

在经过多层压缩，敏感信息文件仍然能够在每一层文件中都能被 DLP 系统检测到，识别引擎对压缩的层数无限制。经过 10 层压缩的敏感文件仍可被检测到。

### 3.9.5. 分卷压缩方式

敏感文件通过压缩工具分卷压缩后，试图往外发送时依旧能够被 DLP 系统检测到，并记录相关事件信息。

## 3.10. 数据发现

奇安信 DLP 系统可发现终端本地存储、网络共享存储、数据库以及云对象存储中的数据，并记录分布情况。

### 3.10.1. 网络数据发现

系统可设置网络共享数据发现策略，支持发现 SMB/CIFS、NFS、FTP、SFTP 等常见网络共享存储服务器中的数据存储，并记录分布情况，支持网页提交、邮件、微博、贴吧、论坛等结构化或非结构化数据进行识别与检测。

### 3.10.2. 数据库数据发现

系统支持发现扫描存储在数据库中的敏感数据，支持 Oracle、SQLServer、MySQL、Postgres、DB2 等数据库。

### 3.10.3. 云对象存储数据发现

系统支持阿里云、腾讯云等云对象存储敏感数据扫描。