# Security 101 for Sales

## Making Sense of Security to Deliver the Solutions

# Agenda

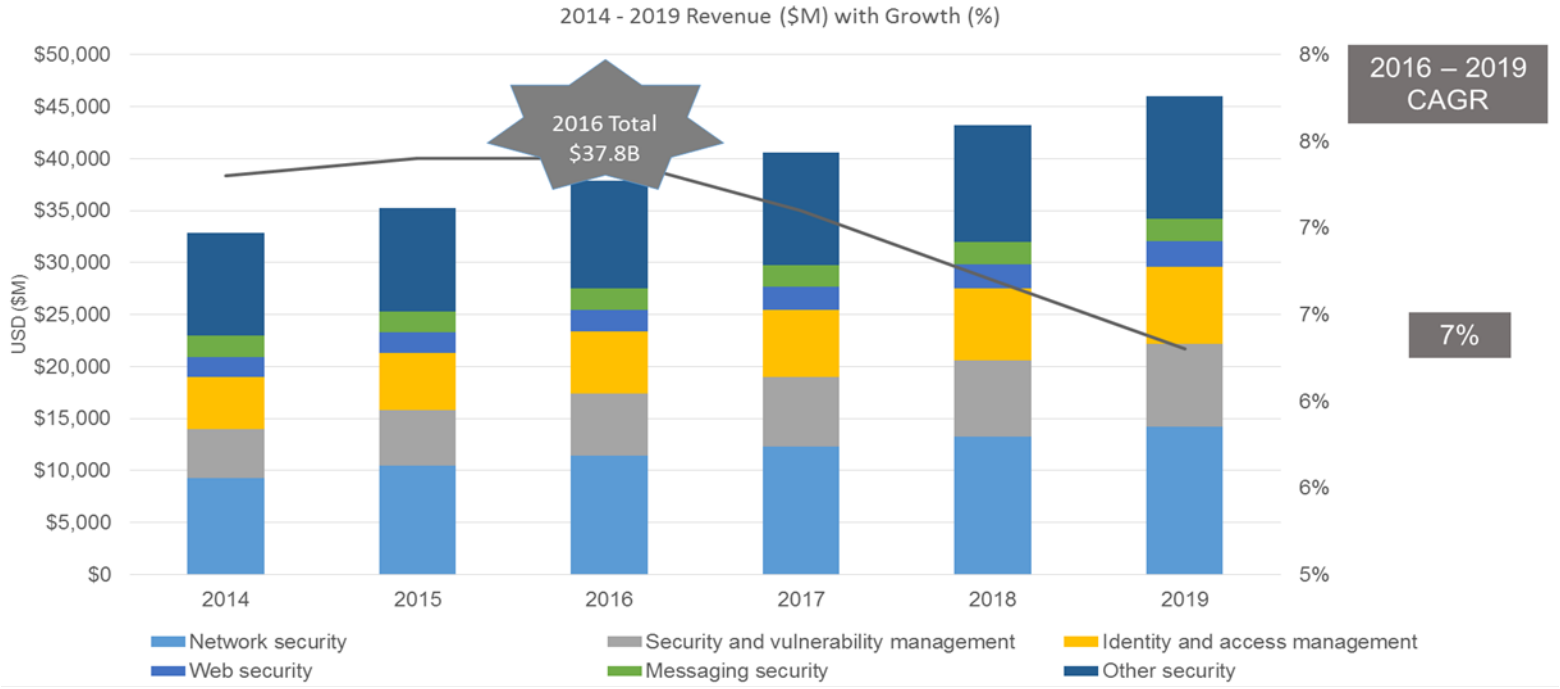
- Introduction – The Evolution of Security
- Security 101 – Getting up to Speed
- Security Concerns Fueling Rapid Market Growth
- Starting The Security Conversation
- Summary – Become the Trusted Security Advisor

# The Evolution of Security

**Security has rapidly evolved**

- Gone are the days…
- Cybercriminals attacking businesses on multiple fronts
- Once the domain of IT
- Now concerns the whole business
- Gaps in corporate security due to mobile and cloud

# Explosive Growth in Security Opportunities




Source: IDC, Worldwide IT Security Products Forecast, 2015–2019, Doc #US40709015, Dec 2015.

# Security 101 – Getting up to Speed

**Security used to be about tools:**

- Antivirus software secured laptops and desktops
- Firewalls secured the perimeter
- Content filtering tools protected against email attacks and malicious websites

*New approach to security requires a change in thinking.*

# New Security Thinking

**When engaging a customer, ask yourself:**

- What's valuable to cybercriminals?
- How would hacker or insider exploit the company?
- How to protect against these actions?

# Four Aspects of Security

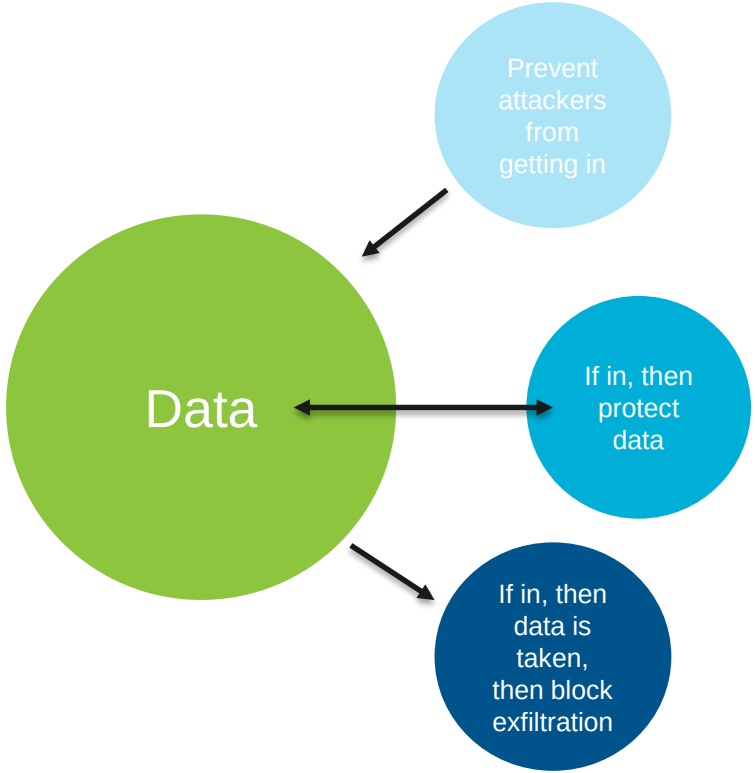
1. **Physical security** – Prevent unauthorized access to facilities.
2. **Network security** – Protect the network from perimeter to endpoints.
3. **Data security** – Protect the data stored on the network.
4. **User security** – Ensure access only by authorized users.


Security Model
Availability
Integrity
Confidentiality

# Primary Goals

**To stop attacks, security technology has three primary goals:**

1. Prevent attackers from getting into the network
2. Prevent access to company data
3. Prevent the exfiltration of the data



# Threats Beyond Data

**Hackers that compromise endpoints can silently perform illegal activities.**

Examples:

- Send spam emails
- Perform denial of service attacks on other targets
- Host illegal content
- Black market rental of “zombie” PCs

***You may never know your computers are exploited***

# Talking the Talk

It pays to learn key terms and definitions.

- **Endpoint** – End-user device like a desktop, laptop, phone, tablet, or other mobile device.
- **Perimeter** – Edge of the business network, where the corporate infrastructure joins the ISP network.
- **Intrusion Detection and Prevention** (IDP) – Analyzes network activity and look for signs of threats.

# Talking the Talk

- **Unified Threat Management** (UTM) – Includes firewall, IDP, and antivirus in a single device.
- **Security Intelligence and Event Management** (SIEM) – Aggregate, analyze, monitor and identify threats.
- **Vulnerability Assessment** – Analyzes the network for known critical vulnerabilities.
- **Hacker** – Someone who takes advantage of network vulnerabilities.

# Security Concerns Fueling Rapid Market Growth

# Security Concerns Fueling Rapid Market Growth

**Mobile, cloud, and Internet of Things (IoT) are moving company data outside the data center.**

- Explosive growth in the number and type of endpoints and devices to protect
- Security now encompasses many different products

# Security Needs Many Different Products

| Web Server Security | Applications | Endpoint | Mobile | Security Intelligence |
|---|---|---|---|---|
| • Web App Firewall<br>• Web Security<br>• WebInspect DAST | • Application Scanning<br>• Source Code Analysis<br>• Application Security | • AntiMalware<br>  • AntiVirus<br>  • AntiSpyware<br>• Management<br>• Patch Management<br>• Zero Day Threat Detection and Prevention | • Enterprise Mobility Management<br>• AntiMalware<br>  • AntiVirus<br>  • AntiSpyware<br>• Encryption<br>• Mobile Application Scanning | • Log Management<br>• SIEM<br>• Advanced Analytics<br>• GRC<br>• Threat Intelligence |

| Perimeter & UTM | Data | Identity & Access | Advanced Fraud |
|---|---|---|---|
| • Gateway Firewall/UTM<br>• Email Security/Gateway<br>• IPS/IDS/IDP<br>• URL Filtering/Web Gateway<br>• VPN Concentrator<br>• Sandboxing and APT Protection<br>• Penetration Testing<br>• Professional Assessment<br>• DoS and DDoS | • Encryption<br>• Backup and Restore<br>• Device control<br>• Database Activity Monitoring<br>• Data Loss Prevention<br>• Data and Discovery Classification | • Directory Management<br>• User Provisioning<br>• lifecycle management<br>• MultiFactor Authentication<br>• NAC<br>• Access Management | • Customer Fraud<br>• Criminal Fraud<br>• Mobile Fraud |

# What Does This Mean for Security Providers?

**Organizations need expert guidance.**

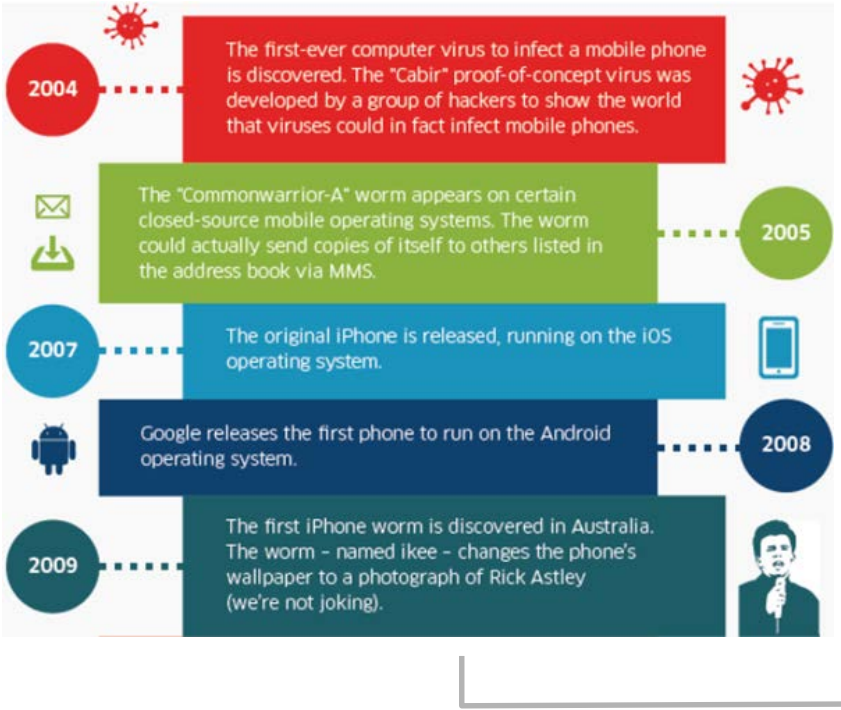
- Time to learn about security
- Become the trusted advisor
- Providing value that competitors can't match

***With $billions at stake, it pays to understand today's threat landscape.***

**Every business has a place in today's threat landscape.**

- Hackers eager to sell stolen information
- Easy for cybercriminals to commit acts of espionage
- Most businesses are unprepared

# Mobile Devices




# Cloud Presents New Threats

**The move to the cloud poses new security challenges.**

- Public and hybrid clouds put data in someone else's hands
- Is data safe at a cloud datacenter?
- Are cloud providers protecting business data?

# The Anatomy of an Attack

# Shadow IT

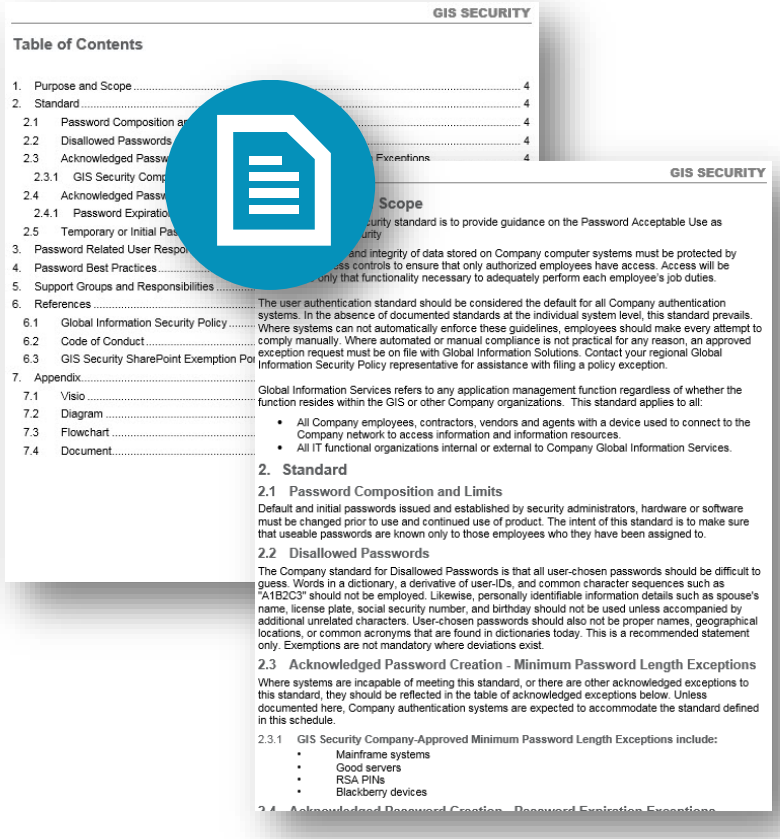
**Using solutions outside the control and governance of IT.**

- Lacks the security controls of IT-managed systems
- Puts company data at higher than normal risk
- No less dangerous than repelling attacks

# What Is A Corporate Security Policy?

**States how a company plans to protect physical and IT assets.**

- Continuously updated as technology and employee requirements change
- Educates employees about protecting company assets
- Shows how security measurements will be enforced
- Includes procedures for evaluating effectiveness of security policy



# Starting Security Conversations

# Starting Security Conversations

**Each role has a unique perspective on security.**

- CxOs (CEO, CIO, CISO)
- IT Director/Manager
- IT technicians and service team
- Influencers outside the IT structure

# Ask – Then Listen

Don’t engage with early-stage product discussions. Ask about:

- **Business goals for security –** Learning what the business expects from a comprehensive security solution
- **Compliance and regulatory concerns** –Ensure the business meets compliance requirements
- **Data storage and access** -- Understanding type of data the company stores, where they store it, and how users access it.
- **Current state** – Learn how they protect their IT assets, including endpoints, perimeter and mobile devices

# Learn As You Go

**Don’t worry about knowing it all up front.**

- Take what you learn from interviews and use it to dive deeper, do research and ask follow up questions
- Security is an ongoing process, not an end state
- Engage with the business on their needs, and uncover sales opportunities

# Become the Trusted Security Advisor

- Security offers a wealth of opportunities to grow revenue and strengthen customer relationships
- Businesses are making larger security investments to protect their critical corporate data
- Solution providers willing to invest in security education will reap the rewards and grow with the security marketplace

# Thank You!

Visit the Knowledge Network for more information and to engage with our Security Solutions team