Looking Ahead – The Path to Moving Security into the Cloud

Gerhard Eschelbeck

Sophos

Session ID: SPO2-107

Session Classification: Intermediate

RSACONFERENCE2012

Agenda

- The Changing Threat Landscape
- Evolution of Application Delivery
- Delivering Real World Security Applications via SaaS

The Changing Threat Landscape

- Financially motivated, computer generated malware
  - Number of variants is growing sharply
  - From Destructive to Stealth
- Vulnerabilities in well known and broadly used software are common attack vectors
- Leveraging technology to increase effectiveness and avoid detection
  - Encryption, Rootkits, Code Injection, Polymorphic, ADS, …
- Social Networking sites are increasingly used as a distribution mechanism
  - Shortened URLs, User contributed content
- Malware research and protection more challenging

The Need for Change

- Explosion of malware variants is challenging traditional security approaches
- Short lifetime (hours to days) but fast mutation
- More “bad” files than “good” files
  - Long tail issue
  - Blacklisting vs. whitelisting
- Relevance, Prevalence, Reputation are key to successful protection
- Multiple Entry Points into Networks
- Mobile Users and De-Perimeterization

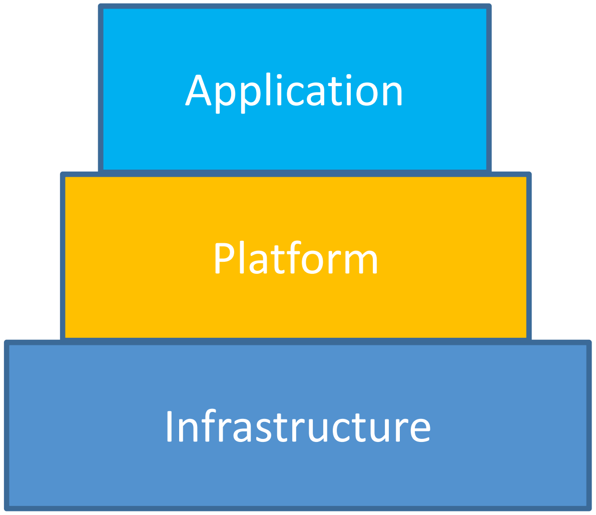
Expand your Infrastructure!
Buy new servers, increase your software costs, provision more datacenter capacity!!

Look to the cloud!

Pay for the bandwidth and server resources that you need. When your job is done then turn the whole thing off!

What is the Cloud Anyway ?

- Infrastructure as a service
  - The infrastructure (hardware, networking, virtualization) in the cloud as the foundation for cloud applications
- Platform as a service
  - Software development platforms in the cloud to develop cloud applications
- Software as a service
  - Pay-as-you-Go solutions/application delivered in the cloud via the Browser.


Application

Platform

Infrastructure

The Evolution of Application Delivery

- Traditional On Premise Installed Application
  - On premise hardware, server, network, database, backup provisioning at customer
  - Ongoing maintenance and management performed by customer
  - Customer is responsible for providing logical and physical security
  - Typically lengthy rollout/update cycles

- Managed Service Application
  - Applications installed, managed and maintained by a third party
  - High involvement of human resources for application management
  - Installation on customer premise or also centralized model
  - Most applicable for highly specialized applications
  - Typically single tenant (dedicated systems) off-the-shelf applications

- Software as a Service (SaaS)
  - Typically no (or very limited) on-premise hw, server, database, backup
  - SaaS provider is responsible for all maintenance, management, infrastructure
  - Application usage via browser
  - Economy of scale due to full automation from the provider
  - Fast rollout and innovation/update cycles
  - Multi tenant architecture (multiple customers share some or all layers of the stack)

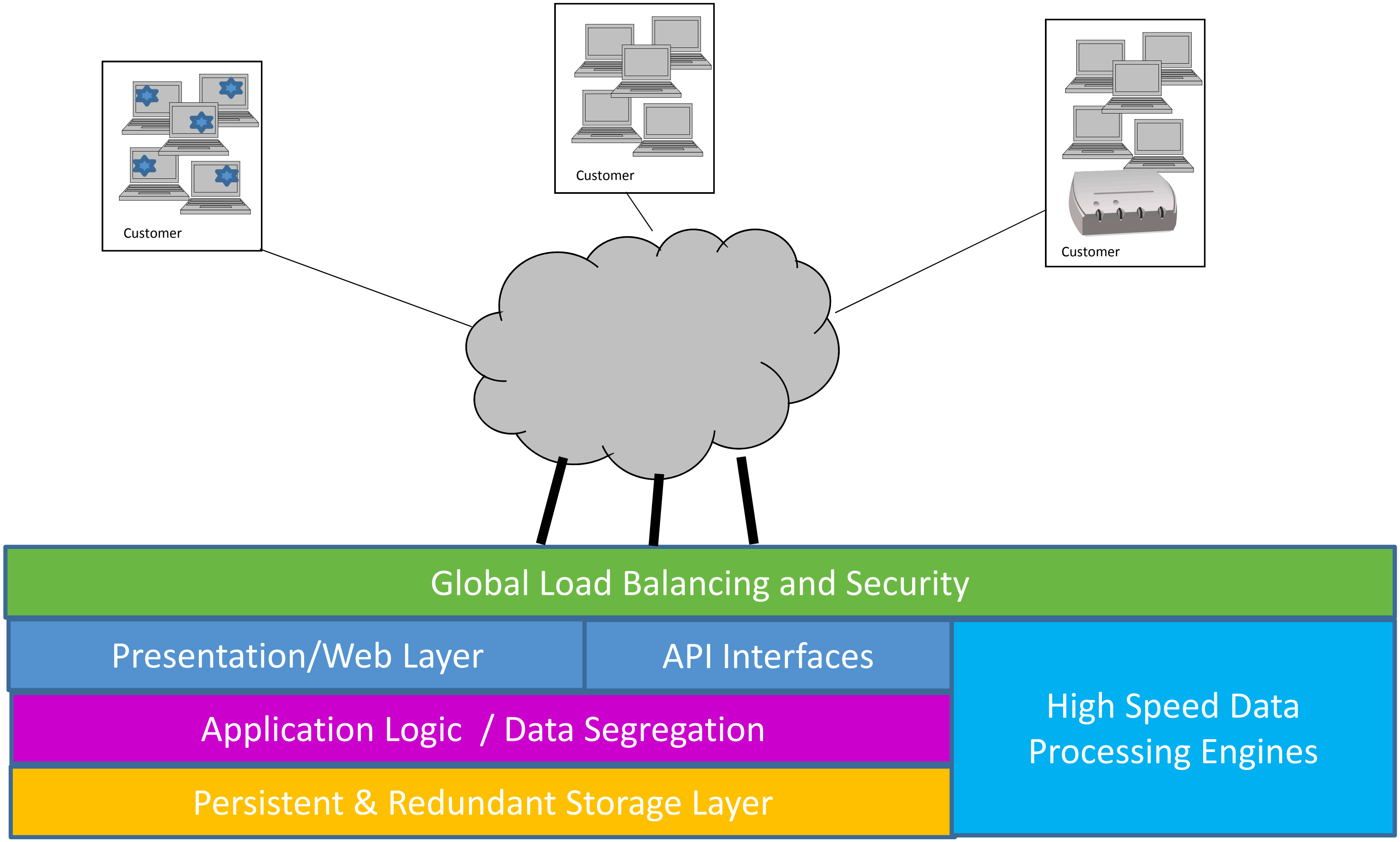
SaaS Deployment Models

- Pure SaaS application
  - Web browser is single interface point with customer
  - All intelligence is centralised at SaaS provider
  - Limited integration between customer and SaaS provider
  - Examples: CRM, Email filtering, Payroll, Customer support applications

- SaaS with customer side software agent
  - Web browser is interface point with customer
  - Additional small client-side software agent (permanent or transient)
  - Enables stronger integration of customer systems and SaaS service
  - Examples: Application sharing, Web-filtering, Online-Backup

- SaaS with customer side appliance
  - Web browser is interface point with customer
  - Additional hardware appliances (remotely managed) on customer premise
  - Enables deep integration of customer systems with SaaS providers
  - Examples: Intrusion Detection, Security Management, Vulnerability Assessment

SaaS Deployment Architecture



Global Load Balancing and Security

Presentation/Web Layer

API Interfaces

Application Logic / Data Segregation

Persistent & Redundant Storage Layer

High Speed Data Processing Engines

Why Security SaaS makes Sense

- Subscription model (pay as you go, per user, per time)
- Reduced risk (performance, uptime, reliability, scalability)
- Lower rollout cost
- No additional IT overhead
- Rapid deployment and implementation
- Compliance requirements (audit trails, archiving, logging)
- Allows to focus on core business

Security as a Service

Delivering Real World
Security Applications
via the SaaS Model

SaaS based Web Security and Content Filtering

- Web is primary delivery vehicle for malware with explosion of malware variants
- Multi-engine approach is required
- Global and aggregate traffic and threat view allows better decision making
- Moving protection layer closer to the source of the malware
- Analyze inbound and outbound HTTP content in the cloud
- Transparently filter and remove malware and categorize/block unwanted websites

SaaS based Email Filtering and Management

- Increasing spam and email-born malware (high network bandwidth utilization)
- Routing inbound and outbound emails for analysis through cloud based filter
- Multi-level engine approach to catch spam, zero-day exploits, virus, Spyware
- Moving protection layer closer to the source of spam/malware
- Tracking content leaks

SaaS based Vulnerability and Compliance Mgmt

- Audit, security assessment, and compliance management
- Discovery, assessment, and prioritization
- Internal and external view
- Validation against security policies
- Remediation tracking

SaaS based Endpoint and Mobile Threat Security

- First Generation (heavy client)
  - All scanning and detection local - definitions downloaded regularly
- Second Generation
  - Submit metadata from unknown executable to the cloud for classification
  - Real-time query the cloud (i.e. URLs, Hashes)
- Third Generation (thin client)
  - Fully cloud based filtering and blocking
  - Leverage reputation data from the cloud

Why the Cloud matters for Security Applications

- Increased computing power
  - Elasticity and Instant Scalability
  - Multiple engines in parallel
  - Compression/Decompression
  - Offloading heavy processing from the client
  - Unlimited memory and disk storage - Storage for white and blacklists

- Know what is relevant
  - Visibility into traffic patterns
  - Reputation (user votes vs. automated reputation scoring)
  - Life attack data from clients
  - Malware spidering

- Utility Model / Pay per use
  - Turn fixed cost into variable cost
  - Reliability and Geo Redundancy
  - Service Orientation and APIs
  - Economies of Scale

Critical Success Factors with Cloud Approach

- Latency
  - Communication overhead
  - Protocol choices, Bandwidth availability
  - Local caching

- Security, Privacy
  - What needs upload (amount, content)
  - Encryption of data in transit and at rest

- Availability
  - Load balancing, Redundancy

Questions to Ask your Cloud / SaaS Provider

- SaaS provider profile and financial strength
- Quality and presence of provider’s customer support
- Existing customers and Service renewal rates
- Technology Innovation and Update Cycle
- Service Level Commitments (SLA’s)

Service Levels and Availability

- Service availability and reliability
- Latency and performance
- Effectiveness
- Accuracy
- Security

Availability %	Downtime per Month
99%	7.20 hours
99.9%	43.2 minutes
99.99%	4.32 minutes
99.999%	25.9 seconds

SLAs should be objectively defined and regularly measured and reported by the provider

SLAs should be enforced through clear consequences

Security Considerations

- Data storage model and architecture (encryption)
- User account management (provisioning, roles, permissions)
- Identity management (single-sign-on)
- Security process and certifications (SAS 70, SSAE 16, ISO)
- Backup, recovery, physical hosting facilities
- Business continuity

The Inside View from a SaaS Provider

- Known platform provides better application quality
- Global deployment and distribution
- Simple application/revision management
- Load management and scale driven by business growth
- Global and Instant update for all customers
- Ability to scale quickly - unlimited scalability
- Integrate and deliver best-of-breed technologies
- Strong customer commitment and support is critical

How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Review your security applications for management overhead
  - Evaluate the feasibility of a Cloud/SaaS based approach for such applications
  - Assess the pros and cons of a Cloud/SaaS approach in your environment
  - Define requirements and identify the risks and success factors of a Cloud based architecture

- Within six months you should:
  - Identify service level requirements according to your organization's needs
  - Launch a pilot program for SaaS

Summary

- Cloud infrastructure and SaaS are significantly improving effectiveness and manageability of Security technology

- SaaS empowers the user/customer - delivers a high level of customer commitment and service, as switching is relatively easy

- Security and Privacy are major factors in the adoption of SaaS/Cloud

- A lot of people think they will make a lot of money – so there is lots of hype, but the cloud is something fundamental.

Thank You

Q&A

Gerhard Eschelbeck

ge@sophos.com