Evolving Technologies Blueprint for Cloud

**Compare and contrast Cloud deployment models**

- Infrastructure, platform, and software services (XaaS)
- Performance and reliability
- **Security and privacy**
- Scalability and interoperability

**Describe Cloud implementations and operations**

- Automation and orchestration
- Workload mobility
- Troubleshooting and management
- OpenStack components
Cloud Security

Arshad Saeed

Feb 21st 2018
Agenda

- Security Enable Digitization
- Overview of Business Case for Cloud
- Cloud Security Use Cases
- Evolution of Threats
- How to Structure capabilities to meet threats
- Architecture of Securing Public Cloud Apps
- Architecture of Securing Public Cloud Workloads
- Recommendations
Digital Disruption, Massive Scale

50B Devices Connected by 2020
$19T Opportunity

Active Adversaries
Attack surface
Threat Actors
Attack Sophistication

Security Industry
Rapidly expanding number of security companies
Not interoperable
Not open

Security Challenges

Changing Business Models
Dynamic Threat Landscape
Complexity and Fragmentation
We live in a cloud-first world

81% evaluating or using public cloud
84% will use multiple clouds
73% Have a hybrid cloud strategy

Source: IDC InfoBrief, sponsored by Cisco, Cloud Going Mainstream. All Are Trying, Some Are Benefiting; Few Are Maximizing Value.
Organizations must adapt to the Cloud due to four key trends

- Critical infrastructure and data moves away from corporate data centers
- Business apps move towards SaaS while application development shifts
- Mobile workforce and BYOD proliferation
- Branch offices have direct internet access
Cloud adoption is driving specific business outcomes

- Reduced Costs
- Improved Agility
- Enhanced Productivity
- Increased Revenue
Key Cloud Security Use Cases
“Cloud Security” means different things

Security to the cloud

“Secure my data and applications as they transition to or are accessed from the cloud”

Security for the cloud

“Secure my cloud based workloads and applications”

Any security solution may be delivered from the cloud
Organizations need to focus on two key cloud security areas:

- **Public Cloud Applications**
  - Cisco Spark
  - Salesforce
  - Box
  - ServiceNow
  - G Suite
  - Dropbox
  - Slack

- **Public Cloud Workloads**
  - Public Cloud (IaaS/PaaS)
    - Amazon Web Services
    - SolarWinds
    - Microsoft Azure
    - VMware

- **Private Datacenter**
Public Cloud Applications

What are my users doing here?
- box
- Cisco Spark

How do I know if an admin’s account is compromised?
- servicenow

Do I have sensitive data here?
- salesforce

Which apps are accessing my corporate data?
- Cisco Spark

How is data flowing between my cloud apps?
Public Cloud Workloads

How can I setup a secure path from my DC to the cloud to support staged migration?

How can I lift and shift applications to the cloud while maintaining security?

How do I extend existing network segmentation to the public cloud?
## Bringing it back together

<table>
<thead>
<tr>
<th>Public Cloud Applications</th>
<th>Public Cloud Workloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure data transitioning between users and public cloud applications</td>
<td>Secure data transitioning between data center and public cloud</td>
</tr>
<tr>
<td>Secure data and identities within public cloud applications</td>
<td>Secure the applications hosted within the public cloud</td>
</tr>
</tbody>
</table>
Threats fall under 4 main categories

- Malware and ransomware
- Gaps in visibility and coverage
- Compromised accounts and malicious insiders
- Data breaches and compliance

Threats extend and evolve to fit new attack targets
Let’s look at how security has evolved
Attackers used to focus on the only legitimate target: the on-premises network.
Security professionals focused on perimeter and network security, from NGFW to IDS/IPS
With increased off-network devices, attackers shifted their focus to endpoints.
Organizations responded with **endpoint security** and by extending network controls to endpoints.
With the rise of cloud computing, attackers shifted their focus yet again.
Organizations responded by **adding new cloud security controls and extending existing capabilities**
Cloud Security Requires an Integrated Approach
A complementary, coordinated approach across the 3 pillars of networks, endpoints, and cloud is required. Each pillar has a set of deployment form factors that can be utilized based on organization’s needs.
A portfolio of capabilities is needed

- Anti-Malware
- NAC
- DNS Security
- Flow Analytics
- UEBA
- Email Security
- Data Security
- IAM
- Web Security
- Firewall
- AVC
- IPS
These capabilities handle specific threats

<table>
<thead>
<tr>
<th>Anti-Malware</th>
<th>NAC</th>
<th>DNS Security</th>
<th>Flow Analytics</th>
<th>UEBA</th>
<th>Email Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious file uploads and downloads</td>
<td>Untrusted and compromised devices</td>
<td>Phishing C&amp;C</td>
<td>Insider Threats Compromised Devices</td>
<td>Compromised Account Insider Threats</td>
<td>Spam Phishing Malicious Files</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Security</th>
<th>IAM</th>
<th>Web Security</th>
<th>Firewall</th>
<th>AVC</th>
<th>IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Content</td>
<td>Weak &amp; Reused Passwords</td>
<td>Content Filtering Malicious Destinations</td>
<td>Rogue Access Zero Day</td>
<td>Malicious &amp; Risky Application Usage</td>
<td>Intrusion</td>
</tr>
</tbody>
</table>
The capabilities are a mix of in and out of band

**In Band**
- NAC
- DNS Security
- IPS
- Firewall
- IAM
- Email Security
- Web Security

**Both**
- Data Security
- Anti-Malware
- AVC

**Out of Band**
- Flow Analytics
- UEBA
Capabilities can be deployed across pillars and form factors

- **Network**
  - NAC in Branch network, but Firewall in corporate network
  - Anti-Malware enforcement on a laptop, but threat intel engine within the data center

- **Endpoint**
  - NAC
  - IPS
  - Data Security
  - AVC
  - Anti-Malware
  - Flow Analytics
  - UEBA
  - Firewall
  - Web Security

- **Cloud**
  - Email Security
  - DNS Security
  - IAM

- UEBA data collection within each network, but UEBA analysis within a SaaS environment
Architecting a solution for your organization

1. Iterate on the use case with a focus on business value

End users must be able to securely access Office 365 to collaborate with their colleagues.
Architecting a solution for your organization

1. Iterate on the use case with a focus on business value
2. Identify the threats that will be prevalent in the execution of the use case

Users need to access Office 365 to collaborate with their colleagues
1. Iterate on the use case with a focus on business value
2. Identify the threats that will be prevalent in the execution of the use case
3. Map the capabilities that can address each relevant threat

Users need to access Office 365 to collaborate with their colleagues
Architecting a solution for your organization

1. Iterate on the use case with a focus on business value
2. Identify the threats that will be prevalent in the execution of the use case
3. Map the capabilities that can address each relevant threat
4. Choose the relevant pillars that best provide the capabilities among different options
Architecting a solution for your organization

1. Iterate on the use case with a focus on business value
2. Identify the threats that will be prevalent in the execution of the use case
3. Map the capabilities that can address each relevant threat
4. Choose the relevant pillars that best provide the capabilities among different options
5. Determine the best form factor for each

- **Anti-Malware**
- **Flow Analytics**
- **IAM**
- **Data Security**
- **UEBA**

Flow Analytics at the branch office? Or is traffic backhauled to corporate?
SaaS-based IAM vs managed with private infrastructure
In-band or out of band-Data Security?
Architecting Caveats

1. The capabilities are presented in sequence, but the actual implementation can be dynamic in nature based on load and choice of form factors.
2. Capabilities will be listed once for clarity although the end product can overlay multiple pillars and form factors for the same capability.
Recommendations
The architecture starting point depends on the organization’s cloud maturity

Focus on visibility & lightweight controls

Focus on highest-impact cloud application and cloud infrastructure controls

Focus on architecture that integrates Network, Endpoint, and Cloud Security
Recommendation: Prioritize business goals and favor solutions and form factors that give the broadest coverage.
Recommendation: Favor cloud-managed solutions
How Cisco Security Helps
Cisco takes a complementary, coordinated approach to security across networks, endpoints, and the cloud