企业安全管理的挑战：没有中心控制点



各种产品的特定控制台

难以揭示…

复杂的安全威胁

无法实现…

合规性监视

存在风险…

业务连续性

ArcSight企业级的风险及威胁管理平台



满足…

安全威胁管理

监视…

合规性控制

确保…

业务连续性

由市场领导者提供的解决方案

公司背景

- 成立于 2000年5月
- 3000+ 客户
- 全球offices worldwide
- NASDAQ: ARST , An HP Company

市场分析

IDC Analyze the Future — 最近四次的报告中保持#1 的市场占有率

TheInfoPro — #1 在使用的SIEM和日志管理解决方案

GartnerGroup — SIEM 领导者象限位置 - 连续8年

业界认可

SC Magazine Awards 2006 Winner

SC Magazine Awards 2006 Europe Winner

Information Security Readers' Choice Awards Gold 2007

Info-Tech Research Group Decision Diamond Leader 2007

Deloitte. 2008 Technology Fast 50 Silicon Valley

Deloitte. 2009 Technology Fast 500

2009 Winner GSN Homeland Security Awards

Everything Channel 5 Star Partner Program Winner 2009

Readers' Choice Awards '09 Gold

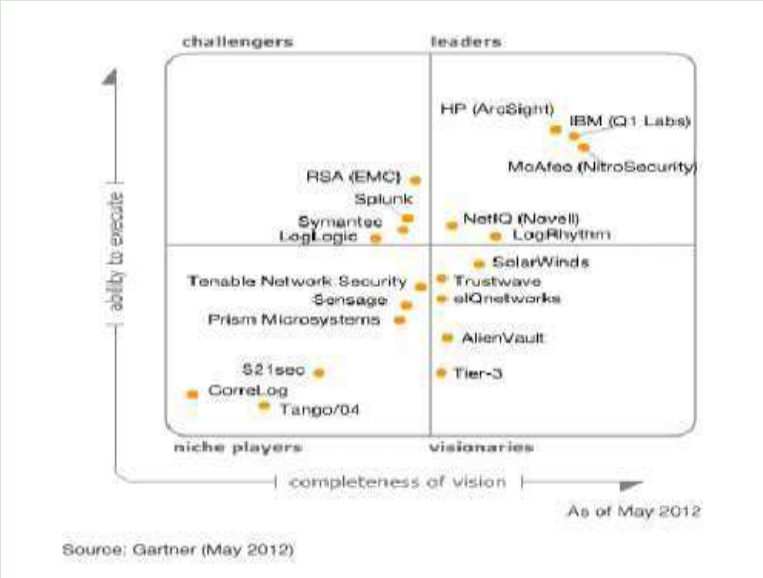
SC Magazine Awards 2010 Winner

Everything Channel 5 Star Partner Program Winner 2010

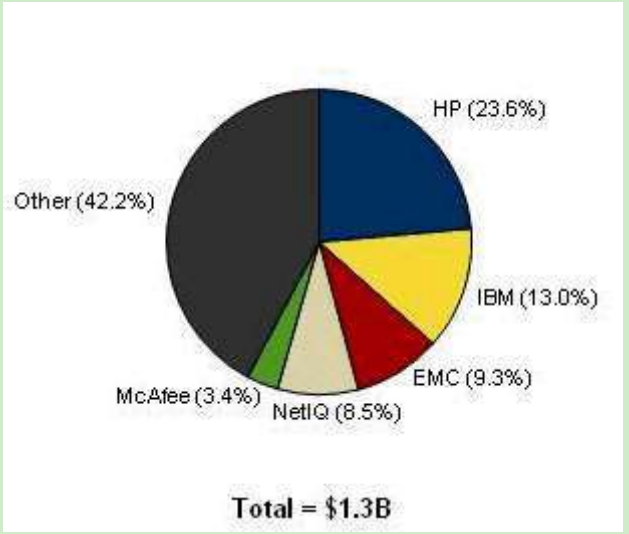
© 2010 ArcSight Confidential

唯一连续九年保持领导者地位的厂商

Gartner 2012 MQ: Leader 9 Years



IDC: Share Leader 5 Years



Source: IDC (Decer

2009 WINNER GSN Homeland Security Awards

Deloitte 2009 Technology Fast 500

Everything CHANNEL 5 STAR PARTNER PROGRAM WINNER 2009

SC AWARDS 2009 FINALIST

大中华区ArcSight 部分客户名单







































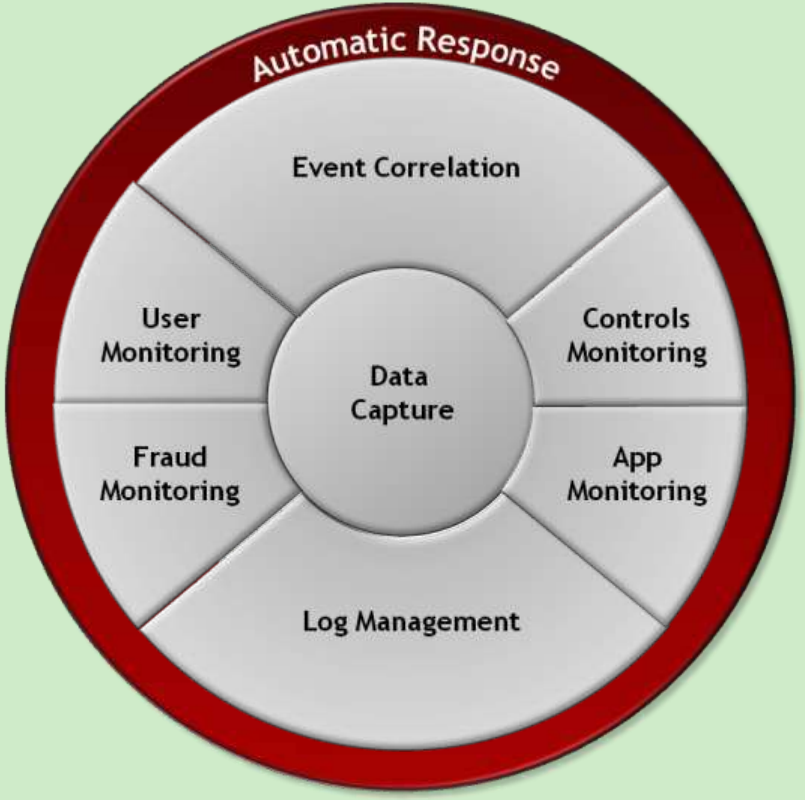




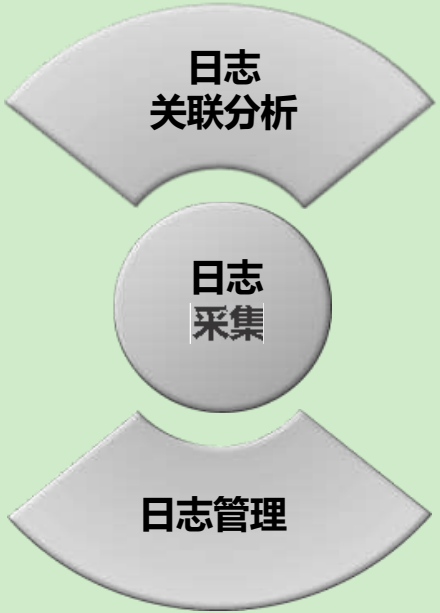




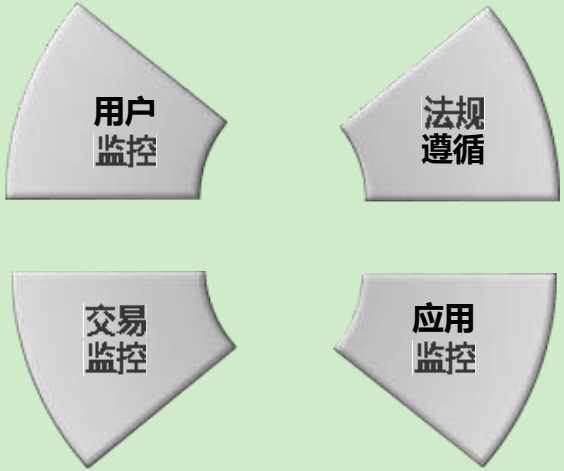
模块化架构适应各种规模企业的需求



企业随自身业务发展逐步完善安全管理架构



HP ArcSight ESM
HP ArcSight Logger
HP ArcSight Express



HP ArcSight IdentityView
Fraud Monitoring
Auditor Apps
SAP Auditor



HP ArcSight TRM

安全日志的收集：
Arcsight Connector简介

强大高效的日志采集功能

- 任何结构化和非结构化的事件均可收集
- 事件的标准化和类型化，为日后分析打好基础
- 符合安全审计要求的收集过程(加密,缓存, 带宽控制)

HP ArcSight Connectors



Rackable Appliances



Branch Office/Store Appliance

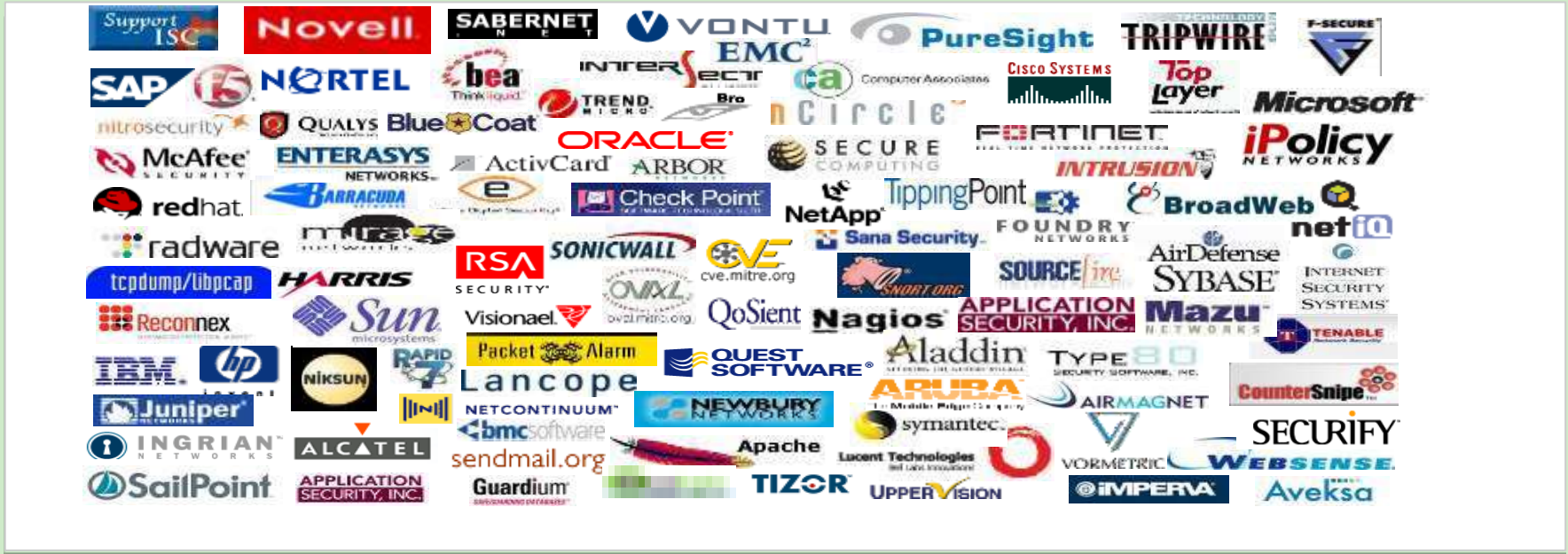


Installable Software

好处：提供独立于设备厂商品牌的事件分析

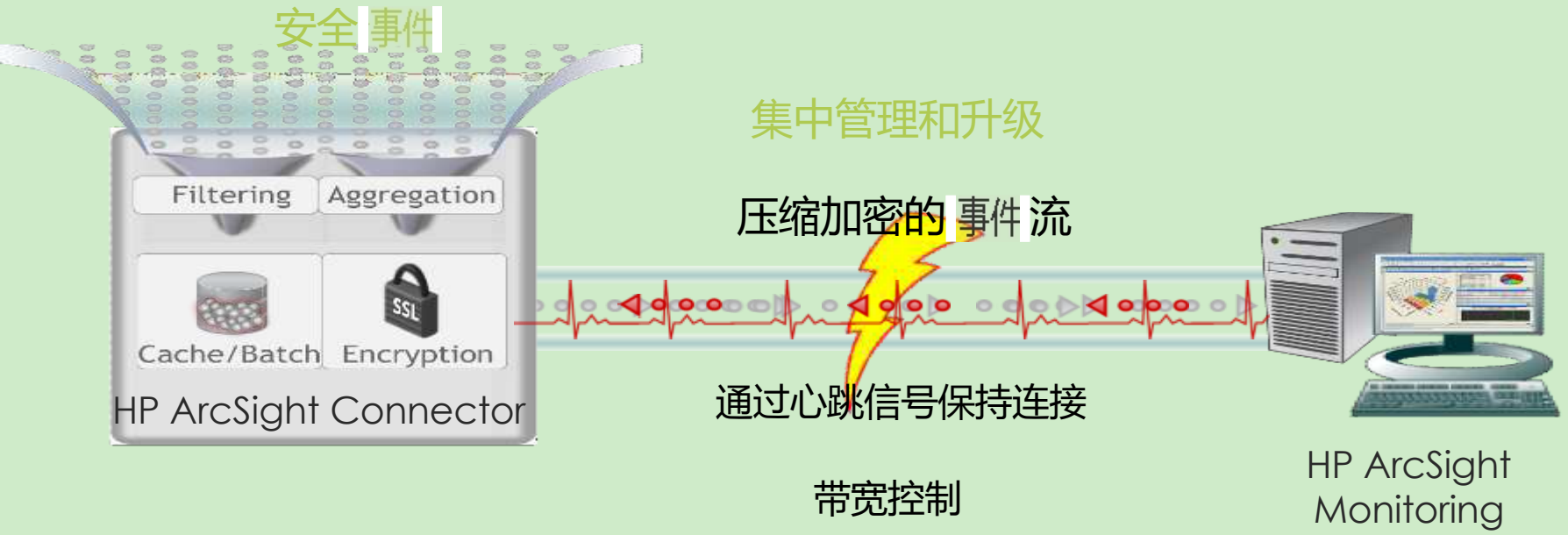
HP ArcSight 事件收集

300+ 产品, 50+ 类型, 80+ 合作伙伴



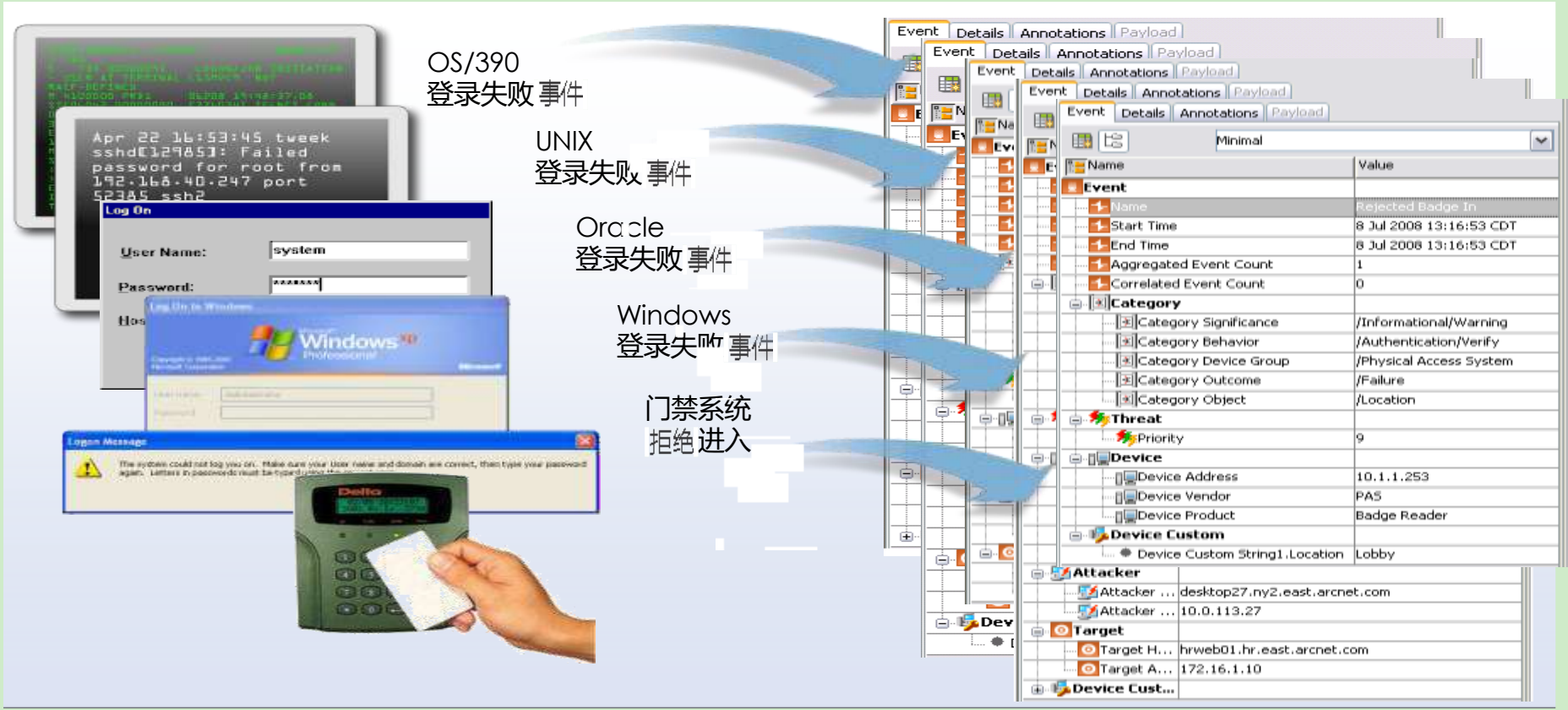
Access and Identity	Data Security	Integrated Security	NBAD	Policy Management	Vulnerability Mgmt
Anti-Virus	Firewalls	Log Consolidation	Network Management	Router	Web Cache
Applications	Honeypot	Mail Filtering	Network Monitoring	Security Management	Web Filtering
Content Security	Host IDS/IPS	Mail Server	Net Traffic Analysis	Switch	Web Server
Database	Network IDS/IPS	Mainframe	Operating System	VPN	Wireless

安全可靠的事件收集过程



Follows NIST 800-92 Log Aggregation Guidelines

核心技术: 事件的标准化


OS/390
登录失败事件
UNIX
登录失败事件
Oracle
登录失败事件
Windows
登录失败事件
门禁系统
拒绝进入
Apr 22 16:53:45 tweek sshd[129851]: Failed password for root from 192.168.40.247 port 52345 ssh2
Log On
User Name:
system
Password:
Windows
Logon Message
Event
Details
Annotations
Payload
Minimal
Name
Value
Start Time
8 Jul 2008 13:16:53 CDT
End Time
8 Jul 2008 13:16:53 CDT
Aggregated Event Count
1
Correlated Event Count
0
Category
Category Significance
/Informational/Warning
Category Behavior
/Authentication/Verify
Category Device Group
/Physical Access System
Category Outcome
/Failure
Category Object
/Location
Threat
Priority
9
Device
Device Address
10.1.1.253
Device Vendor
PAS
Device Product
Badge Reader
Device Custom
Device Custom String1.Location
Lobby
Attacker
Attacker ...
desktop27.ny2.east.arcnet.com
Attacker ...
10.0.113.27
Target
Target H...
hrweb01.hr.east.arcnet.com
Target A...
172.16.1.10
Device Cust...

标准化 和类型化的好处

没有 标准化 的 事件

Jun 17 2009 12:16:03: %PIX-6-106015: Deny TCP (no connection) from 10.50.215.102/15605 to 204.110.227.16/443 flags FIN ACK on interface outside
Jun 17 2009 14:53:16 drop >eth0 product VPN -1 & Firewall-1 src xxx.xxx.146.12 s_port 2523 dst xxx.xxx.10.2 service ms-sql-m proto udp rule 49

标准化 后的 事件

Time (Event Time)	name	Device Vendor	deviceProduct	Category Behavior	Category DeviceGroup	Categorye	Category Significance
6/17/2009 12:16:03	Deny	Cisco	PIX	/Access	/Firewall	/Failure	/Informational/ Warning
6/17/2009 14:53:16	Drop	Checkpoint	Firewall-1/ VPN -1	/Access	/Firewall	/Failure	/Informational/ Warning

好处: 为后续高效高速的 事件 分析打好基础

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/225044044002011110