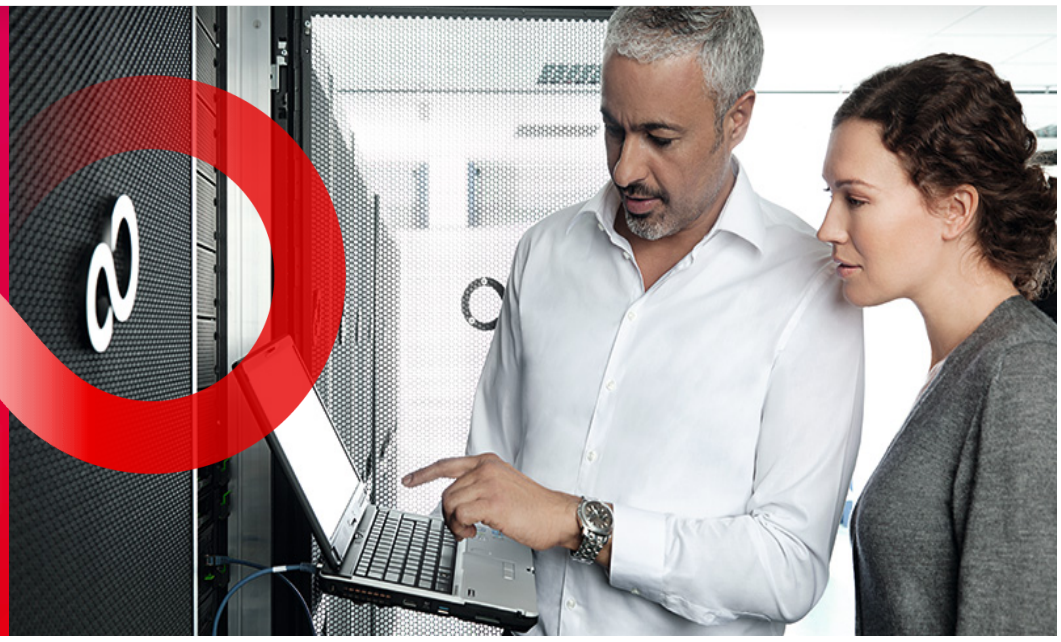
# 安全专家服务



## 定制安全

## 态势感知

态势感知产品的定位是安全大脑，是一个检测、预警、响应处置的大数据安全分析平台。其以全流量分析为核心，以安全大数据为基础，基于动态、整体地洞悉安全风险的能力，结合威胁信息、行为分析建模、大数据关联分析、可视化等技术，实现全网业务可视化、威胁可视化、攻击与可疑流量可视化等，帮助客户在高级威胁入侵之后，损失发生之前及时发现威胁，从全局视角提升其对安全威胁的发现识别、理解分析、响应处置能力。

## 高级持续性威胁防护(APT)

高级持续性威胁(Advanced Persistent Threat，APT)是黑客以窃取核心资料为目的，针对客户所发动的网络攻击和侵袭行为，严重威胁企业数据安全。 APT防护采用主动防御方法，能够有效解决传统防御方法的弊端，例如使用了诱骗技术的沙箱技术以及基于程序行为自主分析判断的实时防护技术和蜜罐技术。

## 网络流量分析

基于网络全流量分析技术，分析和存储各种网络流量，从而检测已知威胁，通过分拆数据包特征，发现可疑网络攻击。

## 威胁捕捉

区别于在攻击者完成攻击，并对业务造成更严重的损害之后才采取行动，本服务通过寻找绕过安全系统的攻击，并抓住入侵来识别企业网络上存在的威胁和未经授权的活动。

## 取证溯源支援服务

根据用户需求，提供各类取证分析服务，可开展Web攻击溯源、邮件攻击溯源、终端取证溯源等支持工作。

## 渗透测试及演练

通过模拟黑客攻击，对各种系统和网络设备的漏洞进行主动分析和检测，可以清晰显示系统和设备目前存在的安全隐患和问题，是评估企业网络系统安全的一种有效的评估方法。同时还可创建系统安全基准线，从而为加固系统提供依据。

## 备份

为应对文件、数据丢失或损坏等可能出现的意外情况，将电子计算机存储设备中的数据复制到磁带等大容量存储设备中的保障措施。

## 容灾技术

作为系统高可用性技术的一个组成部分，容灾系统更加强调处理外界环境对系统的影响，特别是灾难性事件对整个IT节点的影响，提供节点级别的系统恢复功能，保护用户的应用和数据不受故障影响，确保持续使用。

## 灾备演练

为验证已建成灾备系统的可用性、有效性，通过演练结果来修正、补充、完善灾备恢复预案并为灾备系统的升级建设提供理论依据及数据指标，从而使企业在灾备建设中有据可依，保证建成的灾备系统能充分实现建设的目的、达到建设的目标。

# 客户案例及资料获取

| 咨询电话 | 邮件联络 |
| --- | --- |

欢迎您致电了解产品服务信息

021-5887-1000 转市场营销部

受理时间：9:00~17:00（周末及法定假日除外）

欢迎您通过邮件咨询产品服务信息

mimarcom@fujitsu.com

我们通过技术手段保障您的个人信息安全