快页安融合一体机系统
产品白皮书

V1.0

快页

KUAIYE®

南京市大周路 32 号软件谷科创城 D2 南 8 楼 210012

版权声明

商标声明

信息反馈

目录

1 前言 4
2 安融合技术架构 5
2.1 安融合架构定义 5
2.2 系统总体架构 5
3 基础设施虚拟化 5
3.1 主机虚拟化 6
3.2 存储虚拟化 6
3.3 网络虚拟化 7
4 安全设施模块化 8
4.1 网络准入管理系统 8
4.2 下一代防火墙系统 9
4.3 Web 防火墙系统 9
4.4 运维安全管理系统 10
4.5 日志审计分析系统 10
4.6 漏洞扫描系统 12
4.7 数据库审计系统 13
4.8 网络性能管理系统 14
4.9 内容安全监测系统 15
4.10 安全态势感知系统 15
5 安融合核心价值 16
5.1 可靠性 16
5.2 安全性 16
5.3 扩展性 16
5.4 易用性 16
6 安融合最佳实践 17

1 前言

20 世纪 90 年代，随着 Windows 的广泛使用及 Linux 服务器操作系统的出现奠定了 x86 服务器的行业标准地位，然而 x86 服务器部署的增长带来了新的 IT 基础架构和运作难题，包括：基础架构利用率低、物理基础架构成本日益攀升、IT 管理成本不断提高以及对关键应用故障和灾难保护不足等问题。X86 服务器虚拟化技术的出现，通过将 x86 系统转变成通用的共享硬件基础架构，充分挖掘硬件的潜力，提高硬件的利用效率，降低硬件和运营成本，并且简化运维降低管理成本，最终帮助用户把更多的时间和成本转移到对业务的投入上。

随着云计算和虚拟化技术向构建新一代数据中心方向发展，关键以虚拟化为基础，实现管理以及业务的集中，对数据中心资源进行动态调整和分配，重点满足企业关键应用向 X86 系统迁移对于资源高性能、高可靠、安全性和高可适应性上的要求，同时提高基础架构的自动化管理水平，确保满足基础设施快速适应业务的商业诉求，支持企业应用云化部署。

云计算并不是一种新的技术，而是在一个新理念的驱动下产生的技术组合。在云计算之前，企业部署一套服务，需要经历组网规划，容量规划，设备选型，下单，付款，发货，运输，安装，部署，调试的整个完整过程。这个周期在大型项目中需要以周甚至月来计算。在引入云计算后，这整个周期缩短到以分钟来计算。

IT 业有一条摩尔定律，芯片速度容量每 18 个月提升一倍。同时， IT 行业还有一条反摩尔定律，所有无法追随摩尔定律的厂家将被淘汰。 IT 行业是快鱼吃慢鱼的行业，使用云计算可以提升 IT 设施供给效率，不使用则会拖慢产品或服务的扩张脚步，一步慢步步慢。

云计算当然还会带来别的好处，比如提升复用率缩减成本，降低能源消耗，缩减维护人力成本等方面的优势，但在反摩尔定律面前，已经显得不是那么重要。

业界关于云计算技术的定义，是通过虚拟化技术，将不同的基础设施标准化为相同的业务部件，然后利用这些业务部件，依据用户需求自动化组合来满足各种个性化的诉求。云着重于虚拟化，标准化，和自动化。

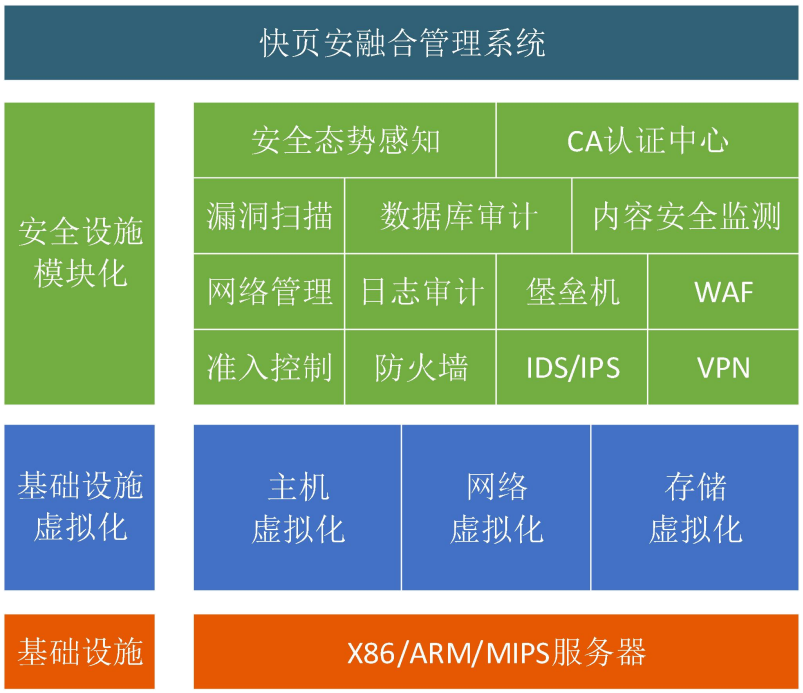
快页的安融合架构是一款成熟的 Iaas 层的云计算解决方案，除满足上面所述的虚拟化，标准化和自动化诉求外，还集成了多种安全模块，向您提供简单易用的模块化安全产品。

2 安融合技术架构

2.1 安融合架构定义

安融合基础架构，这是一种将计算、网络、存储和安全等资源作为基本组成元素，根据系统需求进行选择和预定义的一种技术架构，具体实现方式上一般是指在同一套单元节点（x86服务器）中融入软件虚拟化技术（包括计算、网络、存储、安全等虚拟化），而每一套单元节点可以通过网络聚合起来，实现模块化的无缝横向扩展（scale-out），构建统一的资源池。

2.2 系统总体架构



快页安融合架构图

快页安融合架构在基于底层基础架构（标准的 X86/ARM/MIPS 硬件）上将计算、存储、网络、安全软件化，通过这种软件化的方式，即计算虚拟化 vSV、存储虚拟化 vSAN、网络虚拟化 vNet，构建了数据中心里所需的最小资源单元，通过资源池中的最小单元，提供了数据中心 IT 基础架构中所需的全部资源。

3 基础设施虚拟化

3.1 主机虚拟化

计算资源虚拟化技术就是将通用的 服务器经过虚拟化软件，对最终用户呈现标准的虚拟机。这些虚拟机就像同一个厂家生产的系列化的产品一样，具备系列化的硬件配置，使用相同的驱动程序。

虚拟化技术起源于大型机，最早可以追溯到上世纪六、七十年代大型机上的虚拟分区技术，即允许在一台主机上运行多个操作系统，让用户尽可能充分地利用昂贵的大型机资源。

随着技术的发展和市场竞争的需要，虚拟化技术向小型机或 UNIX 服务器上移植，只是由于真正使用大型机和小型机的用户还是少数，加上各厂商产品和技术之间的不兼容，使得虚拟化技术不太被公众所关注。

20 世纪 90 年代，虚拟化软件厂商采用一种软件解决方案，以 VMM(Virtual Machine Monitor, VMM 虚拟机监视器)为中心使 X86 服务器平台实现虚拟化。然而这种纯软件的“全虚拟化”模式，每个 Guest OS（客户操作系统）获得的关键平台资源都要由 VMM 控制和分配，需要利用二进制转换，而二进制转换带来的开销使得“完全虚拟化”的性能大打折扣。为解决性能问题，出现了一种新的虚拟化技术“半虚拟化”，即不需要二进制转换，而是通过对客户操作系统进行代码级修改，使定制的 Guest OS 获得额外的性能和高扩展性，但是修改 Guest OS 也带来了系统指令级的冲突及运行效率问题，需要投入大量优化的工作。当前，虚拟化技术已经发展到了硬件支持的阶段，“硬件虚拟化”技术就是把纯软件虚拟化技术的各项功能用硬件电路来实现，可减少 VMM 运行的系统开销，可同时满足 CPU 半虚拟化和二进制转换技术的需求，

快页的安融合架构解决方案中的计算虚拟化采用 vSV 虚拟化系统，通过将服务器资源虚拟化为多台虚拟机。最终用户可以在这些虚拟机上安装各种软件，挂载磁盘，调整配置，调整网络，就像普通的 x86 服务器一样使用它。

计算虚拟化是安融合的架构中必不可少的关键因素，对于最终用户，虚拟机比物理机的优势在于它可以很快速的发放，很方便的调整配置和组网。对于维护人员来讲，虚拟机复用了硬件，这样硬件更少，加上云平台的自动维护能力，这样整个 IT 系统的成本显著降低。

3.2 存储虚拟化

虚拟机技术给服务器带来更高的利用率、给业务带来更便捷的部署，降低了 TCO，与此同时，虚拟机应用给存储带来以下挑战：第一，相比传统的物理服务器方式，单个存储系统承载了更多的业务，存储系统需要更强劲的性能来支撑；第二，采用共享存储方式部署虚拟机，单

个卷上可能承载几十或上百的虚拟机，导致卷 IO 呈现更多的随机特征，这对传统的 Cache 技术提出挑战；第三，单个卷承载多个虚拟机业务，要求存储系统具备协调虚拟机访问竞争，保证对 QoS 要求高的虚拟机获取到资源实现性能目标；第四，单个卷上承载较多的虚拟机，需要卷具有很高的 IO 性能，这对传统受限于固定硬盘的 RAID 技术提出挑战；第五，虚拟机的广泛使用，需要更加高效的技术来提高虚拟机的部署效率，加快新业务的上线时间。

业界典型的分布式存储技术主要有分布式文件系统存储、分布式对象存储和分布式块设备存储等几种形式。分布式存储技术及其软件产品已经日趋成熟，并在 IT 行业得到了广泛的使用和验证，例如互联网搜索引擎中使用的分布式文件存储，商业化公有云中使用的分布式块存储等。分布式存储软件系统具有以下特点：第一，高性能：数据分散存放，实现全局负载均衡，不存在集中的数据热点，大容量分布式缓存；第二，高可靠：采用集群管理方式，不存在单点故障，灵活配置多数据副本，不同数据副本存放在不同的机架、服务器和硬盘上，单个物理设备故障不影响业务的使用，系统检测到设备故障后可以自动重建数据副本；第三，高扩展：没有集中式机头，支持平滑扩容，容量几乎不受限制；第四，易管理：存储软件直接部署在服务器上，没有单独的存储专用硬件设备，通过 Web UI 的方式进行软件管理，配置简单。

在充分掌握了用户需求的基础上，快页的安融合架构中，推出以 vSAN 分布式存储软件为核心的解决方案，快页虚拟存储（简称 vSAN）是基于分布式文件系统开发的面对存储虚拟化趋势的一款产品。当前 vSAN 集成在虚拟化管理平台上面，通过网络整合管理集群内所有服务器的硬盘（系统盘除外）。

vSAN 属于安融合解决方案中专门为云计算环境而设计、面向一体化市场应用的新一代产品，融合分布式缓存、SSD 缓存加速、全局负载均衡、及多重数据保护等诸多存储技术，能够满足关键业务的需求，保证客户业务高效稳定运行。

3.3 网络虚拟化

网络虚拟化是构建安融合架构中，非常重要的一部分，我们通过 vSV 实现了服务器虚拟化，vSAN 实现了通过服务器节点构建了存储虚拟化，但还是存在没有解决的问题：

一、如何保障虚拟机可以在我的物理网络环境中进行顺利的迁移，虚拟化后的数据中心涉及业务众多，对外部提供云接入服务时，传统的 Vlan 技术已经无法满足业务隔离的需求，怎么解决大规模租户和租户之间、业务和业务之间的安全隔离也是面临的首要问题。

二、虚拟化后的数据中心的业务系统的构建和上线对网络功能的快速部署、灵活弹性甚至成本，提出了更高的要求。

三、在传统网络中，不论底层的 IT 基础设施还是上层的应用，都由专属设备来完成。这些设备成本高昂，能力和位置僵化，难以快速响应新业务对网络快速、灵活部署的需求。

基于上述问题，快页采用了业界成熟的 SDN+NFV 的解决方案，我们称之为 vNET，通过 Overylay 的方式来构建大二层和实现业务系统之间的租户隔离，通过 NFV 实现网络中的所需各类网络功能资源（包括基础的路由交换、安全以及应用交付等）按需分配和灵活调度，从而实现安融合架构中的网络虚拟化。

4 安全设施模块化

4.1 网络准入管理系统

快页网络准入控制管理系统基于对用户身份和终端风险的双重验证，判断是否允许访问网络以及获得相应的访问权限。系统以身份认证为基础，以准入控制为核心，以行为规范为手段，以监控审计为辅助，将终端作为最小管理单元，能够为用户解决“网络接入不可知、非法外联不可控、违规行为不可管”的网络安全管理问题。

（1）、 部署方式灵活

对网络无任何要求，可以无缝兼容现有网络内所有的网络设备，不会对现有网络内的设备做任何结构上的改变，不会改变网络的物理及逻辑拓扑结构，包括可网管的网络设备及不可网管的 HUB 类网络设备，部署实施成本极低。同时，通过 NAT 网络穿透技术，可以实现跨 NAT 复杂应用下的合法终端识别放行及违规终端拒绝入网功能，实现对极复杂场景下的准入控制功能。

准入防护全面

可以实现强制的入网终端安全管理功能，入网终端强制安装管理插件进行身份认证，未认证拒绝入网。终端入网需经过准入控制、身份认证、安全技术评测、施加管理策略四个标准化流程，确保入网终端均符合安全管理规范。可对客户网络进行全方位立体防护，将客户网络中的互联网资源、服务器资源、终端资源全方位防护起来，杜绝未经授权的随意访问。

（2）、 使用操作简单

简单易用的准入设计，流程化引导终端入网认证，终端用户“0”学习成本，支持高可用性的功能设计，支持 ByPASS、分级级联部署、双机热备等部署方式。所有功能均通过一个服务器平台、一个管理页面、一个终端插件实现，在提供丰富内网安全管理功能的基础上，为用户提供一个简单、易用的内网安全管理方案。

（3）、 权限管控精细

网络访问权限细分，可根据不同的入网身份划定不同的网络访问区域，支持安全区域、来宾区域、隔离区域的设定。支持精细化的安全区域访问权限管理，可按部门设置不同的访问范围，防止随意访问无关服务器及终端资源，如销售仅能访问销售 OA 系统，无法访问财务服务器，提高网络访问的安全性。

4.2 下一代防火墙系统

支持集成第三方下一代防火墙系统，集成防病毒、VPN、IPS 等安全功能。下一代防火墙基于深度应用、协议检测和攻击原理分析的入侵防御技术，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，为用户提供 L2-L7 层网络的全面安全防护，在有效保护用户网络健康及服务器安全的同时提供出色的安全防护性能；通过网络流量深度检测和解析技术，能够基于应用、用户、内容、国家地理等进行多维度的精准识别，可为用户提供丰富而灵活的安全管控功能；通过强大的网络适应性，可实现复杂环境下的安全部署，满足用户多样化的网络功能需求。

4.3 Web 防火墙系统

快页 Web 防火墙系统 NextWAF 产品在数据平面实现了 HTTP(S)的 Web 攻击检测、防御，在管理平面实现了日志告警、漏洞扫描、网页防篡改等基础功能。

NextWAF 产品支持在线串接、旁路检测和服务器负载均衡三种工作模式。能够提供 OWASP Top10 的全面防御，同时可以主动对业务系统建立正向模型，用于防御未知的威胁和 0day 攻击。NextWAF 产品整合了天融信积累的 DDoS 防御能力，可以有效的缓解针对 Web 服务器的 Syn flood、CC、慢速攻击等各种拒绝服务攻击。

NextWAF 产品提供了详细的 Web 流量日志和攻击事件日志，以及基于攻击事件日志实现的各种统计报表，并以可视化方式动态展示，实现实时的威胁监控，是适用于政府、企业、高校以及运营商的可信的防御 Web 威胁的安全产品。

NextWAF 产品提供了精细的防护规则包括：

- ✧ 跨站脚本攻击
- ✧ 扫描器防护
- ✧ SQL 注入攻击
- ✧ 操作系统命令注入
- ✧ 远程文件包含攻击
- ✧ 本地文件包含攻击

- ✧ 目录遍历
- ✧ 信息泄漏
- ✧ WebShell 检测
- ✧ HTTP 协议异常
- ✧ HTTP 协议违规
- ✧ 其他类型的攻击

除了基于规则的检测方法，NextWAF 产品还具备基于自学习建模的主动防御引擎。对于 URI 和 POST 表单，NextWAF 产品的主动防御引擎都可以学习到其参数的个数，以及每一个参数的类型和长度。在学习一段时间之后（通常是一到两周），NextWAF 产品可以建立目标服务器所有动态页面的正向模型。在应用主动防御策略的条件下，所有不符合正向模型的参数都会被阻断，可有效的防御未知威胁和 0day 攻击。

4.4 运维安全管理系统

快页运维安全管理系统集账号管理、授权管理、认证管理和综合审计于一体，为企业提供统一框架，整合企业服务器、网络设备、主机系统，确保合法用户安全、方便使用特定资源。既能有效地保障合法用户的权益，又能有效地保障支撑系统安全可靠地运行。

（1）、 浏览器远程资源访问，告别客户端工具

直接使用浏览器访问资源，无需安装客户端工具，支持原生 RDP/SSH/Telnet/VNC/HTTP 协议，可访问所有 Windows、Linux/Unix 操作系统。

（2）、 操作审计

多面记录运维人员的操作行为，作为追溯的保障和事故分析的依据。

（3）、 职权管控

进行账号管控和权限组管理，分职权进行人员和资产管理。

（4）、 安全认证

引入双因子认证机制，防止运维人员身份冒用和复用。

4.5 日志审计分析系统

快页推出的下一代日志审计分析系统，采用具有自主知识产权的分布式非关系型数据库技术的日志审计系统及日志分析管理解决方案。系统能够通过主被动结合的手段，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息，并将这些信息汇集到审计中心，进行集中化存储、索引、备份、全文检索、

实时搜索、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。

系统采用融合了大数据技术的新一代技术架构，基于分布式节点计算机制，使用非关系型数据库，具有分布式、全文索引、扩展、实时格式化数据搜索和原始数据关键字搜索、高可靠性等特点，帮助用户进行基于日志的综合审计和日志全生命周期管理，从而最大化的保障网络、主机和应用系统安全机制的有效性。

（1）、 日志收集

通过配置多种类型的日志源，快页下一代日志审计分析系统能够支持安全设备、网络设备、操作系统、数据库、中间件及各类应用等多种日志数据的收集。

（2）、 日志存储

快页下一代日志审计分析系统集中存储所有收集到的日志。

集中存储：集中存储可以提高日志的安全性并方便管理。支持灵活的存储策略，可以为不同日志源设置不同时间的存储策略。支持存储空间上限管理，当存储空间不足时会自动删除最旧的日志，优先存储最新产生的日志。

原始格式：快页下一代日志审计分析系统同时存储格式化日志和原始日志，以便能够最大限度还原原始信息，为准确取证提供保障。

（3）、 日志查询

快页下一代日志审计分析系统提供了多样、灵活的日志信息查询功能，方便管理员快速查找定位关键日志和准确地进行事后取证。

条件查询：支持多条件组合查询日志数据，查询结果可以导出查看。如果不输入条件，默认查询所有该时间段内日志。查询结果倒序显示，也就是最近产生的日志在前面。

查询结果可导出：日志查询结果可以导出到文件中，方便离线使用。

（4）、 日志分析

快页下一代日志审计分析系统支持实时统计报表，能够根据预置的各种报表模板实时生成统计报表数据，达到快速生成并展示报表的效果。系统根据各种设备日志类型预置了丰富的报表模板，并提供日、月、季度、年等统计周期。查看统计分析结果不再需要漫长的等待。

（5）、 日志预警

快页下一代日志审计分析系统能够对系统状态和关键事件及时作出响应。目前支持邮件、短信、页面展示等多种响应方式。

（6）、 日志报告

快页下一代日志审计分析系统可以支持自动生成报告、手工定制报告。报告结果支持 word、html 等多种格式。

4.6 漏洞扫描系统

快页洞扫描系统 NextVS，是架构于自有系统之上，使用基于脚本插件的规则库来对目标系统进行黑盒测试的安全评估产品。 NextVS 集 Web 漏洞扫描和系统漏洞扫描于一体，可扫描各类操作系统、思科华为等网络设备、Web 应用系统和数据库应用系统，不但可以给出详细的检测报告，还能针对检测到的网络安全隐患给出相应的解决方案和安全建议。

全方位的扫描对象支持：

- 网络主机：服务器、客户机、网络打印机等；
- 操作系统：Windows 系列、Linux、Sun Solaris、IBM AIX 等；
- 网络设备：Cisco、Juniper、华为、Checkpoint 等主流厂商网络设备；
- 应用系统：数据库、Web、FTP、电子邮件等。

漏洞库覆盖面广

可扫描的漏洞数量超过 5000 种，分为 30 个大类，覆盖了当前网络环境中重要的、流行的系统和数据库漏洞。Web 应用系统漏洞覆盖 OWASP Top10 安全隐患。

OWASP统计的Web前十大安全隐患

4.7 数据库审计系统

NextDA 是由快页公司开发具有自主知识产权的数据库审计系统产品。实现即查即显、实时报表的数据库审计系统，审计分析准确度高达 99%以上。

NextDA 广泛支持 Sybase、DB2、SQL Server、Oracle、Mysql、Informix、Redis、Elasticsearch、Mongodb 等多种数据库审计分析，采用多核、云审计、云存储等多项独特技术。该产品拥有大量成功客户验证，是保障业务安全运营，实现业务审计，并使信息系统符合等保、分保等政策法规、标准、规定的要求，提高信息系统安全级别的不可或缺的产品。

系统支持对国内外主流商业与行业数据库进行安全审计：

- 商业数据库：Oracle， SQLServer，DB2，Infomix，Sybase
- 行业数据库：Cache
- 开源数据库：Mysql，PostgreSQL
- NoSQL 数据库：Redis，Elasticsearch，Mongodb
- 国产数据库：人大金仓、达梦、南大通用

SQL 操作审计主要包括 SQL 语句的解析、SQL 语句的操作类型、操作字段和操作表名等的分析。

- 支持 SQL 操作响应时间的审计,支持 Update、Insert、Delete 操作返回行数的审计，支持数据库操作成功、失败的审计
- 支持数据库绑定变量审计,支持访问数据库的源主机名、源主机用户的审计
- 可审计 SQL 操作的客户端名称
- 可对 SQL 进行语法解析，分析 SQL 语句的操作类型，操作对象等信息。NEXTDA 内置有 SQL 语法解析器，能实现此功能；此外，用户还可以自定义 SQL 语法解析规则，分析用户特有 SQL 操作等。
- 支持自定义审计界面，方面用户直接审计关心的事件

  支持数据采集规则定义，对于不关心的数据可以不采集，有效保证系统审计的稳定性与针对性。

4.8 网络性能管理系统

专注于为客户提供 IT 网络运维整合服务。集网络设备、服务器、数据库、中间件、服务、安全设备、数据库集群、虚拟机集群、存储运维管理、无线运维管理、视频设备运维管理 、机房动力环境管理、业务管理运维管理、可视化大屏展示、云平台等各种软硬件实现一体化 IT 网络监控方案，打造 IT 网管软件产品的智能化运维、自动化管理的网管需求，遵循用户实际使用习惯，以管理概念为导向，为您提供全方面多纬度的 IT 网络运维管理平台整合服务。

综合监控网络设备、主机/服务器、应用服务、网络设备；且无行业、厂商、类型和型号限制。实现智能拓扑管理、自动发现、设备管理、设备配置管理、故障和工作状态管理、性能管理、安全管理等功能，采用多项业内领先的智能化技术，从底层基础上真的实现网络管理智能化和自动化。

（1）、 服务器监控

全面监控服务器的各项性能指标，支持 Linux/Unix、 Windows、HP-UX、AIX、Solaris、VMware 等系统。

（2）、 网络设备监控

帮助您对网络设备进行全面的监控和管理。对路由器、交换机、防火墙、负载均衡器，以及其它网络基础架构进行监控，让您可以深入了解和管理您的网络性能。

（3）、 数据库监控

监控包含 Oracle、SQL Server、MySQL、Sybase、IBM DB2 等多种类异构型的数据库环境。

4.9 内容安全监测系统

快页内容安全监测系统（NextCSM）支持对文字、视频、音频、图片进行多维检测，及时发现涉黄、涉暴、涉政、广告、违禁品、负面等敏感信息内容。

（1）、 色情识别

除了对视频图像进行色情识别，还对视频中的语音、画面中的文字内容进行色情检测和过滤。

（2）、 暴恐识别

对视频中的图像画面、语音、文字等多维内容，进行暴恐内容检测和识别，并支持自定义设置。

（3）、 政治敏感识别

提供政治人物库和敏感内容库，对画面中人脸、语音、文字中出现的敏感信息，实现自动检测和识别，并支持自建敏感人脸库。

（4）、 违禁品检测

对视频画面中的物品、文字进行检测，识别是否出现涉嫌违禁物品，包括枪支、六合彩、管制刀具等。

（5）、 广告检测

支持对视频中的二维码、条形码、水印进行检测和识别，同时支持对视频中的文字进行识别和广告过滤。

（6）、 自定义特征库

基于视频指纹和比对技术，支持将目标视频与自建视频特征库的指纹对比，实现个性化违规视频监测功能。

4.10 安全态势感知系统

快页安全态势感知系统（NextSOC）以安全检测为核心、以事件关联分析、态势威胁情报为重点、以可视化为特色、以可靠服务为保障，可针对企业面临的外部攻击和内部潜在风险进行深度检测，为企业提供及时的安全告警。通过海量数据多维度分析、及时预警，对威胁及时做出智能处置，实现企业全网安全态势可知、可见、可控的闭环。

灵活的数据采集

支持 Syslog、SNMP 等十余种协议采集，同时支持网络抓包方式的网络流量分析。

超大的分析引擎

预置日志收集引擎，事件分析引擎，分析告警引擎，关联分析引擎，可提供风险、脆弱性、态势、溯源等相关分析。

多维度的威胁检测

多维度、多层面检测，进一步提高发现未知威胁的成功率，降低威胁告警的误报率。

人工智能

强大的机器自学习能力，解决众多系统的海量日志问题。不再依靠传统的建模、沙箱等静态匹配策略的模式。

5 安融合核心价值

5.1 可靠性

快页安融合架构，通过软件定义数据中心的方式，将计算、存储、网络包括安全形成一个大的资源池，可以灵活快速的构建数据中心里的业务系统，在不损失业务性能的情况下，还采用了多种技术来为业务系统提供了可靠性方面的保障。比如虚拟机的热迁移技术、虚拟机的 HA 技术、虚拟机数据备份和恢复、存储的多副本技术。

5.2 安全性

安融合架构同样提供了为客户的业务系统安全性的保障。从虚拟化主机层面，为客户提供了虚拟机磁盘数据加密，同时，基于 vNET 中的 vAF 功能为虚拟机提供了 L2-L7 的立体式安全防护，保证了业务系统的安全性。

5.3 扩展性

快页的安融合架构，采用分布式 Scale-out 的架构设计，在业务系统需要扩展升级时，只需增加相应的服务器计算节点，及可实现容量和性能的线性提升。

5.4 易用性

快页安融合一体机依托底层虚拟化技术，通过软件定义交付安全组件，可灵活根据用户需求，统一交付安全能力。等保二级套餐默认配置网络管理、日志审计、堡垒机等安全组件；等保三级套餐默认配置网络管理、日志审计、堡垒机、数据库审计、WAF 等安全组件。用户也可按需选配各类安全组件。

6 安融合最佳实践

安融合架构可以应用到数据中心涉及的众多业务系统的领域，尤其是网络安全实验室、等保合规安全防护是特别适合部署安融合架构。

以下为快页安融合架构的实际应用案例分享

（1）、 某高校客户

背景：需要建设网络安全实验室，之前的方法是购买各类网络及安全设备，投资较大。

解决之道：用 1-2 台安融合一体机，搭建了一套专用的网络安全实验环境。利用计算、网络和存储虚拟化模拟出测试拓扑和各类操作系统，选配各类安全组件模拟出安全系统。

安融合方案价值：上线周期缩短，投资大大减少，无需大量硬件支撑

（2）、 某政府客户

背景：某政府客户需要通过等保测评。

解决之道：通过 1 台安融合一体机部署符合等保二级的安全系统，4 小时内实现正常上线。

安融合方案价值：节约了大量时间用于安全系统的部署，安全管理人员无需太多人工干预就能更好的实现安全合规管理。