网络安全
为金融组织
提供的竞争优势

kaspersky

内容

01

金融业概述

金融部门主要参与者

金融业概要

金融技术正逐步渗透至各类金融服务领域，成为其不可或缺的关键组成部分。它不仅重塑了金融行业的商业模式，更推动金融服务朝着以客户为中心的方向迈进，显著提升了客户导向性。

3 个金融服务组织的优先事项：

客户参与

通过无缝、无摩擦的客户体验增加收入

弹性基础设施

提高技术灵活性和可扩展性，
更好地支持业务目标

数字信任和管理

确保强大的安全、风险和合规性基础设施，
以保护客户并支持前瞻性商业模式

金融服务组织的优先事项

	目标	短期计划	中期计划	长期计划
客户参与 通过无缝、无摩擦的客户体验增加收入	• 改进的数字和辅助渠道 • 个性化方法 • 改善的客户体验	• 增强移动银行应用和提升全方位渠道体验 • 可采取行动的客户警报 • 个性化数字服务	• 人工智能虚拟助理与呼叫中心管理 • 通过为交易增值来提高收入：提供基于数据的新服务 • 客户价值和资产负债表优化	• 银行生态系统 • 生活方式银行：运营与客户的生活方式旅程相结合 • 利用大数据进行战略定价优化
数字信任和管理 确保强大的安全、风险和合规性基础设施，以保护客户并支持前瞻性商业模式	• 现代客户识别 • 增强的网络安全 • 综合风险管理	• 优化数字身份验证流程 • 事件追踪和报告 • 运营风险和弹性管理	• 聪明地了解您的客户(KYC)/客户尽职调查(CDD) • 先进的反洗钱交易监控 • 第三方风险管理	• 数据驱动的身份风险评分 • 云安全服务 • 贷款组合健康分析和遵守监管机构的要求
弹性基础设施 提高技术灵活性和可扩展性，更好地支持业务目标	• 弹性数字银行平台 • 积极使用云服务 • 构建灵活且可扩展的 IT 架构	• 逐步将业务应用程序迁移到基于云的基础架构 • 准备适应云服务的框架 • 将整体应用转换为微服务	• 确定特定工作负载的优先级，开始向现代开发方法转型 • 云迁移的工作负载选择 • 简化工作流程以加快应用程序输出	• 实时监控所有应用程序和工作负载 • 使用 AI 来监控基础设施并主动解决事件 • API 管理，以支持各种设备、应用程序和数据之间的互连

客户参与

通过无缝、
无摩擦的客户体验增加收入

目标：

1. 改进的数字和辅助渠道
2. 个性化方法
3. 改善的客户体验

短期计划

- 增强移动银行应用和提升全方位渠道体验
- 可采取行动的客户警报
- 个性化数字服务

中期计划

- 人工智能虚拟助理与呼叫中心管理
- 通过为交易增值来提高收入：提供基于数据的新服务
- 客户价值和资产负债表优化

长期计划

- 银行生态系统
- 生活方式银行：
  运营与客户的生活方式旅程相结合
- 利用大数据进行战略定价优化

弹性基础设施

提高技术灵活性和可扩展性，
更好地支持业务目标

目标：

1. 弹性数字银行平台
2. 积极使用云服务
3. 构建灵活且可扩展的 IT 架构

短期计划

- 逐步将业务应用程序迁移到基于云的基础架构
- 准备适应云服务的框架
- 将整体应用转换为微服务

中期计划

- 确定特定工作负载的优先级，开始向现代开发方法转型
- 云迁移的工作负载选择
- 简化工作流程以加快应用程序输出

长期计划

- 实时监控所有应用程序和工作负载
- 使用 AI 来监控基础设施并主动解决事件
- API 管理，以支持各种设备、应用程序和数据之间的互连

数字信任和管理

确保强大的安全、风险和合规性基础设施，
以保护客户并支持前瞻性商业模式

目标：

1. 现代客户识别
2. 增强的网络安全
3. 综合风险管理

短期计划

- 优化数字身份验证流程
- 事件追踪和报告
- 运营风险和弹性管理

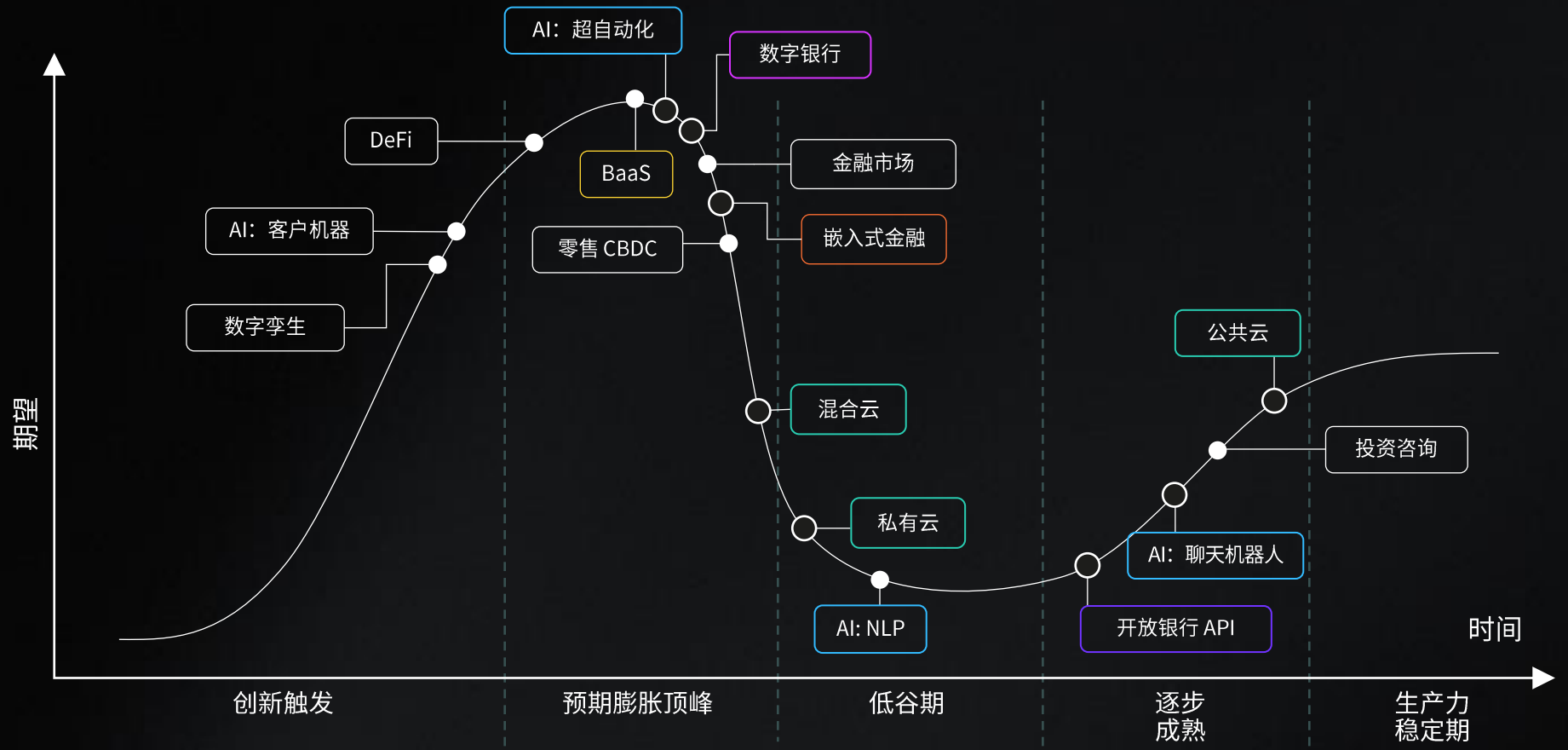
中期计划

- 聪明地了解您的客户(KYC)/客户尽职调查(CDD)
- 先进的反洗钱交易监控
- 第三方风险管理

长期计划

- 数据驱动的身份风险评分
- 云安全服务
- 贷款组合健康分析和遵守监管机构的要求

全球金融业趋势的技术成熟度曲线



云服务

- 混合云
- 私有云
- 公共云

AI

- 超自动化
- 聊天机器人
- NLP

所确定的许多趋势早已存在于市场中，但它们仍在继续扩大，并日益成为"新现实"

*基于 Gartner 技术成熟度曲线

金融业的主要趋势

金融业的发展趋势表明，它的未来正在迅速变化，超越国界，灵活多样。新技术已然成为金融公司实现战略优先事项的核心支撑手段。然而，在带来机遇的同时，也引发了新的风险，一旦遭遇失败，后果将极为严重。

1	开放银行 API	开放银行使第三方能够使用银行数据，从而提高客户服务质量。 实施开放 API 标准需要遵守增强的信息安全措施，包括由合格专家进行审计。
2	BaaS	银行即服务 (BaaS) 涉及从银行购买现有的银行产品以支持业务。 BaaS 为其他企业提供基础设施、产品和服务，因此他们可以提供自己的服务。
3	嵌入式金融	嵌入式金融是 BaaS 的一个分支，涉及将支付服务集成到销售产品或服务的公司的网站/应用程序中。嵌入式金融不像 BaaS 那样专注于业务；相反，它面向最终用户。
4	云服务	云服务可帮助企业扩展和快速启动新项目，而无需寻找额外的计算能力。
5	数字银行	银行在继续开发远程访问、产品数字化和在线服务。
6	人工智能 (AI)	IDC 预测，到 2026 年，85% 的组织将使用人工智能和计算机视觉，从而使生产力提高 25%。

金融业的其他趋势

- 数字货币
- DeFi（去中心化金融）
- 金融市场
- 数字孪生
- 投资顾问

趋势概览

开放银行使第三方能够使用银行数据，从而提高客户服务质量。
实施开放 API 标准需要遵守增强的信息安全措施，包括由合格专家进行审计。

而开放银行的使用也引入了更多的漏洞区域，客户数据可能会受到损害。
根据 Gartner 分析师的说法，对 API 的攻击将成为最常见的攻击媒介，频率翻倍。
这将导致企业 Web 应用程序的数据泄漏。

2022 年的网络攻击真实案例（基于思科分析）

Texas Department of Insurance

原因：Web 服务应用程序中的漏洞无意中允许访问应用程序的受保护部分。这可以归类为 BFLA 漏洞利用。

180 万名客户的数据泄露

Twitter

原因：一个 API 漏洞允许用户找到其他用户，并错误地透露 PII。其中一些数据被在暗网上出售，而有些据称被免费发布。这里的根本问题是不安全的数据，因此这是一个BOLA 漏洞利用。

540 万个账户的数据泄露

1 开放银行 API

实施发起人

监管机构/合规

金融机构在法律上有义务实施开放 API 或建议实施

目标受众

银行　金融科技　客户

开放银行的发展趋势

- 账户聚合可为不同银行账户提供统一视图。
- 使用数据分析来组织支出、创建预算和更有效地储蓄的财务管理工具。
- 基于交易历史的个性化产品，扩大贷款渠道。

趋势概览

BaaS

银行即服务 (BaaS) 涉及从银行购买现有的银行产品以支持业务。

BaaS 是银行与不持有银行执照的企业合作的一种方式，其中银行提供一系列金融服务"供出租"。

BaaS 模型使用开放 API、智能合约和分布式分类账技术实现了企业和银行 IT 系统之间的基本无缝集成。

嵌入式金融

BaaS 的一个分支，涉及将支付服务集成到销售产品或服务的企业的网站/应用程序中。嵌入式金融并不像 BaaS 那样专注于企业，而是面向最终用户。

这为客户在支付商品或服务时提供了简单、无缝的体验。嵌入式融资模块集成到网站或页面中。

网络攻击案件

在电子支付系统中，网络犯罪分子几乎完全专注于 **PayPal：84% 的网络钓鱼页面针对此平台。**
深受欢迎的 **加拿大零售连锁店 LCBO** 于 2023 年 1 月遭到袭击。
恶意代码被嵌入到公司网站中，该网站收集了客户的个人数据、密码和客户的银行卡数据。
这次网络攻击从 12 月 28 日持续到 1 月 10 日。考虑到这个零售网络的网站每月有超过 300 万人访问，这个时期非常长。

2 3 BaaS 和嵌入式金融

实施发起人

业务

目标受众

BaaS

- 银行提供基础设施
- 金融科技和其他行业的企业是银行基础设施的"租户"

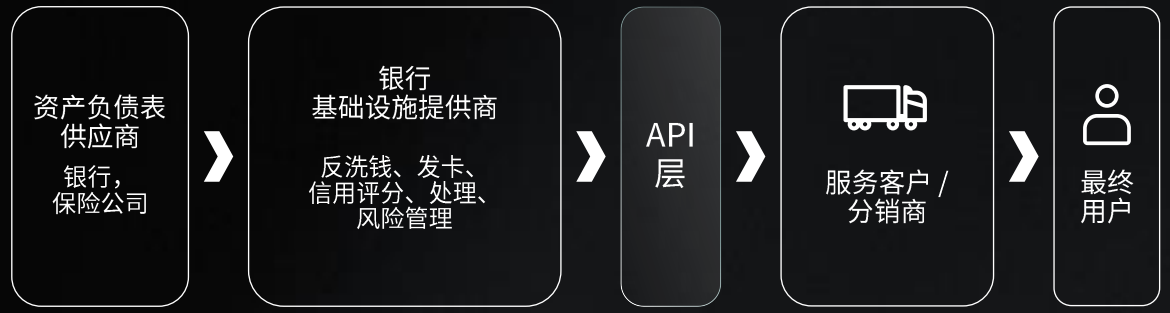
嵌入式金融

- 整个金融部门：提供服务的企业。
- Fintechs 可以在没有获得银行许可证的情况下扩大其金融服务范围，并将银行服务嵌入其平台中。
- 电子商务机构接受付款，在线提供分期付款/BNPL选项。

趋势概览

BaaS (EmFi) 模型包括与第三方业务的集成，从而扩大攻击面

嵌入式金融如何运作（BaaS 模型的变体）*



摩根大通
汇丰控股
BBVA

摩根大通
汇丰控股
BBVA

可融资债券
Solarisbank

Synctera
Clear.Bank

Plaid
Solarisbank

amazon
lamoda
WeChat Pay
Alipay

*资料来源：全球数据

2 3 BaaS 和嵌入式金融

网络安全

EmFi 总是涉及与第三方业务的集成，从而再次增加了攻击面。

主要网络风险：

1. 数据泄漏 — 未经授权访问机密信息：个人客户数据，账号，密码，付款信息。
2. 欺诈 — 使用恶意软件、被盗的登录名和密码来获取机密信息或窃取金钱。
3. 利用合作伙伴企业的漏洞，包括金融科技公司，其安全性往往比银行弱。

- 开放银行和 BaaS 的使用意味着银行客户的个人数据可以通过 API 供第三方企业访问。
- 通常，第三方企业不如银行关心网络安全。
- 如果第三方组织遭到入侵，攻击者可以访问与银行交互的 API，并在发现其中的漏洞后渗透到银行本身。
- 实践表明，银行 API 中的漏洞经常被发现，因此必须采取措施保护它们。

趋势概览

未来，没有开始使用云服务的银行可能会被甩在后面。

网络安全

- 根据卡巴斯基分析师，使用云技术作为攻击媒介的趋势日益增长。
- 越来越多的企业正在将他们的信息系统迁移到云中，通常使用外部合作伙伴的服务来做到这一点。
- 然而，在迁移到云时，信息安全经常被忽视：组织往往甚至没有与他们的虚拟化服务提供商讨论这一点。
- 如果确实发生事件，没有足够的数据进行调查，因为云提供商不会收集或记录有关系统事件的信息。这使事件调查显著复杂化。

与云环境相关的最常见网络风险

- 云基础设施的风险，包括不兼容的遗留系统和第三方数据存储服务的故障。
- 由于人为错误导致的内部威胁，例如不正确的用户访问权限设置。
- 外部威胁，几乎总是与犯罪活动有关，如恶意软件、网络钓鱼和 DDoS 攻击。

云服务网络攻击成功案例

2019 年，Capital One（美国）遭遇数据泄露，导致存储在 AWS 云中超过 1 亿客户的个人信息被盗。2022 年，在微软发生一起客户数据泄漏，实际上来自微软自己拥有的 Azure 云服务。
泄露的数据存储在配置错误的 Azure Blob 存储中。

4 云服务

云服务可帮助企业扩展和快速启动新项目，而无需寻找额外的计算能力。

实施发起人

开发部门

金融机构在法律上有义务实施开放 API 或建议实施

目标受众

与所有行业相关。
金融部门的企业是云最不活跃的用户。

如何使用云？

- 存储大量数据
- 确保全渠道能力并实施数字银行
- 优化流程
- 节省 IT 基础设施的成本

趋势概览

银行在继续开发远程访问、产品数字化和在线服务。

网络安全

- 在这里，我们谈论的是与银行应用程序和服务相关的网络威胁，这些应用程序和服务可以集成到数字银行平台 (DBP) 中。
- 2022 年，网络犯罪分子继续使用恶意软件瞄准网上银行客户：银行木马，窃取程序和远程控制程序。
- 最危险的木马可以完全接管设备，拦截双因素身份验证代码，并从受害者的账户进行交易。
- 在 2023 年第二季度，卡巴斯基解决方案阻止了不止一个恶意程序的启动，这些程序旨在从 95,546 个独立用户计算机上的银行账户窃取资金。

统计数据怎么说

- 2022年，全球检测到的移动银行木马比前一年多得多，仅在第二季度就记录了 55,000 次攻击。为了进行尽可能多的攻击，网络犯罪分子专门针对移动设备创建银行木马。
- 2022 年，卡巴斯基专家确定了 190 多个应用程序，Harly 木马通过这些应用程序进入用户的设备，这些应用的下载次数超过 480 万次。
- 该恶意软件以合法软件的名义通过官方应用商店分发，并在安装后让毫无戒心的用户订阅付费服务。

2023 年 3 月，澳大利亚金融公司 Latitude Financial 被黑。犯罪分子获得了数百万份身份证件和银行卡数据的访问权限。

此外，由于许多俄罗斯银行应用被从国际应用市场中删除，包含恶意代码的这些应用的假版本开始在互联网上传播。

5 数字银行

实施发起人

业务

目标受众

银行

数字银行平台

- 远程银行的最新发展是数字银行平台 (DBP)，Gartner 也强调了这点。
- 它结合了一组零售和企业银行的应用程序和服务，建立在使用统一架构解决方案的通用技术堆栈上。
- 服务通过 API 连接到平台。
- DBP 与新银行和试图跟上时代的传统银行都有关。
- 对于传统金融机构来说，DBP 的实施有助于组织和自动化银行运营。

趋势概览

IDC 预测，到 2026 年，85% 的组织将使用人工智能和计算机视觉，从而使生产力提高 25%。

前台 → 后台

脸部扫描支付 – "微笑支付"	发放网络贷款时对借款人进行快速分析	用于身份验证和授权的生物识别技术（语音、人脸、指纹）	实时交易风险监控
聊天机器人和语音助手	使用人形机器人的分支机构的客户服务。	机器视觉和自然语言处理 (NLP) 用于扫描和处理文档	用于检测网络攻击的机器学习

6 人工智能 (AI)

发起者

业务

目标受众

与所有行业相关。

成功的网络攻击案例

- 一家英国能源公司的负责人接到一个电话，要求在一小时内将 220,000 欧元转移到公司的中央办公室。
- 冒充中央办公室高管的来电者使用了深度伪造技术。

趋势概览

AI 使用示例

中国银行 BANK OF CHINA

2019 年：中国银行 实施了 iAM 智能技术，用于在开设移动银行账户时使用面部识别进行身份验证。

Nordea

2017 年：
Nordea Life & Pension 推出了 一个名为 Liv 的机器人，
瑞典客户服务的"虚拟员工"。
根据 Nordea 的数据，
这导致了 80% 的流程速度加快和 100% 的错误数量减少。

6 人工智能 (AI)

发起者

业务

目标受众

与所有行业相关。

成功的网络攻击案例

- 一家英国能源公司的负责人接到一个电话，要求在一小时内将 220,000 欧元转移到公司的中央办公室。
- 冒充中央办公室高管的来电者使用了深度伪造技术。

使用人工智能的领域

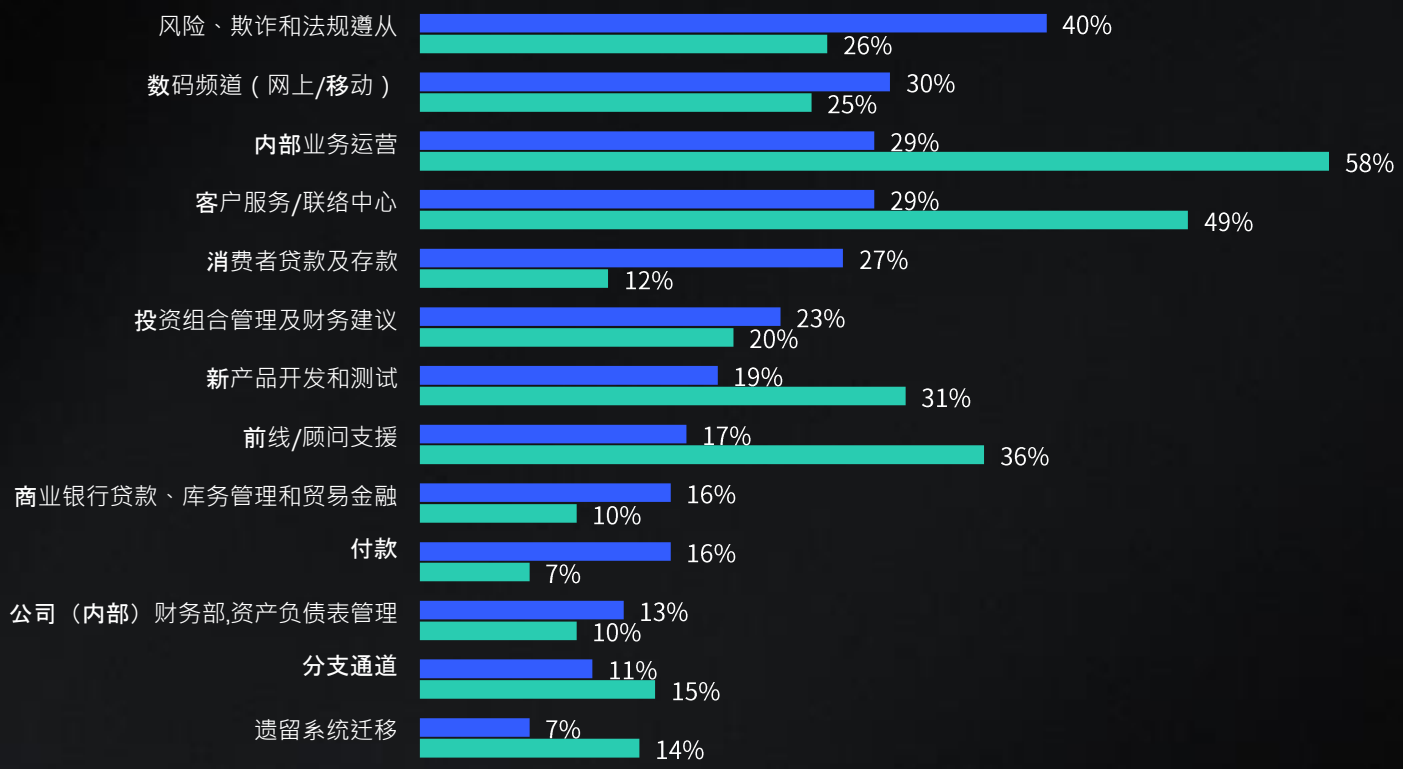
人工智能仍然是银行和投资服务行业最主要的新兴技术之一，77% 的 CIO 报告他们的企业已经或计划在未来 12 个月内部署人工智能。

资料来源：2024 年 Gartner 金融服务研究小组 AI 实施趋势调查

使用人工智能的领域

Q：在贵公司的哪些领域，AI 和 GenAI 计划目前正在进行或已经部署？

正在进行 AI 计划的银行/投资机构的高级行政人员百分比



资料来源：2024 年 Gartner 金融服务研究小组 AI 实施趋势调查

财务中常见的 AI 用例类型

- 客户信用管理
- 发票配对 — AP
- T&E 优化
- 现金申请

- 重复支付识别
- 合同分析
- 交易和余额监控
- 合规与风险监控

- 方案和资本支出规划
- 客户行为预测
- 预测和规范分析建模
- 预测（需求、收入、现金流、费用）

- 智能仪表板
- 聊天机器人/数字助理
- 决策支持
- 定价自动化
- 自然语言查询

资料来源：2024 年 Gartner 金融服务研究小组 AI

披荆斩棘：
通过网络安全威胁直接到优先事项

优先级	涉及的趋势
客户参与	1 2 3 5 6
弹性基础设施	1 4 5 6
数字信任和管理	2 3 4 5

	2023 年	优势	挑战	
1	开放银行 API	• 金融包容和无障碍 • 竞争和创新加剧 • 增强的客户体验	• 复杂合规 • 数据隐私和安全	
2	BaaS	• 降低应用成本和上市时间 • 多元化产品供应 • 增加收入 • 减少研发需求	• 数据隐私和安全 • 减少对技术的关注	
3	嵌入式金融	• 增强的客户体验 • 增加收入	• 合规运营，助力企业稳健前行 • 复杂的商业关系 • 数据隐私和安全	
4	云服务	• 更具可扩展性和弹性的基础设施 • 降低基础设施成本 • 快速支付处理	• 管理多个云提供商 • 数据隐私和安全	
5	数字银行	• 庞大的客户群 • 增强的客户体验 • 缩短服务上市时间	• 数据隐私和安全	
6	人工智能 (AI)	• 日常任务优化 • 竞争力和创新发展 • 改善的客户体验	• 数据隐私和安全	

内容

02

金融业的常见威胁

42%
2024 年的所有事件涉及勒索*

勒索软件

1/14
信息盗窃病毒感染可能导致卡数据被盗*

信息盗窃病毒

44%
2024 年的网络钓鱼尝试针对银行服务用户**

欺诈

30%
信息安全专业人员担心 DDoS 攻击增加**

DDoS

*根据卡巴斯基报告，2025 年

**根据卡巴斯基报告，2024 年

金融业的常见威胁

24%
2024 年的所有网络事件涉及网络钓鱼*

钓鱼

26%
过去两年的所有网络事件中，
都是由员工故意违反信息安全政策造成的**

内部人员

常见威胁通常是更
高级攻击的切入点

高级威胁

*根据 2025 年卡巴斯基 MDR 分析师报告

** 根据卡巴斯基人为因素 360⁰ 报告，2023

金融业的主要高级威胁

高级持续性威胁 (APT)

10 亿美元

Carbanak 是一场大规模的金融网络犯罪活动，造成 10 亿美元的总损失

2023 年

- LoneZerda
- BlindEagle
- Dark Caracal

2024 年

- Zanubis
- SideWinder

在过去两年里，卡巴斯基检测到五次针对金融组织的主要 APT 活动。

金融业的主要高级威胁

零日漏洞攻击

Google Chrome

2024 年，卡巴斯基专家在全球最受欢迎的浏览器中发现了一个零日漏洞*

供应链攻击

XZ Backdoor

可能是 2024 年最危险的供应链攻击，也是 Linux 系统历史上最重要的攻击之一*

*根据卡巴斯基报告，2024 年

金融业的主要高级威胁

银行业务木马

Grandoreiro

1700

金融机构及其用户于 2024 年在全球成为目标

郊狼

一个多阶段银行业务木马，
针对 60 多家金融机构的客户，
使用高度复杂的感染链*

*根据卡巴斯基报告，2024 年

2024 年的犯罪软件和金融网络威胁

1. 人工智能网络攻击增加
2. 以直接付款系统为目标的欺诈计划
3. 勒索软件目标选择
4. 巴西银行木马复苏
5. 开源后门软件包
6. 利用配置错误的设备和服务
7. 附属团体的流动组成
8. 采用不太流行/跨平台的语言
9. 黑客行动主义团体的出现

2025 年的犯罪软件和金融网络威胁预测

金融网络威胁的格局将在一年中发生怎样的变化？以下是我们预计在 2025 年保护企业和个人时面临的一些值得注意的攻击趋势。

1. 盗窃软件活动激增
2. 对中央银行和开放银行举措的攻击
3. 对开源项目的供应链攻击增加
4. 基于区块链的新威胁
5. 中文犯罪软件在全球范围内的扩展
6. 通过勒索软件进行合成数据投毒
7. 抗量子勒索软件
8. 勒索软件攻击者对合规的武器化
9. 勒索软件即服务泛滥
10. 在防御端有更多 AI 和机器学习
11. 针对智能手机的金融网络攻击激增

https://securelist.com/ksb-financial-and-crimeware-predictions-2025/114565/

网络攻击对金融组织的后果

- 勒索软件
- 信息盗窃病毒
- 欺诈
- 钓鱼
- 内部人员
- DDoS
- 高级持续性威胁 (APT)
- 零日漏洞攻击
- 供应链攻击
- 银行业务木马

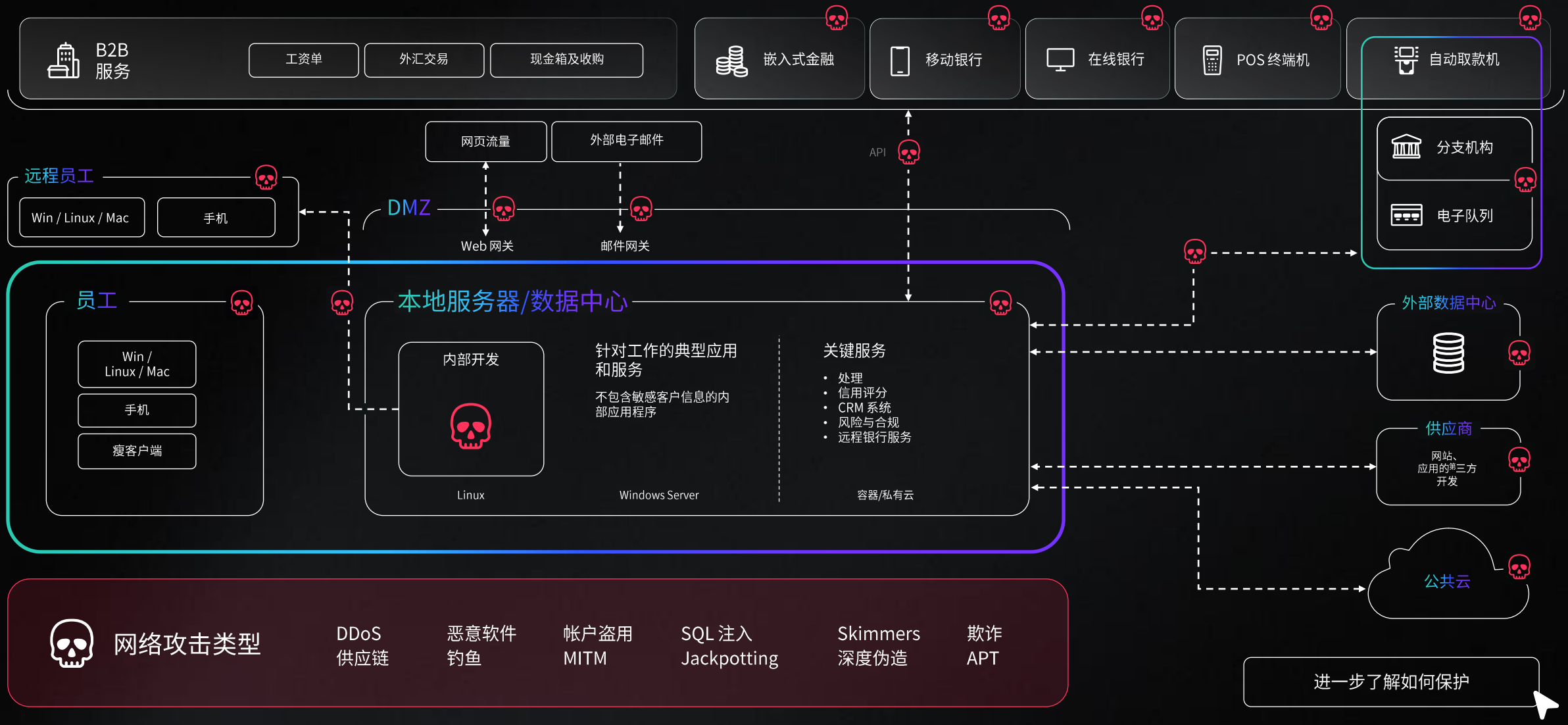
数据泄露

业务流程中断

盗窃钱财

声誉受损

具有潜在攻击入口点的基础设施示例和可能威胁



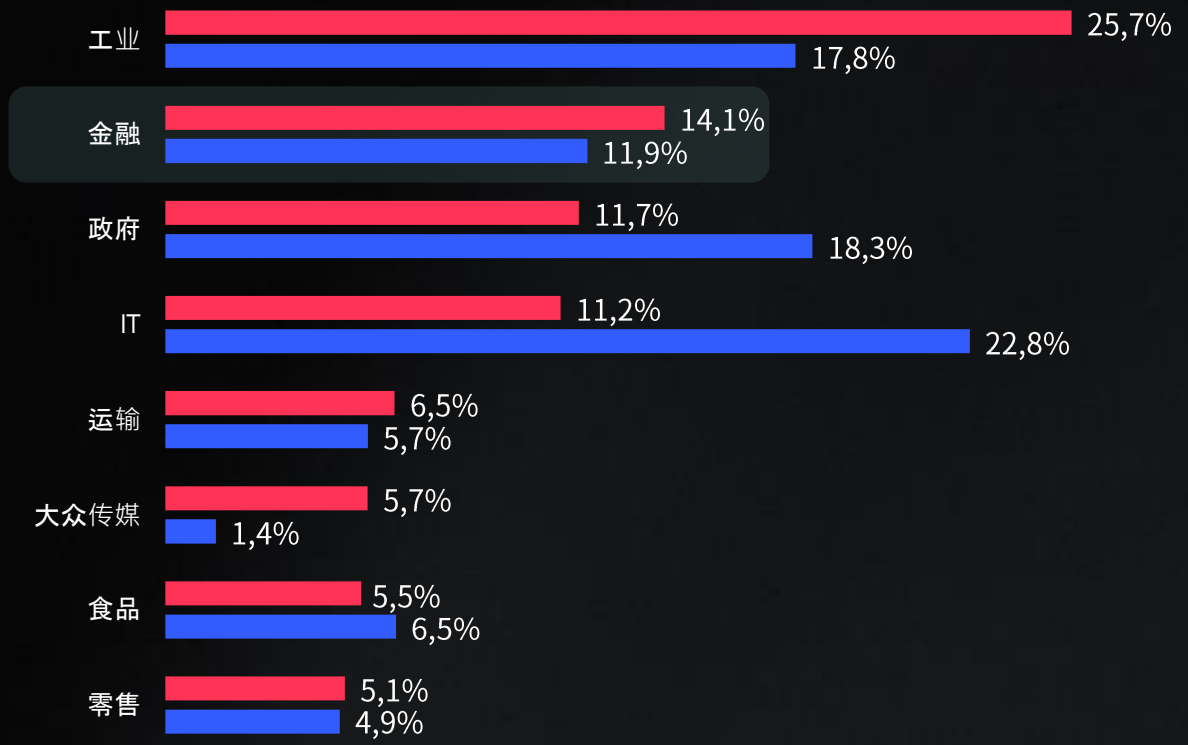
金融业的网络事件

近 270,000
2024 年金融行业观察到安全警报*

18.3%
2024 年金融行业报告事件的份额*

320 万美元
2024 年 BFSI 公司的平均亏损**

14.9%
2024 年金融行业报告高严重性事件的份额*



2

在此处放置

按普通事件

4

在此处放置

按严重事件

普通

某一特定行业的报告事件在所有行业的事件总数中所占的比例

严重

某一特定行业报告的高严重性事件在所有行业的高严重性事件总数中所占的比例

*根据 2025 年卡巴斯基 MDR 分析师报告

** 根据卡巴斯基 2024 年 IT 安全经济影响分析

金融组织中的知名恶意软件

QBot 银行木马

它也被称为 QuackBot 和 Pinkslipbot，首次发现于 2007 年，从那以后一直在不断演化。
目前，该木马通过计算机上已经存在的恶意软件以及社会工程和垃圾邮件传递给潜在的受害者。
卡巴斯基的家庭和企业解决方案使用多层方法（包括行为分析）来检测和阻止该威胁。

Prilex 恶意软件

Prilex 是一群网络犯罪分子，自 2014 年以来一直在寻找银行卡数据。最近，他们一直专注于通过 POS 终端进行攻击。Prilex 不断演化。他们的发展包括可通过 NFC 阻止交易。犯罪分子使用社交工程方法在 POS 终端上安装恶意软件。Prilex 的活动最常在拉丁美洲观察到。该恶意软件也在德国被使用过。

*APK（Android 软件包）是 Android 操作系统用于安装和分发应用程序的文件格式。

安全列表/卡巴斯基的威胁研究和报告

金融组织中的知名恶意软件

PixPirate Android 银行木马

PixPirate 属于最新一代的Android 银行木马，因为它可以执行自动转账系统（ATS）功能。此功能允许攻击者通过 Pix 即时支付平台自动执行恶意转账的过程，该平台由几家巴西银行积极使用。用于交付 PixPirate 的滴管应用伪装成身份验证器应用，通常通过钓鱼网站上的 apk* 文件分发。

Emotet 木马

借助 Emotet，网络犯罪分子可以访问其他人设备上的机密数据。Emotet 因能够欺骗基本的防病毒程序而臭名昭着，因此他们无法识别它。一旦得到下载，该程序的行为就像一个计算机蠕虫，试图渗透到网络上的其他设备。Emotet 主要通过网络钓鱼电子邮件传播。电子邮件包含恶意链接或受感染的文档。Emotet 在 2014 年首次被发现，当时它攻击了德国和奥地利银行的客户。现在，Emotet 已经遍布全球，可以攻击任何行业的公司，包括政府机构。

*APK（Android 软件包）是 Android 操作系统用于安装和分发应用程序的文件格式。

安全列表/卡巴斯基的威胁研究和报告

CISO 调查

对于银行来说，
目前什么是最大的的网络安全挑战?

快速的行业数字化

不断扩大和日益复杂的基础设施需要更有力的保护。

严格的监管要求

安全系统的构建必须符合监管机构的要求。

如今，数字化帮助金融组织扩展其服务产品、自动化日常流程并节省资源。然而，它也增加了网络风险。

数字化转型必须考虑网络安全风险，同时安全策略必须与监管要求保持一致。

基于卡巴斯基进行的深入访谈。

金融组织面临的主要数字化挑战

挑战

- 攻击面扩大
- 新的漏洞和威胁
- 复杂基础设施的管理和保护
- 老系统
- 知识差距
- 专业人员短缺
- 预算限制
- 严格规定

可能面临的风险

- 定向攻击可能此时就在您的系统中
- 恶意的内部活动已是司空见惯
- 数据中心攻击可能造成大规模损失
- 勒索软件攻击会锁定关键的数据和设备
- 机密数据丢失不仅仅是金钱损失（信誉、客户）
- 必须完全克服合规和法规挑战

所需操作示例

- 整体基础设施防御
- 保护网上银行平台及其客户
- 透过不同渠道（例如 ATM、PoS 及网上银行）保障金融交易的安全
- 保护客户数据免受泄露和窃取
- 应对与第三方供货方和供应商相关的风险
- 确保符合新兴法规，包括 GDPR、SOX、PCI-DSS等。

符合标准

我们认识到遵守金融业监管要求的重要性。

这些标准构成了金融部门网络安全抵御能力的基础，确保保护支付系统、客户数据和业务流程免受网络威胁。

合规文档

标准

- SO/IEC27001：2022-信息安全、网络安全和隐私保护 — 信息安全管理系统 — 要求
- ISO/IEC27002：2022 — 信息安全、网络安全和隐私保护 — 信息安全控制
- PCI DSS（支付卡行业数据安全标准）v4.0

内容

03

金融业可如何抵御现代网络攻击？

实施全面战略，为内部专家提供装备、信息和准备，以应对当今的各种威胁。

0

准备

检查

通过对整个金融基础设施进行盘点，优化流程并更新信息资产。
这可以由内部或外部专业人员完成。

1

技术

解决方案

为内部安全专家配备必要的
工具来处理网络事件

2

知识

培训和分析

掌握最新威胁，
提高您的安全专业人员
应对网络事件的能力

3

专业知识

服务

依靠外部专家进行安全分析、
操作协助以及额外的保护和建议

按照你的优先事项进行全面防御

了解有关产品和服务的更多信息（第 57-98 页）

1. 技术
2. 知识
3. 专业知识

为了应付日益增加的网络犯罪活动，金融组织需要应用生态系统方法

1

全面防范各种威胁

针对广泛威胁的基本保护

- 卡巴斯基 混合云安全
- 卡巴斯基 网络安全解决方案 – 邮件服务器安全
- 卡巴斯基 移动安全管理

针对复杂威胁的高级防御

- 卡巴斯基 统一监控和分析平台
- 卡巴斯基 反针对性攻击

- 卡巴斯基 新一代安全 EDR 基础版
- 卡巴斯基 新一代安全 EDR 优选版
- 卡巴斯基 新一代安全 EDR 专业版
- 卡巴斯基 新一代安全 XDR 专家版

针对行业需求量身定制的解决方案

- 卡巴斯基 嵌入式系统安全
- 卡巴斯基 移动安全 SDK
- 卡巴斯基 欺诈防御
- 卡巴斯基 来电显示 SDK / REST API
- 卡巴斯基 分布式拒绝服务 (DDoS) 保护
- 卡巴斯基 扫描引擎

超越传统网络安全

- 卡巴斯基 容器安全
- 卡巴斯基 SD-WAN
- 卡巴斯基 瘦客户端

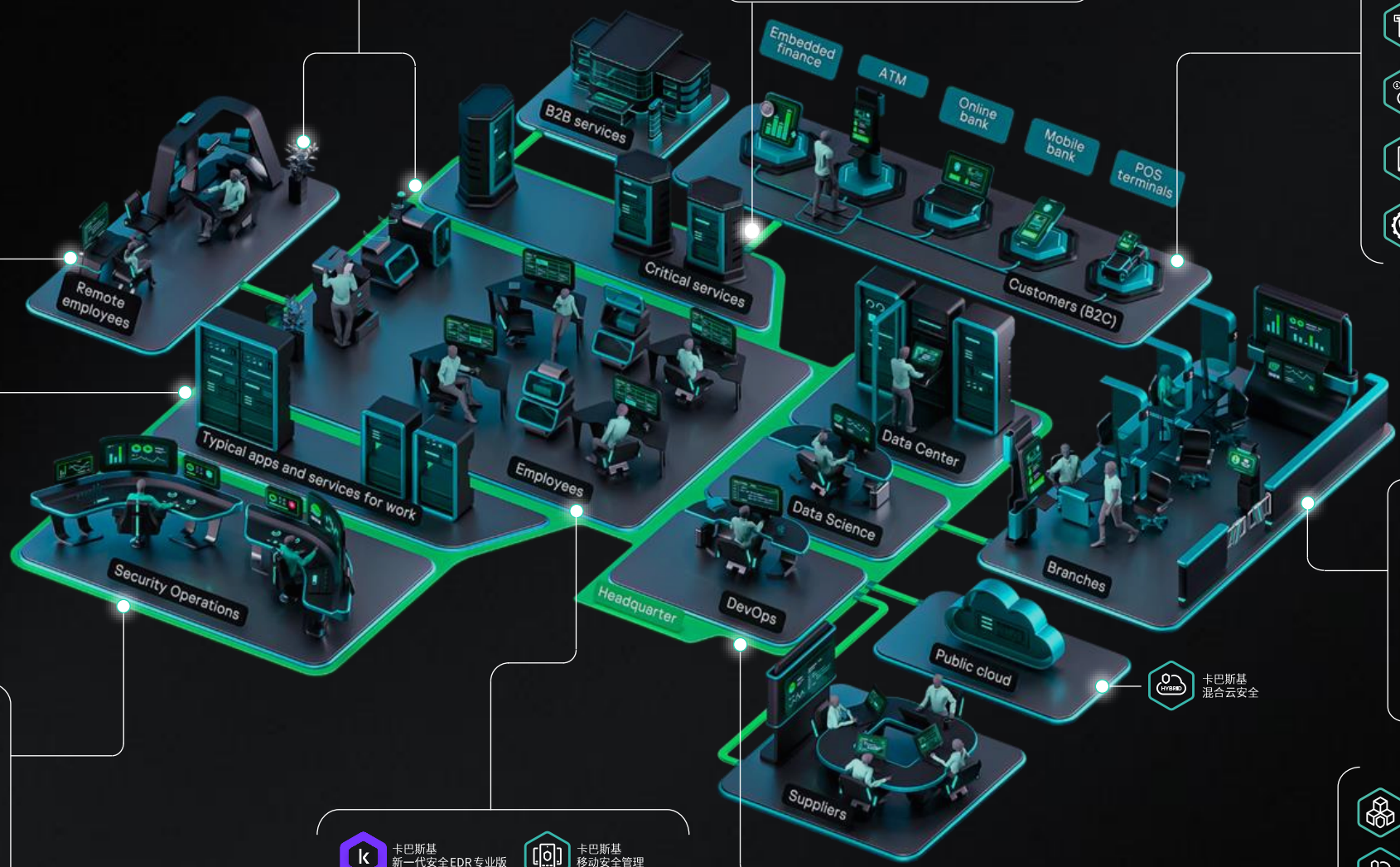
2

- 意识
  - 卡巴斯基 安全意识
- 威胁情报
  - 卡巴斯基 威胁情报
- 培训
  - 卡巴斯基 网络安全培训

3

- 评估
  - 卡巴斯基 安全评估
  - 卡巴斯基 支付系统安全评估
- 托管安全
  - 卡巴斯基 托管检测和响应
- 事件响应响应
  - 卡巴斯基 事件响应
- 入侵评估
  - 卡巴斯基 损害评估
- SOC 咨询服务
  - 卡巴斯基 SOC 咨询
- 专业服务
  - 卡巴斯基 专家服务

卡巴斯基如何保护金融组织的例子



卡巴斯基 瘦客户端

卡巴斯基 DDos防护

卡巴斯基 欺诈防御

卡巴斯基 扫描引擎

卡巴斯基 嵌入式系统安全

卡巴斯基 支付系统安全评估

卡巴斯基 移动安全 SDK

卡巴斯基 来电显示 SDK

卡巴斯基 新一代安全EDR基础版

卡巴斯基 新一代安全EDR优选版

卡巴斯基 邮件服务器安全

卡巴斯基 新一代安全EDR优选版

卡巴斯基 嵌入式系统安全

卡巴斯基 移动安全管理

卡巴斯基 SD-WAN

卡巴斯基 混合云安全

卡巴斯基 统一监控和分析平台

卡巴斯基 新一代安全EDR专业版

卡巴斯基 反针对性攻击

卡巴斯基 威胁情报

卡巴斯基 事件检测和响应

卡巴斯基 事件响应

卡巴斯基 SOC 咨询

卡巴斯基 安全服务

卡巴斯基 新一代安全EDR专业版

卡巴斯基 移动安全管理

卡巴斯基 新一代安全EDR优选版

卡巴斯基 自动化安全意识平台

卡巴斯基 容器安全

卡巴斯基 混合云安全

卡巴斯基 开源软件威胁数据源

您通过我们的网络安全策略可获得的结果

- 容错基础设施
- 敏感数据受到保护
- 降低了财务损失风险
- 您遵守规定

- 业务连续性和服务可用性
- 客户和合作伙伴信任您
- 您可以专注于自己的关键优先事项

内容

04

卡巴斯基在金融行业的经验

我们的技术和专业知识有效将金融组织的风险降低到最低水平。
我们解决方案的功能符合全球最佳保护实践。

>15 年

> 100 个国家

>3,400
BFSI 遍布
世界各地

~1900
在独联体

~430
在亚太地区

~530
在欧洲

~360
在美洲

~230
在 META

成功案例

文档链接

意大利银行

Banca Popolare di Sondrio

挑战

- 对以前的 IT 安全解决方案不满
- 前供应商没有清晰的路线图
- 不确定供应商是否可跟上时代
- 该银行希望在短时间内找到解决方案，既能提供有效的攻击保护，同时又易于管理

银行通过 KES 产品开始熟悉卡巴斯基。
该解决方案的成功实施给我们的新客户留下了深刻的印象，
他们后来购买了 KPSN 和 KATA

卡巴斯基解决方案

- 卡巴斯基 反针对性攻击
- 卡巴斯基 EDR 专业版
- 卡巴斯基 企业用端点安全

超过2600
员工

330
分支机构

2
数据中心

成功案例

文档链接

多米尼加共和国的银行

挑战

- 全国范围内对金融业的网络攻击增加
- 业务发展和服务范围扩大，需要实施可靠的网络安全解决方案
- 银行缺乏最新的解决方案来帮助控制整个边界

“

该银行的首席技术官："公司的业务和战略领域以技术为导向，以安全为核心。我们目标的影响涉及许多需要更高安全性的金融工具。我们需要站在最前沿"

"卡巴斯基提供了一个综合解决方案，不仅包括产品，还包括服务

卡巴斯基解决方案

- 卡巴斯基 反针对性攻击
- 卡巴斯基 托管检测和响应
- 卡巴斯基 企业用端点安全
- 卡巴斯基 专家服务

\+ 通过技术客户经理增强了支持

500	31
员工	分支机构

成功案例

文档链接

孟加拉国伊斯兰银行

挑战

- 国家基础设施薄弱，缺乏明确监管
- 缺乏对日常活动的中央控制
- 缺乏对其 ICT 网络和系统的强大保护

不计其数大规模的破坏性感染，以及分行完全关闭的风险，阻碍了银行建立网上银行服务的努力

后果

- 本地总部网络和各分支网络遭到许多病毒、蠕虫和特洛伊木马攻击
- 不受控制地访问载有病毒的网页和广泛使用未经授权的 USB 设备

成果

- 系统现在运行平稳安全
- 使用受感染的可移动设备被禁止，访问恶意网站受到限制

为了解决当前问题和防止未来的潜在问题，
该银行集成了 Kaspersky Endpoint Security for Business

卡巴斯基解决方案

卡巴斯基
企业用端点安全

2600+
员工

119
分支机构

1000+
用户

内容

05

为何选择卡巴斯基?

我们独特的信息安全专家团队保护世界免受最复杂和危险的网络威胁。积累的知识库丰富了我们的解决方案和服务，使其质量达到无与伦比的水平

>27 年

建设更安全的世界

>467,000

卡巴斯基日均检测出的新恶意文件数量

>49 亿

卡巴斯基在 2024 年检测到的网络攻击数量

>220,000

全球企业客户选择我们的保护

>900

与 APT 相关的活动组和操作由我们监控

5

独一无二的专业中心

无与伦比的专业知识

5个独一无二的专业中心

我们拥有一支独一无二的专家团队，他们在五个专业中心紧密协作，凭借深厚的专业知识与精湛技能，共同应对最为复杂、危险的网络威胁。

这种协作方法加强了我们最先进的保护技术并确保我们的产品和解决方案为安全性和可靠性设定了行业标准。

卡巴斯基专业技术中心：每个中心都拥有密封点

GREAT

突出的
APT 发现

作为 APT 研究的
副产品发现了不计
其数的 0 日 CVE

Threat Research

在指标成功和年度
检测统计数据方面
持续位列前三

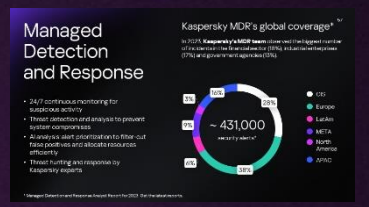
安全研究、
安全开发

AI Technology Research

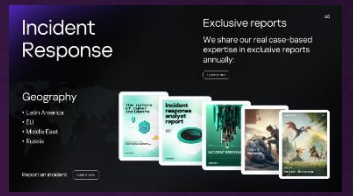
人工智能在网络安全
中的广泛应用历史

90% 的卡巴斯基产品
以某种方式使用 AI

Security Services



全球直供专业知识
（以服务形式）



通过报告公开提供独
特的现实生活经验

ICS CERT

首个商业 ICS CERT 及作
为 ICVE 权威获得认可

工业 CVE 发现领头羊

汇聚专业技术知识，铸就安全基石

研究和调查

世界领先的威胁研究和事件调查专业知识是我们产品组合的核心

无与伦比的全球专业知识使我们的客户领先于威胁，并通过我们的产品和服务在整个事件响应周期中得到支持

由 AI 驱动的安全方法

AI 安全技术 – 内置于我们的解决方案中

从利用 AI 增强的威胁发现和警报分类，到由生成式 AI (GenAI) 驱动的威胁情报，我们多年来一直致力于 AI 领域，并且始终保持领先地位

软件开发安全

从安全的软件开发生命周期到设计即安全

开发安全是我们产品设计流程的指导原则，使我们能够创建完全安全的系统，让客户安心无忧

20 多年来，卡巴斯基使用机器学习和人工智能保持领先于不断演化的网络威胁

我们的专门人工智能中心致力于推动创新，同时确保人工智能和机器学习得到安全、符合道德规范的使用。

重点关注领域

推进人工智能网络安全解决方案

开发增强人工智能的安全和负责任使用的技术

跟踪人工智能威胁以预测新出现的攻击媒介

使用卡巴斯基的 LLM 基础设施进行 GenAI 研究

建立 AI 系统安全部署指南

人工智能使我们能够比其他任何人更好保护客户的 5 个关键方法

人工智能是产品组合的核心

1. 人工智能和机器学习支持的威胁发现
2. 通过 AI 提高 SOC 效率
3. 生成式人工智能用于威胁情报和安全运营
4. 安全的人工智能方法及方法论
5. 在 IT 和 OT 环境中进行基于 AI 的行为分析和异常检测

透明且获得独立认可

Proven.
Transparent.
Independent.

卡巴斯基全球透明度倡议建立在具体、可操作的措施之上，允许利益相关者验证我们的产品、内部流程和业务运营的可信度。

13

全球各地的透明中心

定期独立评估

- SOC 2 审计
- ISO 27001 认证

了解更多

Bug赏金

卡巴斯基始终推行开展公开的漏洞奖励计划

重要认可

卡巴斯基产品定期接受领先研究公司的独立评估，我们的网络安全专业知识得到了顶级行业分析师的一致认可。

久经考验，屡获殊荣

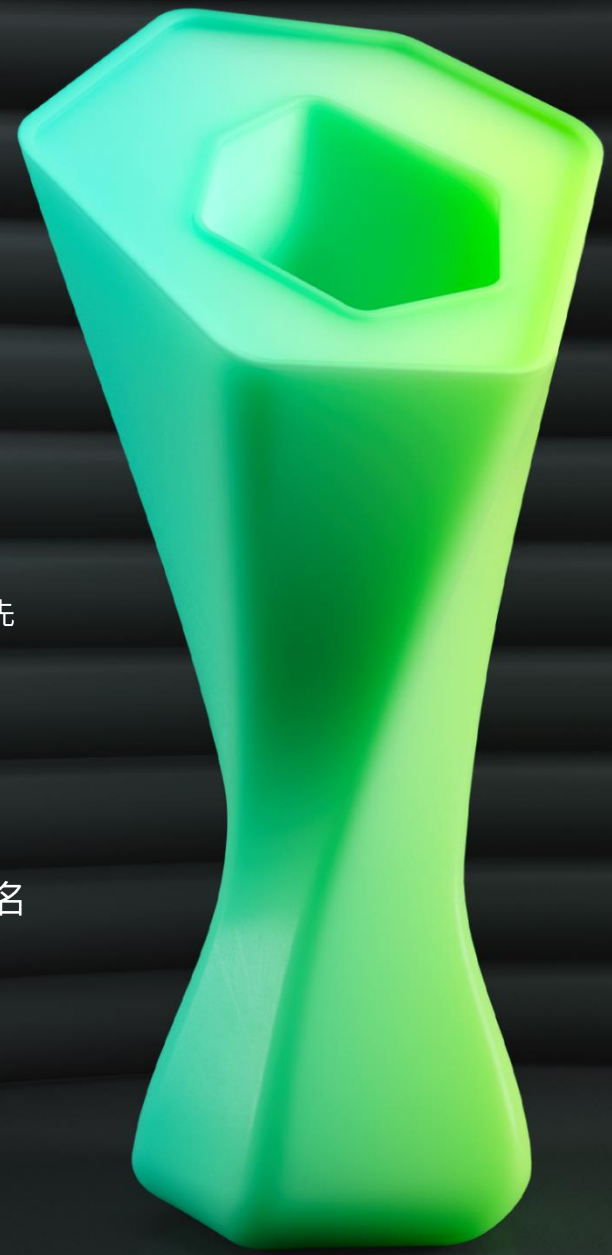
十多年来，卡巴斯基产品参与了 927 项独立测试和评审，获得 680 项第一名和 779 项前三名，见证了我们行业领先的保护能力。

在 2023 年

100
项测试和评测

93
次第一名

了解更多



积极的行业贡献者

作为全球威胁情报领域的关键和积极参与者，我们与更广泛的网络安全社区密切合作，打击全球网络犯罪。

INTERPOL

PARIS CALL
FOR TRUST AND SECURITY IN CYBERSPACE
11 • 12 • 2018

industrial internet CONSORTIUM

AFRIPOL

Coalition Against Stalkerware

我们与国际刑警组织、执法机构、CERT 和全球 IT安全社区等国际组织合作，共同开展网络犯罪调查和行动。

MITRE | ATT&CK®

我们为包括 MITRE 在内的全球计划提供关键的网络威胁情报，以提高 ATT&CK 框架的准确性。

我们的工作以负责任披露漏洞的道德原则为指导。

卡巴斯基通过识别和帮助修复 Adobe、微软、谷歌、苹果等领先公司的零日漏洞来加强各个行业的安全性。

今日推动创新，为明天的挑战做好准备

专利，发明，我们自己的操作系统 (OS)

1,500+

成功注册的专利

500+

2005-2024年 间的发明

KasperskyOS
Be Immune

我们的突破性 KasperskyOS 实现了从网络安全到网络免疫的转变。

关于 KasperskyOS

具有增强网络安全要求的微内核操作系统

- 微内核架构最大限度地减少了攻击面和漏洞风险，安全监视使未经授权的操作变得不可能
- 由卡巴斯基从头开始开发，内核中不包含任何第三方代码
- 创建网络免疫产品和解决方案的基础

kaspersky cyber immunity

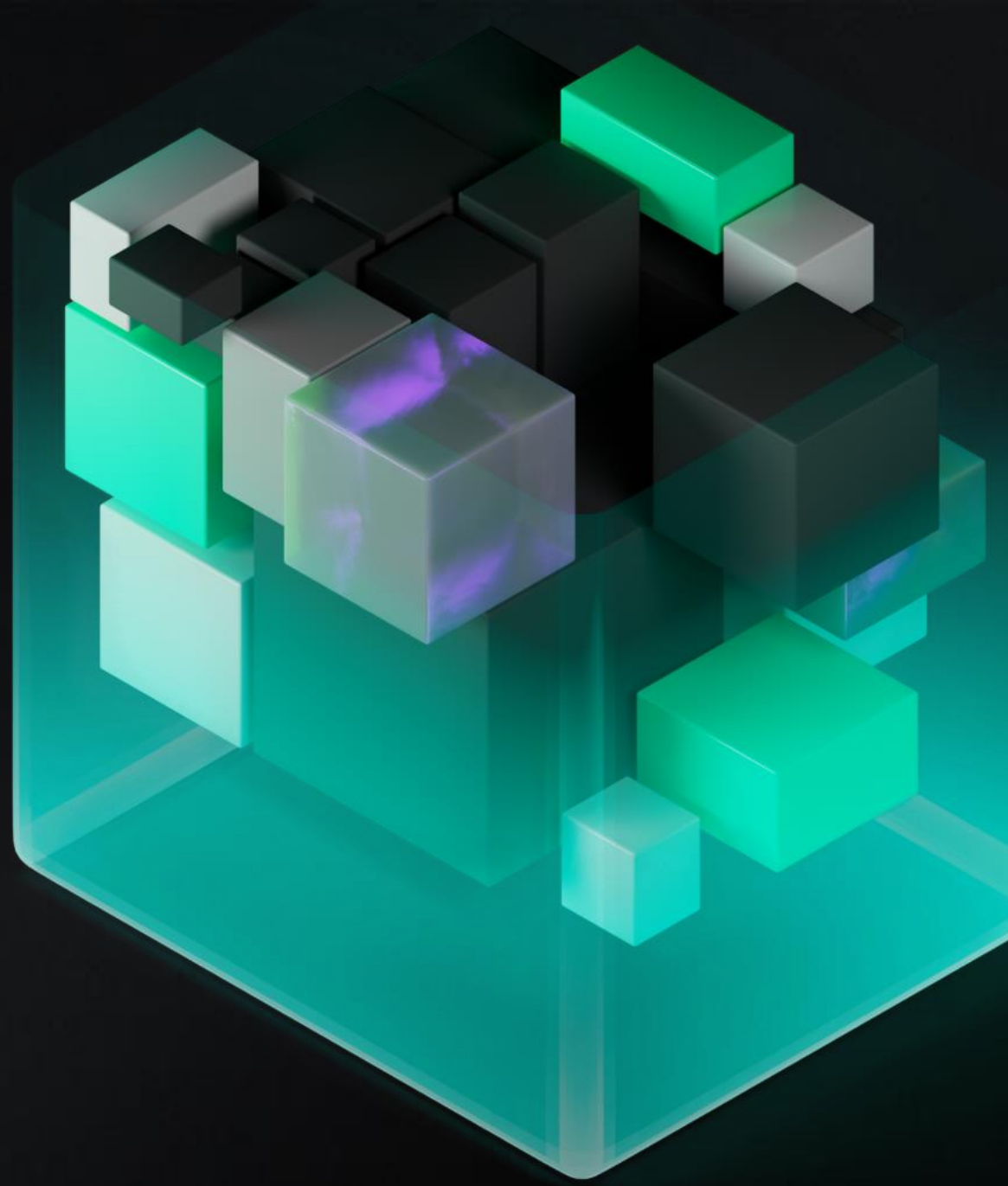
网络免疫是我们开发设计即安全解决方案时所采用的方法

网络免疫系统的关键资产最初能够抵御甚至是未知的威胁，并确保在攻击下稳定工作。

内容

06

卡巴斯基产品组合
支持您的优先事项



有效的网络安全策略，保障金融服务的完整性。
工具

全面防范各种威胁

对所有可能的攻击媒介进行网络控制，保护所有资产，覆盖所有安全场景。

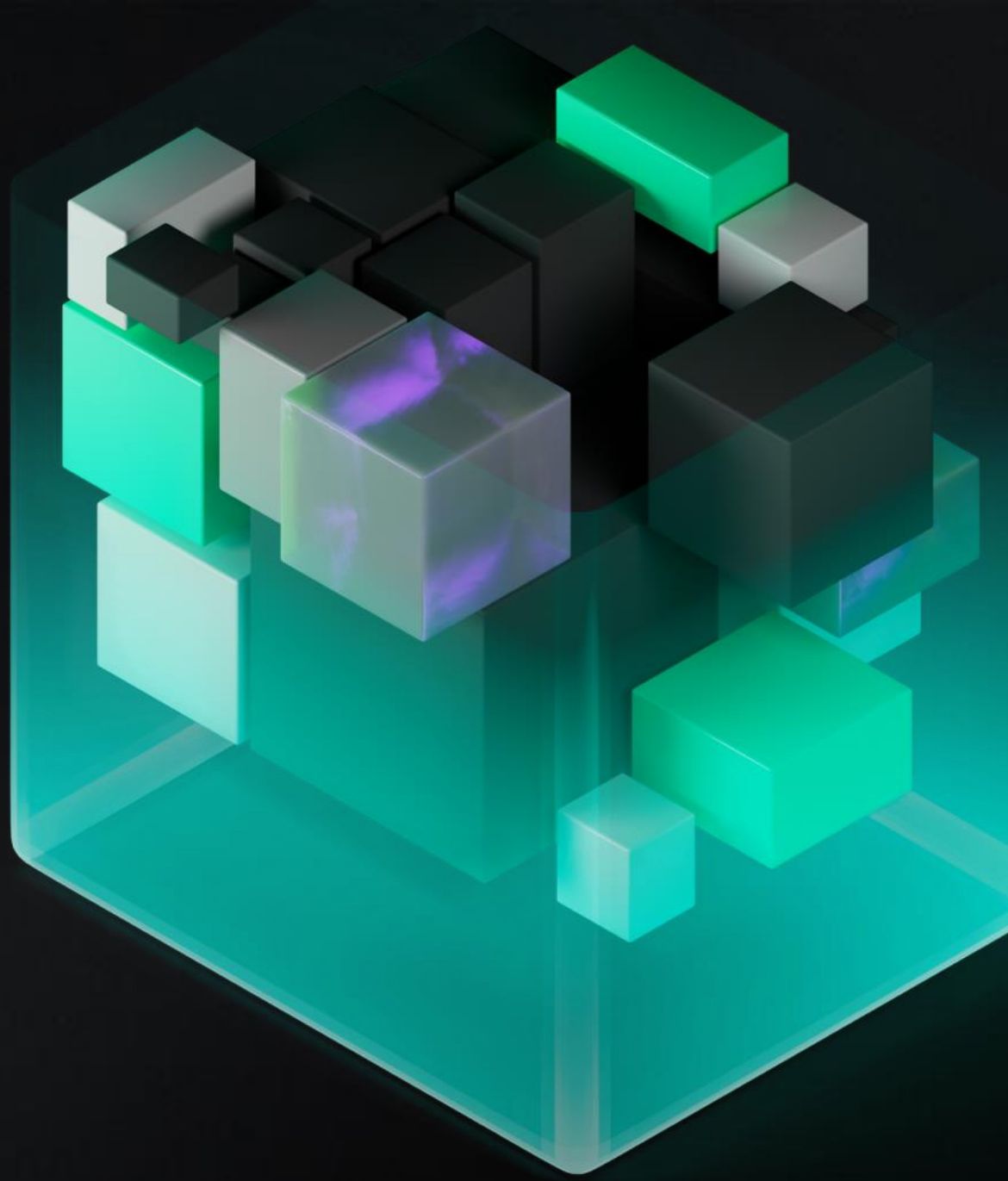
针对行业需求量身定制的解决方案

考虑到金融业的行业特性和监管要求，以及威胁格局的特点。

超越传统网络安全

我们不仅保护金融组织的 IT 技术和流程，还提供一个富有凝聚力的安全网络，确保今天打造面向未来的网络免疫解决方案。

全面防范
各种威胁



卡巴斯基新一代安全

将强大的端点保护和控制、EDR 的透明度和速度以及 XDR 的可见性和强大工具结合在一起，产品层级简单明了。

强大、经过验证的端点防御

卡巴斯基
新一代安全 EDR 基础版

适用于小型网络安全团队的 EDR

卡巴斯基
新一代安全 EDR 优选版

适用于大型网络安全或 SOC 团队的终极工具

卡巴斯基
新一代安全 XDR 专家版

卡巴斯基
新一代安全 EDR 专业版

卡巴斯基新一代安全产品层级的比较

1 技术

卡巴斯基
新一代安全 EDR 基础版

卡巴斯基
新一代安全 EDR 优选版

卡巴斯基
新一代安全 XDR 专家版

每层都包括上一层的特性和功能

卡巴斯基新一代安全 EDR 基础版 提供直接、经济实惠的保护，确保您的业务平稳运行，同时卡巴斯基还可以阻止勒索软件、无文件恶意软件、零日攻击和其他新兴威胁。

卡巴斯基新一代安全 EDR 优选版 提供强大的端点保护、经过改进的控制、培训、补丁管理等，这些都通过关键 EDR 功能得到增强。

威胁可见性、调查和响应简单、快速、具有导向性，有助于以最少的资源快速转移攻击。

卡巴斯基新一代安全 XDR 专家版 提供企业基础设施中端点的全面概览以及每个调查阶段的可视化。它配备了先进的检测引擎和根本原因分析工具，确保有效的威胁检测和精简的调查。

卡巴斯基新一代安全 XDR 专家版 将一流的端点保护、电子邮件和混合环境的安全性与卡巴斯基新一代安全 EDR 专业的高级检测功能相结合。它包括强大的关联引擎、自动响应，并支持第三方连接器集中管理数据。

返回计划

1 技术

卡巴斯基
新一代安全 EDR 基础版

产品页面

卡巴斯基新一代安全 EDR 基础版拥有强大的基于机器学习的端点保护、灵活的安全控制和 EDR 根本原因分析工具，为您提供了最直接的方式来构建强大的网络安全核心。简单的控制台、云或本地部署以及各种提升工作生活质量的功能，所有这些可降低复杂性并提高效率。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 知识差距
- 专业人员短缺
- 严格规定
- 预算限制

我们如何帮助

确保金融基础设施中每个端点的安全性

为集中式端点管理提供单一控制台

防范漏洞利用和加密，评估和修复端点级别的漏洞

帮助监控服务器上运行的程序、设备和应用程序

支持所有主要操作系统和虚拟化工具

返回计划

1 技术

卡巴斯基
新一代安全 EDR 优选版

产品页面

卡巴斯基新一代安全 EDR 优选版提供强大的端点保护、经过改进的控制、培训、补丁管理等，所有这些都通过关键 EDR 功能得到增强。威胁可见性、调查和响应简单、快速、具有导向性，可帮助您以最少的资源快速转移攻击。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 知识差距
- 专业人员短缺
- 严格规定
- 预算限制

我们如何帮助

确保您的金融基础设施中每个端点的安全性

为集中式端点管理提供单一控制台

防范漏洞利用和加密，评估和修复端点级别的漏洞

监控服务器上运行的程序、设备和应用程序

支持所有主要操作系统和虚拟化工具

阻止文件、电子邮件和 Web 威胁，防止入侵

卡巴斯基
新一代安全 EDR 专业版

产品页面

卡巴斯基新一代安全 EDR 专业版是一款强大的端点检测和响应 (EDR) 解决方案，与端点保护平台 (EPP) 配合使用，可阻止大规模攻击、检测更复杂的网络威胁，帮助您主动调查事件，并为 IT 专业人员配备综合响应工具。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 专业人员短缺
- 严格规定

返回计划

1 技术

我们如何帮助

有效阻止大规模威胁，检测和帮助调查整个端点基础设施的复杂威胁

通过将 EPP 和 EDR 技术结合到单一解决方案中，增强对复杂威胁和目标攻击的检测

提供金融组织基础设施中所有工作的全面可见性

优化端点级别的事件处理成本

提供用于主动威胁搜寻和回顾性分析的工具

支持各种响应措施

返回计划

1 技术

卡巴斯基
新一代安全 XDR 专家版

产品页面

卡巴斯基新一代安全 XDR 专家版是新一代安全产品线中最先进的一款强大的网络安全工具，专为您的 SOC 团队打造。它利用各种响应工具和数据源（包括端点、网络和云数据），通过完全可视性、实时关联和自动化，全面控制受保护的基础设施。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 预算限制
- 专业人员短缺
- 严格规定
- 复杂基础设施的管理和保护

我们如何帮助

提供整个受保护企业基础架构的全面概述，以便识别复杂和持续的威胁，提高 MTTD

通过卓越的端点、混合云和电子邮件安全，确保在不打扰您的信息安全专家的情况下自动停止大规模威胁

利用行动手册和高级案例管理，帮助建立响应流程以改进 MTTR 并最大限度地减少频繁场景中的错误

通过我们的现场安装，提供数据主权，确保客户数据处理的机密性

利用 AI 组件快速检测基础设施中的可疑活动，帮助最大限度地减少网络事件造成的潜在危害

利用内置和自定义连接器的强大功能，连接来自卡巴斯基和第三方供应商的数百个来源，以减少安全团队必须执行的配置相关任务的数量

卡巴斯基
移动安全管理

产品页面

返回计划

1 技术

卡巴斯基移动安全管理将领先的安全技术与移动生命周期管理最佳实践相结合，为管理您的移动舰队提供统一解决方案。它支持所有主要平台，并通过符合监管建议来确保合规性。轻松集成到卡巴斯基安全生态系统中，将企业移动性转变为 IT 基础架构的安全有机组成部分，简化工作流程并提高整体效率。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 老系统
- 预算限制
- 严格规定
- 攻击面扩大

我们如何帮助

通过单一集成解决方案为不同类型的移动设备提供强大的安全性和管理

通过统一管理和 XDR 生态系统集成，实现更有效的事件遏制和问责制

通过自动化重复的生命周期管理任务，降低运营成本和员工的工作量。

降低可能危害安全的人为错误，这种错误在银行和金融业所施加的严格条件下不可接受

通过一套全面的管理、保护和安全策略实施工具，帮助确保符合机构和监管的要求

返回计划

1 技术

卡巴斯基 混合云安全

产品页面

该解决方案可降低云环境中固有的安全风险，包括恶意软件、网络钓鱼和网络威胁，并减少虚拟化资源消耗。卡巴斯基混合云安全可提高业务弹性，并为混合环境提供有效保护，无论使用何种云。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 攻击面扩大
- 新的漏洞和威胁
- 专业人员短缺
- 严格规定

我们如何帮助

保护混合环境，无论 工作负载类型和您使用哪种云

支持各种云平台和虚拟化环境

提高您的混合基础设施的可见性并减少 IT 事件

提供单一管理控制台适用于您的整个云基础架构

通过优化的轻量级代理最大限度地提高混合基础设施投资的回报

持续合规助力，构建安全可信的软件环境

返回计划

1 技术

卡巴斯基
邮件服务器安全

产品页面

卡巴斯基邮件服务器安全可确保安全高效地使用企业的主要通信通道电子邮件，打击垃圾邮件、通过电子邮件传播的感染、各种形式的网络钓鱼和其他威胁。它还实现了对信息传输的控制，有助于降低业务中断、由于诈骗造成财务损失和数据泄露的风险。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 攻击面扩大
- 新的漏洞和威胁
- 预算限制
- 老系统

我们如何帮助

在不牺牲通信速度的情况下，提供可信、安全的企业电子邮件交换

使用高级内容过滤规则降低感染风险和数据泄漏

使用机器学习技术，防御各种攻击，检测和阻止恶意软件、勒索软件、垃圾邮件、网络钓鱼、BEC、APT 等

利用可信赖的外部威胁情报来源以及我们自己的尖端研究和威胁情报数据

通过与 KATA 集成，可以在隔离环境中分析对象，甚至可以检测到精心伪装的恶意软件

可轻松与现有基础设施集成，作为已部署的电子邮件安全解决方案的补充

卡巴斯基
反针对性攻击

产品页面

全面的反 APT 解决方案，防止复杂的网络威胁，提供网络沙盒、先进的 NDR 和 EDR 功能。通过覆盖网络和端点级别的主要攻击入口点，卡巴斯基反针对性攻击解决方案可确保整个 IT 基础设施的全面可见性和对针对性攻击的全面防御。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 攻击面扩大
- 新的漏洞和威胁
- 预算限制
- 严格规定
- 专业人员短缺

返回计划

1 技术

我们如何帮助

提供对针对性攻击的高级保护 在网络，邮件 和端点级别

通过主动风险检测和寻找威胁和异常情况，最大限度地减少泄漏和财务损失的风险

使用先进的检测技术和主动式威胁搜索，揭露针对您的基础设施的攻击

分析网络流量并识别外部和内部网络威胁

提供对网络中的所有设备、相关威胁和需要优先关注的资产的全面概述

使用针对金融组织的当前 APT 和威胁的全球分析数据

返回计划

1 技术

卡巴斯基
统一监控和分析平台

产品页面

卡巴斯基统一监控和分析平台是高性能的下一代 SIEM 解决方案，专为集中收集、分析和关联来自各种来源的信息安全事件而设计，以识别网络事件并及时处理。这是一项适用于任何构建自己的 SOC 的金融组织的关键技术。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 预算限制
- 专业人员短缺
- 严格规定

我们如何帮助

通过收集、规范化、存储和关联来自不同来源的事件，检测对银行基础设施的攻击

通过及时发现欺诈交易并暂停其处理以及任何其他网络犯罪活动，最大限度地减少欺诈交易造成的损失

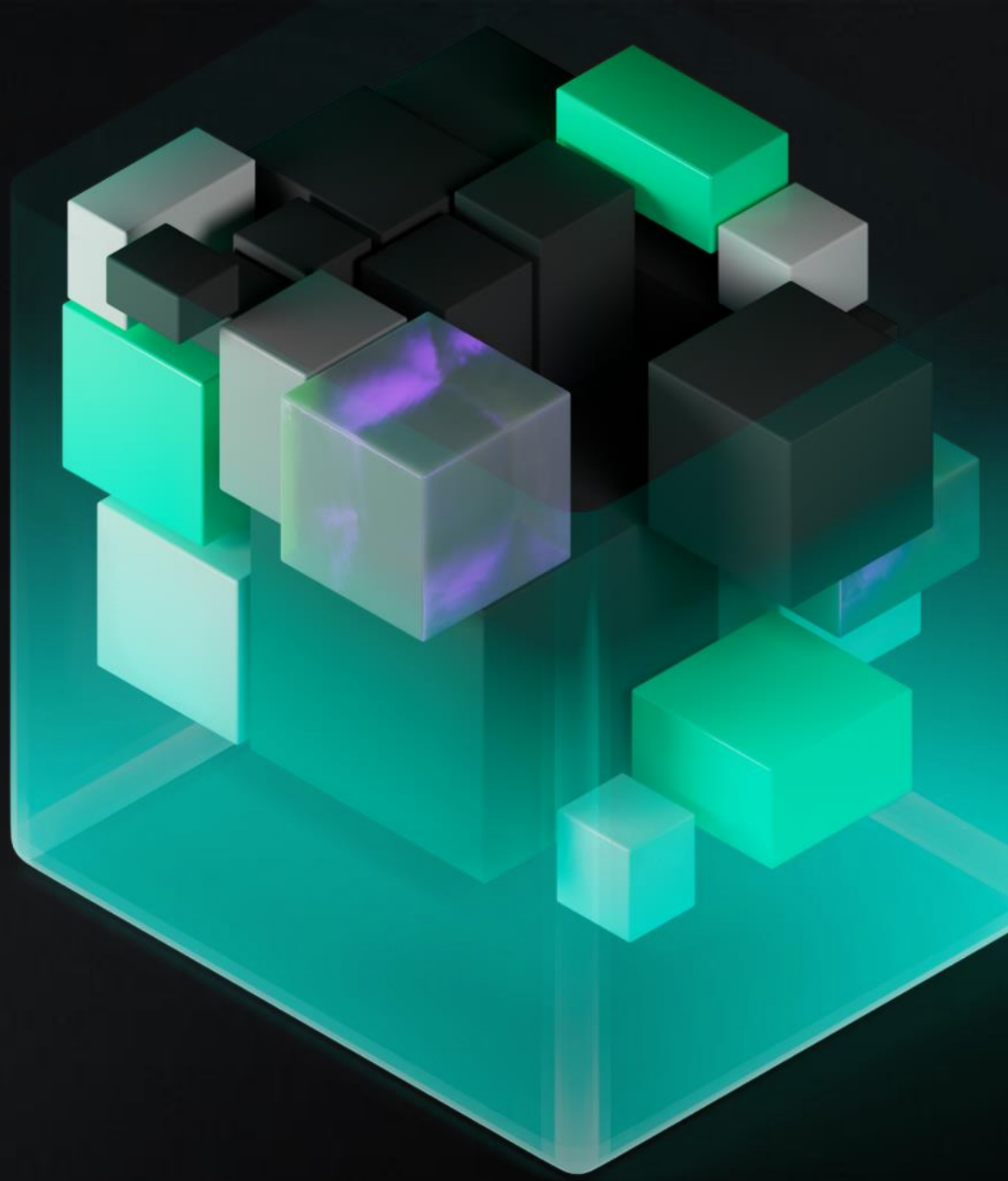
利用 AI 优化日常监控、警报优先级排序和主动搜索流程

通过轻松搜索存储数据，提供可靠且经济高效的日志存储解决方案

提高对金融组织基础设施的复杂攻击的检测速度

通过安全的本地日志存储，帮助您以经济高效的方式满足监管要求

针对行业需求
量身定制的解决方案



卡巴斯基
嵌入式系统安全

产品页面

卡巴斯基嵌入式系统安全可针对 ATM 和支付终端等嵌入式设备面临的独特挑战提供量身定制的强大保护。它可保护基于 Windows 的设备（包括那些运行过时版本（如 Windows XP）的设备）和基于 Linux 的设备。多层技术堆栈可为不同功率水平的设备提供最佳的安全性，同时也支持合规性。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 老系统
- 严格规定
- 攻击面扩大

返回计划

1 技术

我们如何帮助

通过为您的混合舰队（包括系统资源有限的低功耗 ATM 和 PoS）提供有效保护来优化成本

通过集中式事件日志记录的统一安全性，实现更有效的事件遏制和责任制

提供抵御外部干扰和内部威胁的高度弹性

支持不同的嵌入式平台（Windows，Linux）和不同类型的设备

帮助确保符合法规要求

通过高稳定性和对直接维护的最小依赖来降低运营成本

卡巴斯基扫描引擎

产品页面

卡巴斯基扫描引擎是一款网络威胁检测和缓解解决方案，可轻松与几乎任何应用程序集成。它通过 HTTP 和 ICAP 协议运行，可扫描传递的流量和传输的对象。该解决方案可与信息系统、Web 应用程序、代理服务器、网络数据存储和电子邮件网关集成。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 复杂基础设施的管理和保护
- 严格规定

返回计划

1 技术

我们如何帮助

保护您的财务系统免受客户上传的基于文件的威胁

过滤恶意、网络钓鱼和广告网址

中和受感染的文件、档案和加密对象

保护您的文件和备份存储

提供与各种平台和企业系统的广泛集成能力

返回计划

1 技术

卡巴斯基 移动安全 SDK

产品页面

一组库，您可以使用它们快速设计安全应用程序，并在开发阶段将安全功能直接集成到应用程序中。卡巴斯基移动安全 SDK 支持在移动设备上为银行应用程序创建安全环境，提供对金融机构服务器的安全访问，从而检测和阻止各种常见网络威胁。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 严格规定

我们如何帮助

确保客户的移动设备得到可靠保护	确保只向指定收件人安全传送财务资料
阻止访问恶意网站、钓鱼网站和短信	支持遵守安全规则和政策
减少针对客户的成功欺诈尝试次数	通过最大限度地减少欺诈活动，帮助您维护客户忠诚度

返回计划

1 技术

卡巴斯基
来电显示 SDK

产品页面

卡巴斯基来电显示 SDK 是一组库，集成在您组织的移动应用程序中，以保护您的客户免受欺诈和不必要的垃圾邮件呼叫。该应用程序内置 卡巴斯基来电显示 SDK 库和 AI 算法，可以从广泛的数据库中辨识电话号码，识别危险呼叫并阻止它们。这些功能也可卡巴斯基来电显示 REST API Web 服务的一部分提供，该服务集成早您的 PBX 中。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 严格规定
- 攻击面扩大
- 知识差距

我们如何帮助

识别来自电话号码和消息应用的呼叫

识别和阻止欺诈和广告/垃圾电话

提供有关电话号码的详细信息，包括其声誉

利用宝贵数据丰富您的内部反欺诈系统

减少针对客户的成功欺诈尝试次数

帮助支持和维护客户忠诚度

返回计划

1 技术

卡巴斯基欺诈防御

产品页面

我们基于会话的反欺诈功能可以在早期阶段（实时）于数字渠道（网站和移动应用程序）中识别复杂的欺诈计划。通过结合各种技术，卡巴斯基欺诈防御可提高金融机构客户的安全性，并增强您提供的客户体验。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 预算限制
- 严格规定

我们如何帮助

检测用户账户被盗、未经授权的账户访问和欺诈账户

帮助识别任何洗钱或恐怖主义融资

揭露社会工程欺诈

减少欺诈并增强您的客户体验

降低索赔工作和第二个身份验证因素（SMS、推送通知等）的成本)

通过丰富额外数据，提高欺诈监控的有效性

揭露任何滥用营销活动和奖金计划

帮助您遵守国际和国家立法

卡巴斯基 DDos 防护

产品页面

卡巴斯基 DDos 防护可最大限度地减少 DDoS 攻击的影响，确保整个基础设施和关键在线资源（如客户服务）的持续可用性。该解决方案包括防止所有类型的 DDoS 攻击并减轻其后果所需的一切：持续流量分析、潜在攻击警报、流量重定向到洗刷中心以及将"干净"流量返回到网络。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

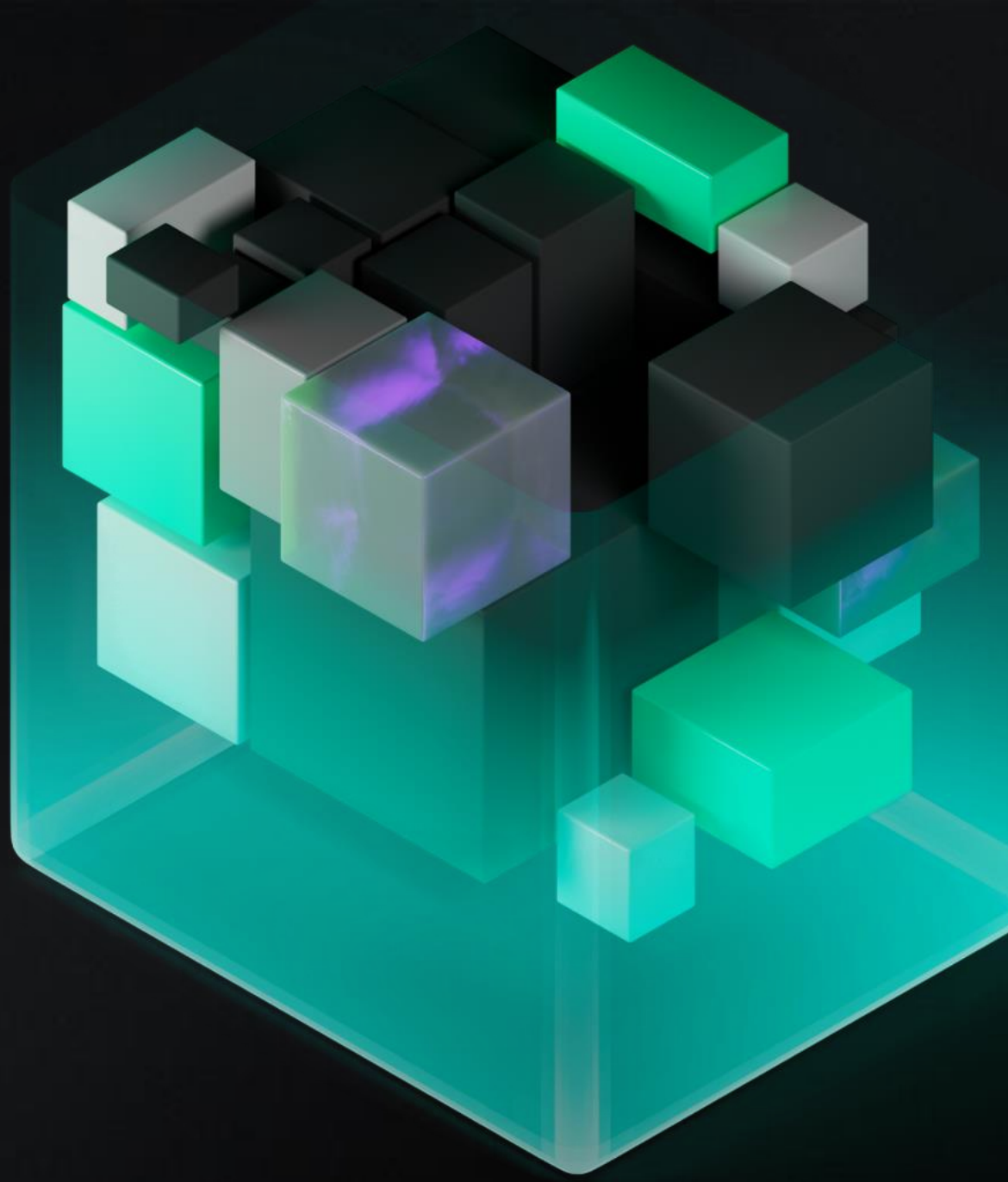
应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 预算限制
- 专业人员短缺
- 严格规定

我们如何帮助

从第一个数据包开始检测和过滤 DDoS 攻击	确保您的基础设施和服务在高水平可用 (99.95%)
确保金融组织的 Web 资源的安全性，包括模拟机器人攻击	在不暴露 TLS 证书的情况下保护加密流量
提供与 WAF 解决方案的集成功能以防御威胁	合规助力，构建安全可信的软件环境

超越传统网络安全



卡巴斯基容器安全

产品页面

该解决方案在容器化应用程序生命周期的所有阶段保护它们。卡巴斯基容器安全可无缝集成到软件开发过程中，考虑到容器化环境的细节，并保护从容器镜像存储库到编排器的每个组件。用户友好的小部件可帮助您监控产品运行状况并检测安全事件。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 严格规定

返回计划

1 技术

我们如何帮助

为容器化应用程序提供安全保障，无论是内部还是面向客户端

提高开发环境和流程的透明度

在开发和操作的每一步保护应用程序

支持主要管编排器、CI/CD平台及镜像存储库

审计您的基础设施及应用程序以遵守监管要求

加速面向客户端的应用程序和服务的发布

卡巴斯基 SD-WAN

产品页面

卡巴斯基 SD-WAN 通过统一管理构建容错、可扩展且安全的网络，解决与传统 Wan 相关的挑战。该解决方案允许您使用多样化的通信渠道，以零接触体验快速连接新位置，优化成本和云连接，增强应用程序的安全性和提高性能，并加快新服务的实施。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 复杂基础设施的管理和保护
- 预算限制
- 老系统
- 严格规定
- 专业人员短缺

我们如何帮助

- 轻松快速地连接新办公室、ATM 和数据中心
- 通过单个控制台管理整个网络，修改 CPE 设置和安全策略
- 确保数据传输和金融应用程序的性能
- 轻松集成安全工具以及云服务
- 优化通信渠道和基础设施维护的成本
- 减少 IT 事件的数量以及平均恢复时间
- 优化日常任务和网络监控
- 消除分支机构对 IT 专业人员的需求

卡巴斯基瘦客户端

产品页面

卡巴斯基瘦客户端是基于 KasperskyOS 的网络免疫瘦客户端基础架构。瘦客户端旨在为用户提供对远程桌面的访问权限，并用作本地工作站的替代品。得益于我们的网络免疫方法，基于 KasperskyOS 的瘦客户端在默认情况下是安全的。该解决方案可快速集成到您的基础架构中，并自动接收设置。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 复杂基础设施的管理和保护
- 攻击面扩大
- 严格规定

我们如何帮助

为员工提供安全的网络免疫工作站

监视到远程桌面的用户网络连接

确保您的员工和金融基础设施之间传输的数据的安全性

为您的网络安全和 IT 专业人员提供集中管理系统

支持灵活管理和控制整个瘦客户端基础架构，该基础架构最多可包含 100，000 个节点

有效的网络安全策略，保障金融服务的完整性。——知识

威胁情报

我们以各种格式提供可靠、相关的威胁数据.独特分析可增强安全系统并为决策提供信息。

网络意识

培训计划可帮助员工发展网络安全技能，并鼓励他们在日常运营中实际应用。

实际事件响应培训

实践培训将教授专家如何分析数字证据、检测和调查恶意软件、以及如何有效地响应事件。

卡巴斯基安全意识

产品页面

组合的解决方案，旨在增加企业对安全的参与和减少与人有关的事件，使用灵活的方法来应对不同级别的人员。我们针对金融行业、基于游戏的培训可帮助高管和经理实施有效的网络安全策略，而我们的自动化平台可让员工安全行事，通过主动防御业务免受威胁提高公司整体韧性。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 知识差距
- 严格规定
- 攻击面扩大

我们如何帮助

减少和预防与人类相关的安全事件

通过提高员工的技能，为您的整体安全增加一层保护

识别和纠正员工知识上的差距

在保护机密数据的过程中提高员工的参与度

使您能够根据员工培训结果管理安全解决方案设置

培养员工识别攻击迹象的技能，并在发生事故时采取适当的行为

卡巴斯基
威胁情报门户

产品页面

该门户通过统一的 Web 界面提供对所有人类可读的威胁情报数据的访问，其中服务协同工作以增强彼此。通过结合所有知识和经验，利用数据处理和分析技术，该门户可帮助金融组织有效地应对现代网络威胁。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 专业人员短缺

返回计划

2 知识

我们如何帮助

为早期攻击预防提供最新、可靠的威胁情报单一接入点

增强内部专业人员对威胁的了解并提高事件响应效率

提供灵活的威胁搜索服务和关联功能，加速事件调查

通过跟踪暗网资源中的数字资产和威胁，帮助保护品牌声誉

通过沙盒、攻击归因和文件相似性检测加强文件分析流程

考虑到行业和地区的具体情况，提供相关的威胁格局

提供与 APT 团体和有经济动机的网络犯罪分子有关的威胁报告

帮助分析人员跟踪网络犯罪基础设施

卡巴斯基威胁数据源

产品页面

超过 30 个随时可用的威胁情报数据源，用于解决金融组织面临的各种网络安全挑战。这些数据源提供有关已知恶意软件、钓鱼网站、最新漏洞、漏洞利用等信息，可增强各种安全解决方案。卡巴斯基威胁数据源使安全团队不仅能够检测威胁，而且能够有效地确定需要立即修复的事件的优先级，从而从卡巴斯基网络的各种来源中提供额外的宝贵上下文。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 专业人员短缺

我们如何帮助

通过持续更新的入侵指标和可操作上下文，增强包括 SIEM、XDR、防火墙、IPS/IDS 和安全代理在内的各种安全解决方案

利用高质量的威胁情报和相关上下文丰富 SIEM 系统，提高检测质量并减少误报

与包括 Kaspersky Cyber Trace 在内的 TI 平台集成，可实现有效的威胁情报管理和主动式网络威胁防护

支持将高置信度指标集成到周边安全解决方案（包括第三方 NGFW）中，以实现实时威胁拦截

帮助安全团队快速识别关键警报并为事件响应团队确定优先级

在软件开发过程中防御与开源组件相关的威胁

返回计划

2 知识

卡巴斯基 数字足迹情报

产品页面

全面的数字威胁保护服务，帮助客户监控他们的数字资产，并检测暗网和可见互联网中的威胁。通过实时警报，卡巴斯基数字足迹情报使组织能够快速有效地响应潜在威胁。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 新的漏洞和威胁
- 攻击面扩大
- 知识差距
- 专业人员短缺

我们如何帮助

确保对所有可能成为目标或受到损害的金融组织资产进行全面监控

识别可能成为潜在攻击媒介的网络资源和服务

监控可能损害公司声誉或欺骗客户的欺诈活动

检测遭泄露的员工、合作伙伴和客户数据，包括银行卡详细信息

为客户的金融组织提供持续的暗网监控

防止对业务运作造成负面影响

卡巴斯基 网络安全培训

产品页面

我们的全面培训计划旨在加强您的 IT 安全团队在恶意软件分析、逆向工程、威胁搜寻和事件响应方面的技能，使他们能够降低组织的风险并有效响应事件。通过增强内部专业人员的知识和技能，我们可以帮助您留住网络安全专业人员，避免招聘额外专业人员。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 攻击面扩大
- 严格规定
- 知识差距
- 专业人员短缺

我们如何帮助

发展您的 IT 安全团队的专业技能和能力	在全球合格专家短缺的情况下，减少和缓解您的招聘需求
提高威胁检测的有效性并加速事件响应	使您的员工能够完全控制基础设施的保护，而不需要外部的专业知识
促进风险缓解和团队效率	为有价值的员工提供额外的网络安全资格，以证明您对他们的承诺

有效的网络安全策略，保障金融服务的完整性。——支持

3 专业知识

托管保护

卡巴斯基专家提供24/7全天候托管安全，以应对日益增长的网络威胁。

咨询和安全评估

综合评估系统和安全措施是否有足够韧性。

专业服务

部署、维护和优化卡巴斯基产品，以最大限度地提高其效益。

卡巴斯基
应用程序安全评估

产品页面

卡巴斯基应用程序安全评估服务可帮助识别跨 Web 和移动应用、网上银行和其他系统的漏洞。该服务利用专家分析和高级工具，专注于发现应用程序架构和业务逻辑中的弱点，提供可操作的见解以加强安全性。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 知识差距
- 新的漏洞和威胁
- 专业人员短缺
- 攻击面扩大

我们如何帮助

为关键应用程序提供全面的专家主导评估

识别应用程序中的软件漏洞和逻辑缺陷

提供专家建议以增强应用程序安全性

通过早期发现应用程序中的漏洞，最大限度地减少财务损失

通过发现关键业务系统中的弱点，降低数据泄露和欺诈风险

通过发现和修复应用程序中的关键缺陷来保护业务运营并保护您的声誉

卡巴斯基渗透测试

产品页面

卡巴斯基渗透测试包括主动识别和探索针对关键资产的攻击媒介。通过模拟真实世界的攻击者行为并应用相关的策略、技术和程序（TTP），我们的团队展示对关键业务流程的潜在影响（无论您的基础设施的复杂性如何），所有这些都在一个受控和安全的环境中进行。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 老系统
- 新的漏洞和威胁
- 专业人员短缺
- 攻击面扩大

我们如何帮助

发现整个基础架构中可利用的漏洞	通过及早发现关键漏洞，最大限度地减少财务损失
评估您的组织对针对您的基础设施的现实网络威胁的韧性	优先考虑安全措施以获得最大影响
通过发现基础设施中的弱点来保护数据并防止欺诈	提供专家建议以增强基础设施的韧性

卡巴斯基红蓝对抗

产品页面

卡巴斯基红蓝对抗可模拟真实的黑客攻击，评估您的检测和响应能力，以帮助您保护关键业务功能。该服务由安全专家提供，确保机密性、完整性和可用性，同时遵循国际标准和最佳实践。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 知识差距
- 新的漏洞和威胁
- 专业人员短缺
- 攻击面扩大

我们如何帮助

Assess Blue Team 检测和响应能力	评估针对关键业务功能的攻击的韧性
分享可操作的见解，以加强您的安全态势	通过与行业相关的真实模拟，增强对针对性攻击的韧性
通过发现关键系统中的弱点，降低泄露和运营中断的风险	通过尽早检测关键风险，最大限度地减少财务损失

卡巴斯基
支付系统安全评估

产品页面

卡巴斯基支付系统安全评估是一项专家主导的服务，可发现 ATM/POS 系统中的漏洞。它将真实世界的攻击模拟与深入的专家分析相结合，可识别潜在的漏洞，并提供可操作的建议，以加强您的支付基础设施的安全性。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 老系统
- 新的漏洞和威胁
- 专业人员短缺
- 攻击面扩大

我们如何帮助

- 评估您的 ATM/POS 基础设施的安全状况
- 识别支付系统中可利用的漏洞
- 提供量身定制的建议，以加强 ATM/POS 系统
- 分析潜在的泄露情况和网络攻击的后果
- 通过识别 ATM/POS 设备中的漏洞来防止欺诈和服务中断
- 对安全措施进行优先排序，以增强支付系统的韧性

卡巴斯基
托管检测和响应

产品页面

卡巴斯基托管检测和响应 (MDR) 是一项提供全天候托管保护的服务，可抵御传统自动化安全措施检测不到的网络威胁和复杂攻击。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 攻击面扩大
- 新的漏洞和威胁
- 专业人员短缺
- 预算限制
- 严格规定

返回计划

3 专业知识

我们如何帮助

为您的专家团队提供全天候监控和主动式威胁搜索

利用人工智能驱动的洞察，主动检测和响应威胁

重新调配内部 IT 安全资源，以应对关键业务问题

提供可操作的报告，以帮助指导明智的决策

降低整体安全成本，无需继续招聘和培训昂贵的 IT 安全专业人员

通过尽早检测高级威胁和网络攻击，最大限度地减少潜在的停机时间和财务损失

卡巴斯基事件响应

产品页面

卡巴斯基事件响应可提供事件的完整、详细情况。服务涵盖整个事件调查和响应周期：从早期事件响应和证据收集到识别主要攻击向量和制定攻击缓解计划。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 专业人员短缺
- 新的漏洞和威胁
- 严格规定
- 预算限制
- 知识差距

我们如何帮助

迅速遏制威胁，防止进一步损害

详细的取证分析，以发现攻击媒介和根本原因

重建事件时间线并确定根本原因

提供定制的修复计划以恢复运营

通过加速事件恢复，最大限度地降低数据泄露和经济处罚的风险

提供专家指导，增强您的长期安全态势

卡巴斯基损害评估

产品页面

卡巴斯基损害评估服务专注于发现主动的网络攻击以及可能躲过您的 IT 安全工具和流程的先前未知攻击。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 专业人员短缺
- 新的漏洞和威胁
- 严格规定
- 知识差距
- 预算限制
- 攻击面扩大

我们如何帮助

进行彻底调查以发现隐藏的威胁

提供有关特定恶意软件文件的行为和功能的信息

提供全面报告，内含可行建议

就解决已识别的风险提供专家指导并加强防御

对基础设施入侵的风险进行公正的评估

通过检测隐藏的威胁，降低数据泄露和财务损失的风险

卡巴斯基 SOC 咨询

产品页面

卡巴斯基 SOC 咨询让您的组织能够构建和优化自己的安全运营中心。从架构设计到流程改进，该服务有助于确保有效检测和响应不断变化的网络威胁。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 专业人员短缺
- 新的漏洞和威胁
- 严格规定
- 知识差距
- 预算限制

我们如何帮助

- 设计或优化 SOC 架构以提高效率
- 实施最佳实践以简化流程和工作流程
- 评估 SOC 的成熟度，并确定需要进一步改进的领域
- 为您的内部 SOC 团队提供培训
- 通过简化 SOC 流程降低运营成本
- 提高威胁检测和响应的效率

卡巴斯基专家服务

产品页面

返回计划

3 专业知识

卡巴斯基专家服务提供专家支持，以优化和保护您的 IT 环境。通过利用卡巴斯基的高级解决方案，我们的专家提供量身定制的支持，以增强基础设施保护并构建抵御复杂网络威胁的能力。

受支持的优先事项

- 客户参与
- 弹性基础设施
- 数字信任和管理

应对的挑战

- 知识差距
- 老系统
- 专业人员短缺

我们如何帮助

提供旨在满足金融组织独特需求的安全解决方案

提供持续支持，确保您的安全系统始终提供最佳性能

处理日常安全任务，让您的团队专注于更高优先级的问题

提高安全基础架构的性能和有效性

加强您的基础设施，抵御高级和不断变化的网络风险

优化您的网络安全支出，提供更大的价值和保护

kaspersky

感谢您的关注！

请联系我们了解有关金融服务网络安全的更多信息

了解更多