



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



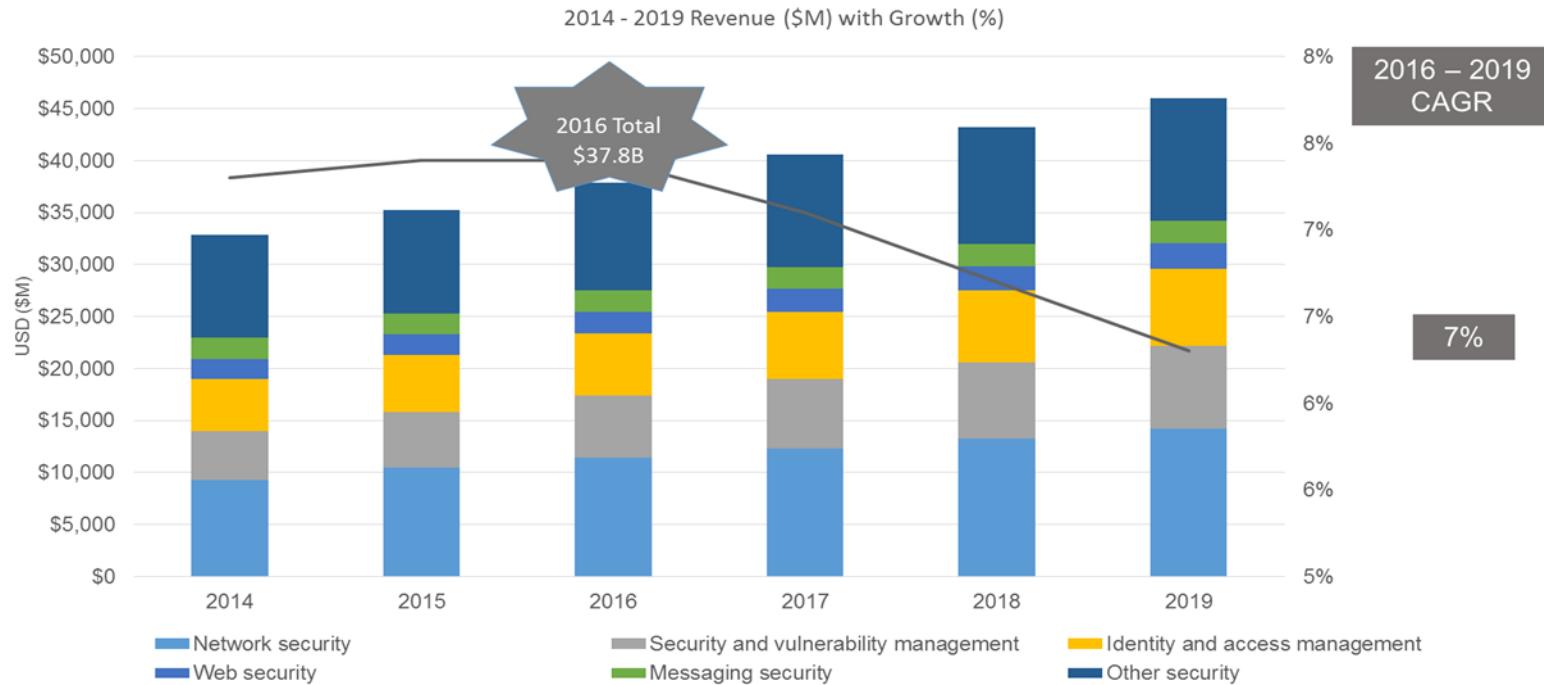
Security has rapidly evolved

- 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



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

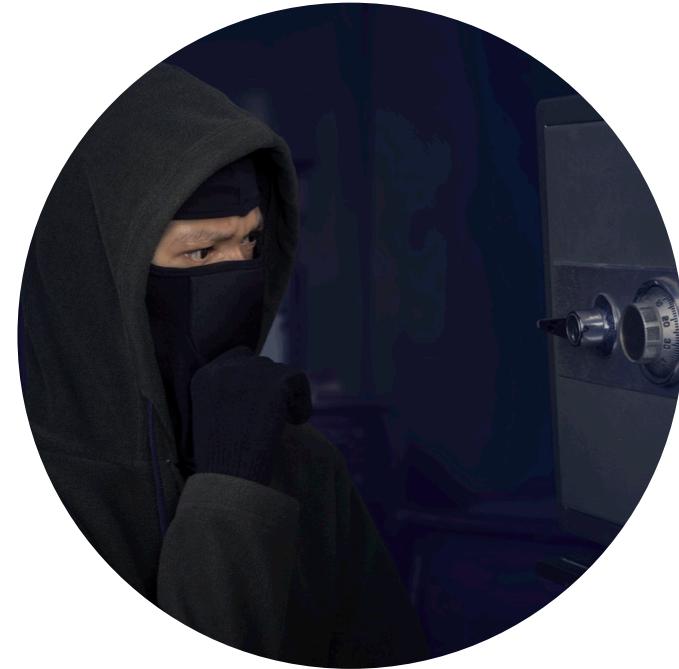
New approach to security requires a change in thinking.





When engaging a customer, ask yourself:

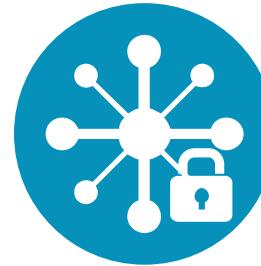
- What's valuable to cybercriminals?
- How would hacker or insider exploit the company?
- How to protect against these actions?





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

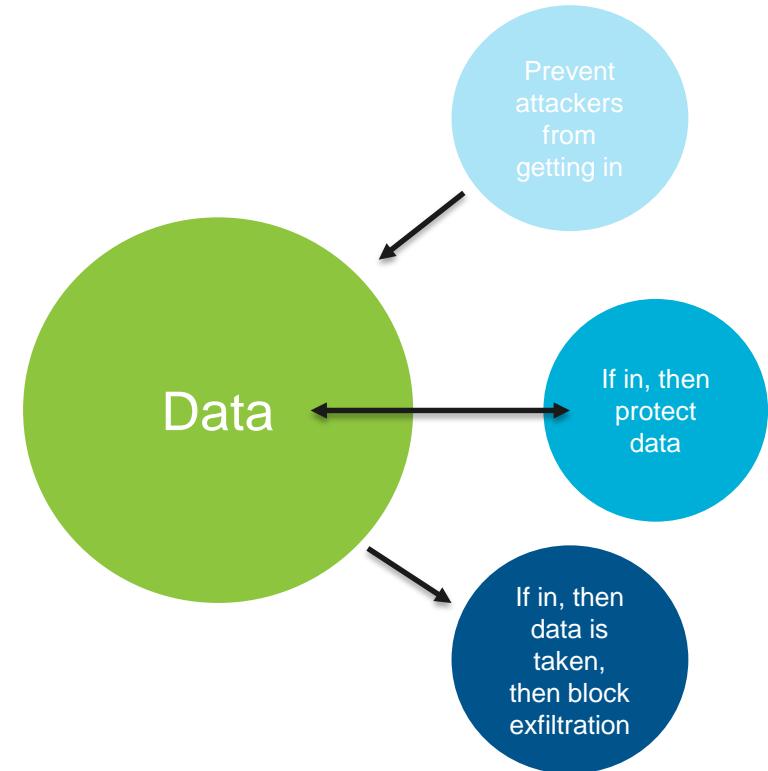




Primary Goals

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





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



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.



- **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.

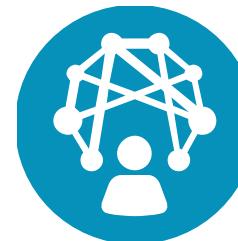
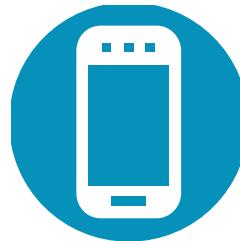
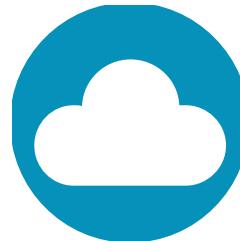
Security Concerns Fueling Rapid Market Growth



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 |
|---|--|---|--|--|
| <ul style="list-style-type: none"> • Web App Firewall • Web Security • WebInspect DAST | <ul style="list-style-type: none"> • Application Scanning • Source Code Analysis • Application Security | <ul style="list-style-type: none"> • AntiMalware <ul style="list-style-type: none"> • AntiVirus • AntiSpyware • Management • Patch Management • Zero Day Threat Detection and Prevention | <ul style="list-style-type: none"> • Enterprise Mobility Management • AntiMalware <ul style="list-style-type: none"> • AntiVirus • AntiSpyware • Encryption • Mobile Application Scanning | <ul style="list-style-type: none"> • Log Management • SIEM • Advanced Analytics • GRC • Threat Intelligence |



| Perimeter & UTM | Data | Identity & Access | Advanced Fraud |
|---|---|---|--|
| <ul style="list-style-type: none"> • Gateway Firewall/UTM • Email Security/Gateway • IPS/IDS/IDP • URL Filtering/Web Gateway • VPN Concentrator • Sandboxing and APT Protection • Penetration Testing • Professional Assessment • DoS and DDoS | <ul style="list-style-type: none"> • Encryption • Backup and Restore • Device control • Database Activity Monitoring • Data Loss Prevention • Data and Discovery Classification | <ul style="list-style-type: none"> • Directory Management • User Provisioning • Lifecycle management • MultiFactor Authentication • NAC • Access Management | <ul style="list-style-type: none"> • Customer Fraud • Criminal Fraud • 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.



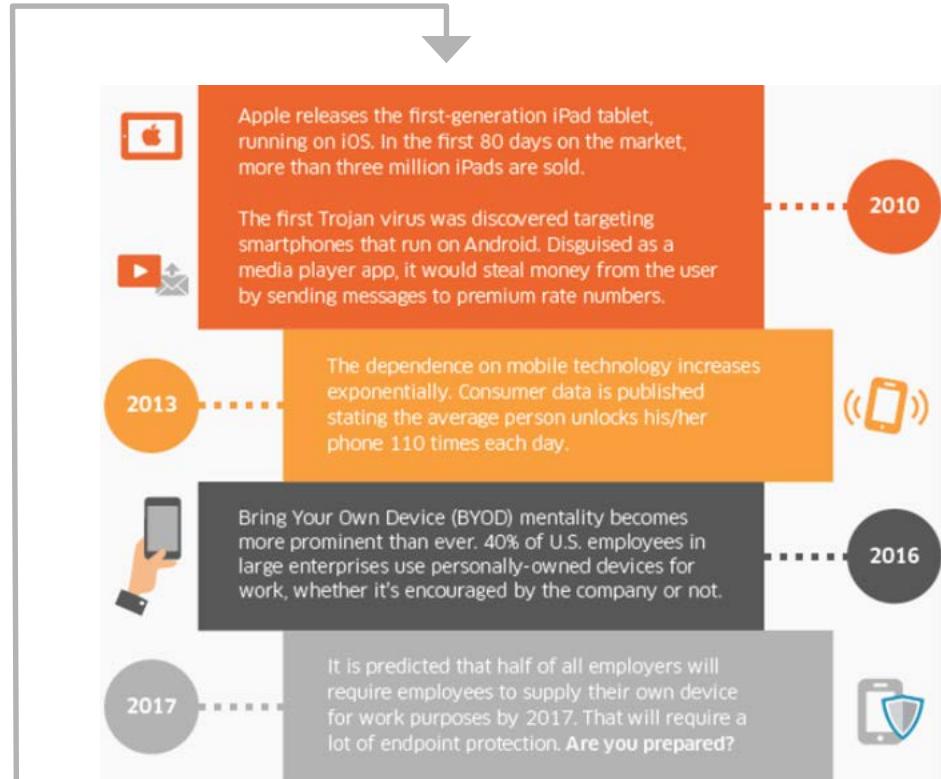
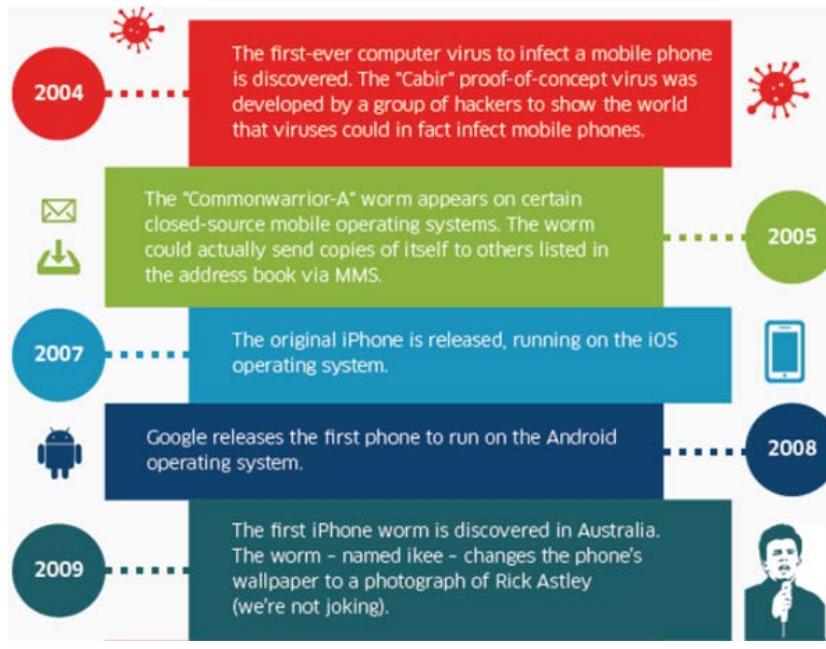


Every business has a place in today's threat landscape.

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



Mobile Devices





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





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

The screenshot shows a table of contents for a 'GIS SECURITY' document. The table of contents includes sections such as Purpose and Scope, Standard, Password Related User Response, Password Best Practices, Support Groups and Responsibilities, References, and Appendix. The 'Standard' section is highlighted with a blue circle containing a white document icon. The 'Scope' section is also visible at the bottom of the page.

Table of Contents

1. Purpose and Scope
2. Standard
- 2.1 Password Composition and Limits
- 2.2 Disallowed Passwords
- 2.3 Acknowledged Passwords
- 2.3.1 GIS Security Company-Acceptable Use Exceptions
- 2.4 Acknowledged Password Creation
- 2.4.1 Password Expiration
- 2.5 Temporary or Initial Passwords
3. Password Related User Response
4. Password Best Practices
5. Support Groups and Responsibilities
6. References
- 6.1 Global Information Security Policy
- 6.2 Code of Conduct
- 6.3 GIS Security SharePoint Exemption Po
7. Appendix
- 7.1 Visio
- 7.2 Diagram
- 7.3 Flowchart
- 7.4 Document

Scope

This security standard is to provide guidance on the Password Acceptable Use as well as the protection and integrity of data stored on Company computer systems must be protected by Company security controls to ensure that only authorized employees have access. Access will be limited only to functionality necessary to adequately perform each employee's job duties.

Standard

2.1 Password Composition and Limits

The user authentication standard should be considered the default for all Company authentication systems. In the absence of documented standards at the individual system level, this standard prevails. Where systems can not automatically enforce these guidelines, employees should make every attempt to comply manually. Where automated or manual compliance is not practical for any reason, an approved exception request must be on file with Global Information Solutions. Contact your regional Global Information Security Policy representative for assistance with filing a policy exception.

2.2 Disallowed Passwords

The Company standard for Disallowed Passwords is that all user-chosen passwords should be difficult to guess. Words in a dictionary, a derivative of user-IDs, and common character sequences such as "A1B2C3" should not be employed. Likewise, personally identifiable information details such as spouse's name, license plate, social security number, and birthday should not be used unless accompanied by additional unrelated characters. User-chosen passwords should also not be proper names, geographical locations, or common acronyms that are found in dictionaries today. This is a recommended statement only. Exemptions are not mandatory where deviations exist.

2.3 Acknowledged Password Creation - Minimum Password Length Exceptions

Where systems are incapable of meeting this standard, or there are other acknowledged exceptions to this standard, they should be reflected in the table of acknowledged exceptions below. Unless documented here, Company authentication systems are expected to accommodate the standard defined in this schedule.

2.3.1 GIS Security Company-Accepted Minimum Password Length Exceptions include:

- Mainframe systems
- Good servers
- RSA PINs
- BlackBerry devices

2.4 Acknowledged Password Creation - Password Expiration Exceptions



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



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