The Cyber Threat Landscape

Oliver Rochford

Research Director

Gartner

First You See Me …

External Attack

Internal Attack

… Then You Don't!

Gartner

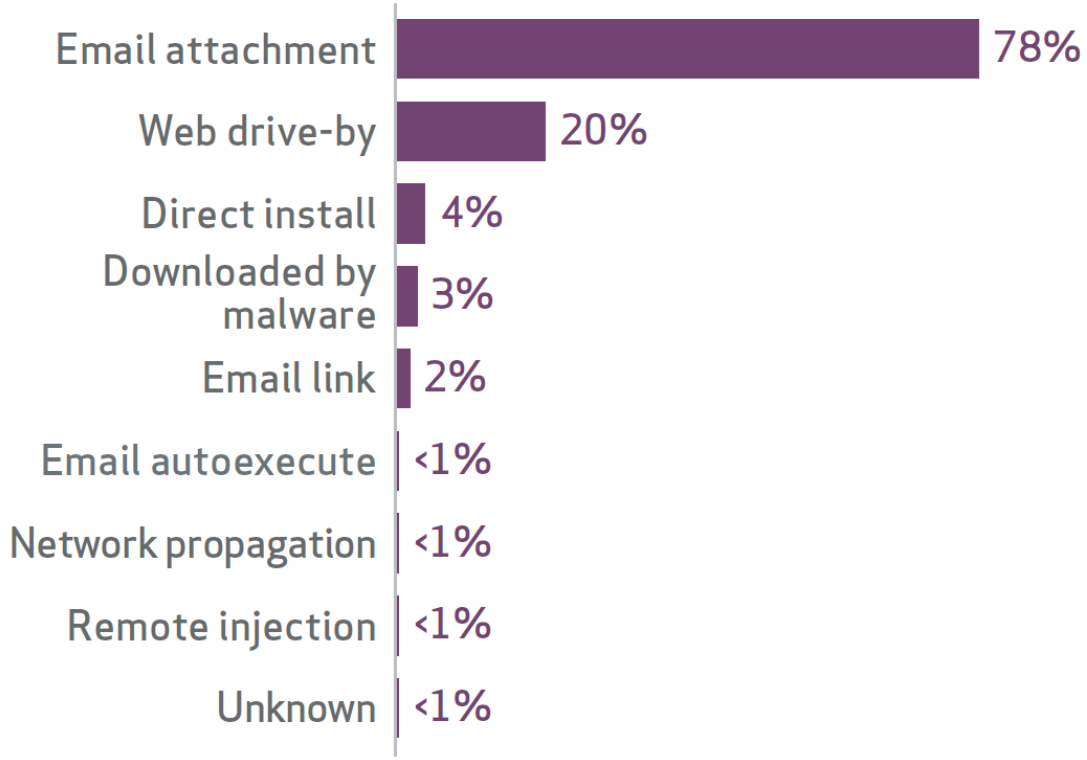
Key Issues

1. What are the **key trends** in cybersecurity attacks?
2. Which **tools and processes** should enterprises adopt to defend against these attacks?
3. What are the **best practices** for mitigating cyberthreats?

Gartner

Spear Phishing Still Works

Vector for malware actions within cyber-espionage



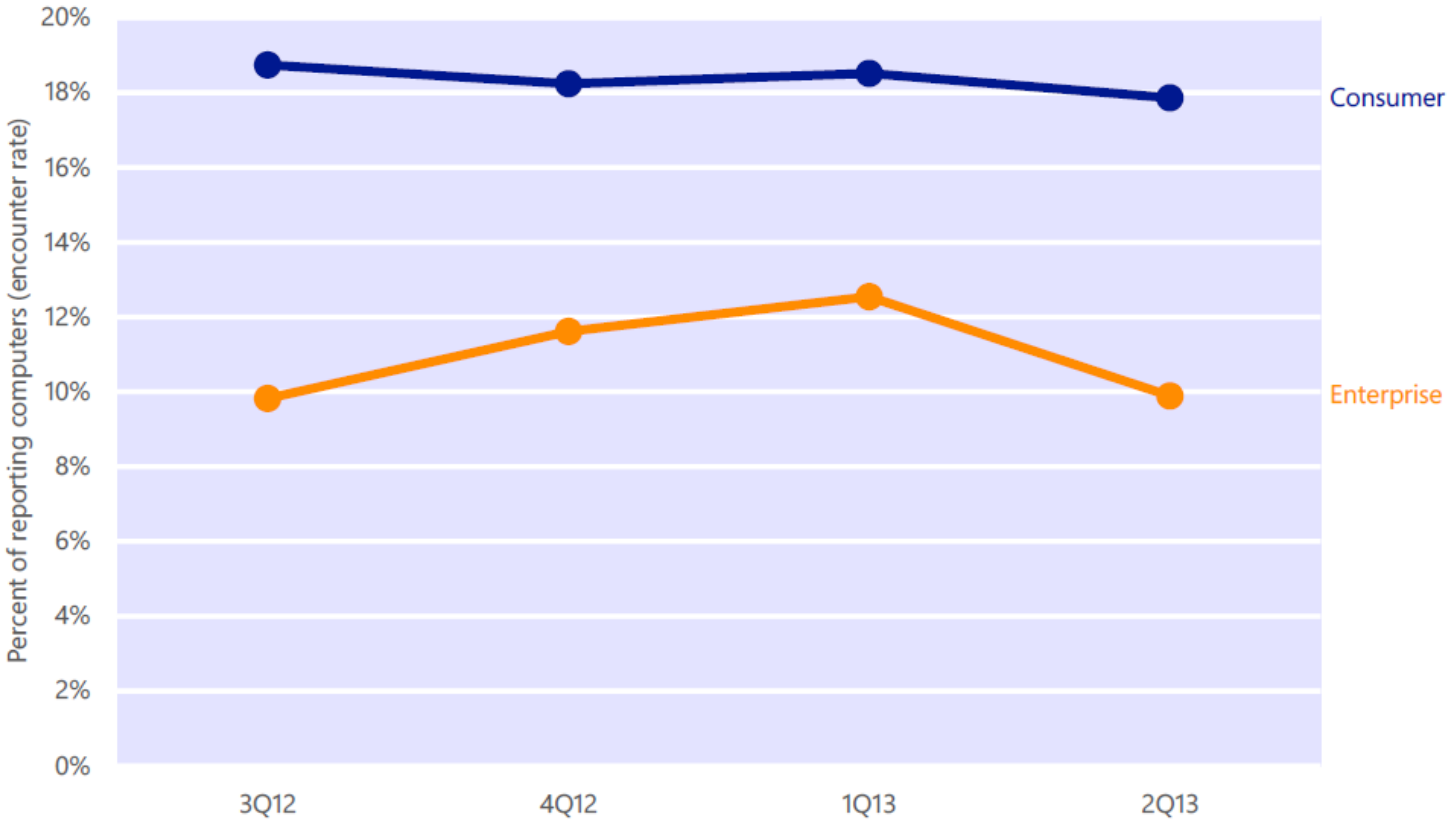
n = 329

Source: Verizon 2014 Data Breach Investigations Report

Gartner

Malware Rates: Consumers Outpace Enterprises Nearly 2x

A Challenge for BYOD



Source: Microsoft Security Intelligence Report, Volume 14, July through December, 2012

Gartner

Off-network Traffic Grows to 25% by 2018

*By 2018, **25%** of corporate data traffic will bypass perimeter security (up from **4%** today) and flow directly from mobile devices to the cloud.*

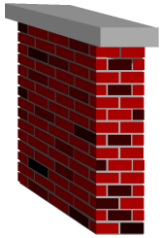
Gartner Predicts 2014: Infrastructure Protection, 25 November 2013

Gartner

We Call Them "Advanced" Threats …

Because they bypass traditional defenses:

Firewall



Intrusion Prevention

Endpoint Protection

Secure Web Gateway

Secure Email Gateway

Traditional defense-in-depth components are still necessary, but are no longer sufficient.

Gartner

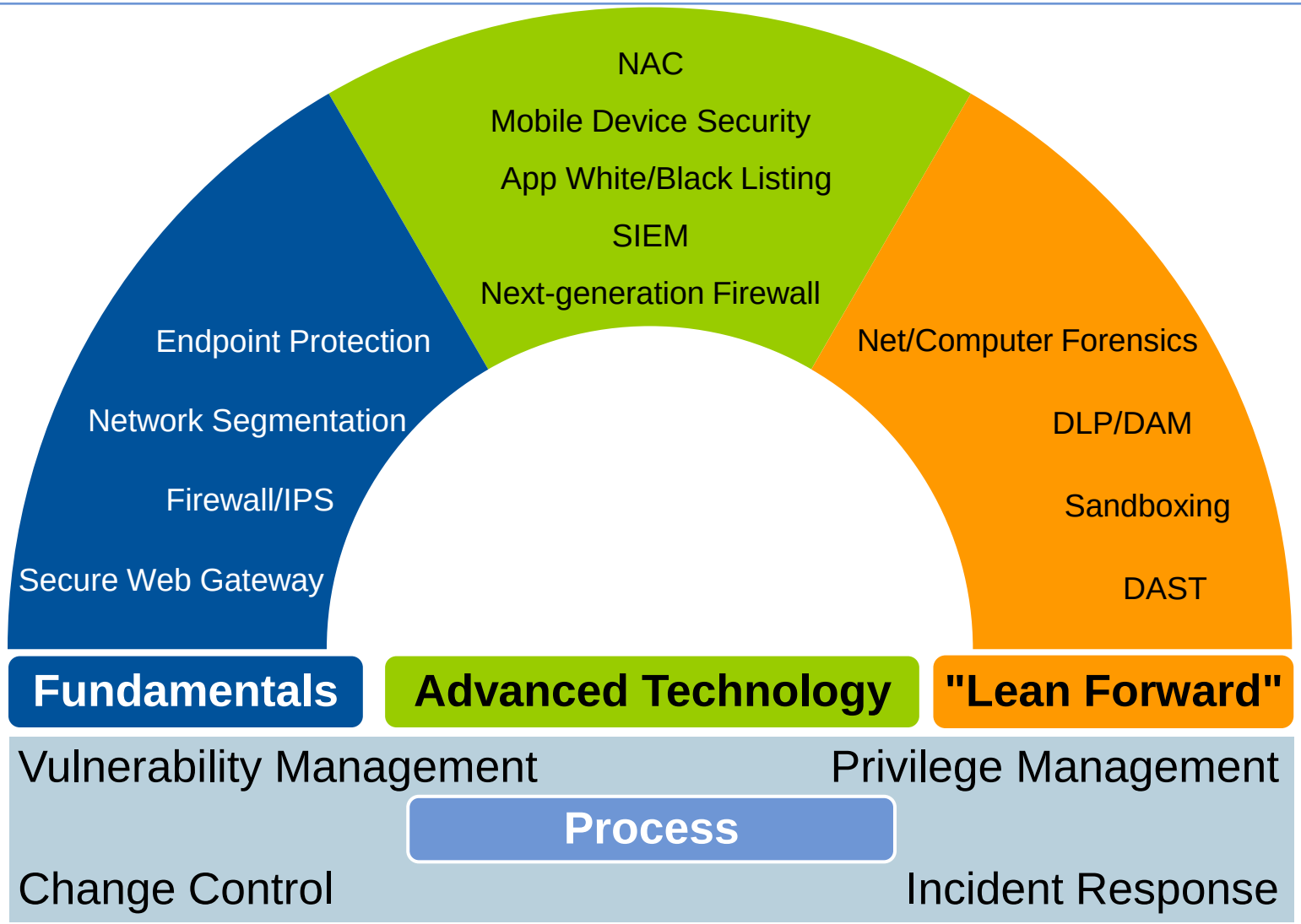
Cyberattack on German Steel Plant

- Unnamed steelplant targeted in Germany
- Multistage persistant attack, initiated via spearphishing
- Control components were manipulated, leading to damage to a blast furnace
- Germanys Federal Agency for Information Security (BSI) stated the attackers possessed advanced technical knowledge of OT

Source: https://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report

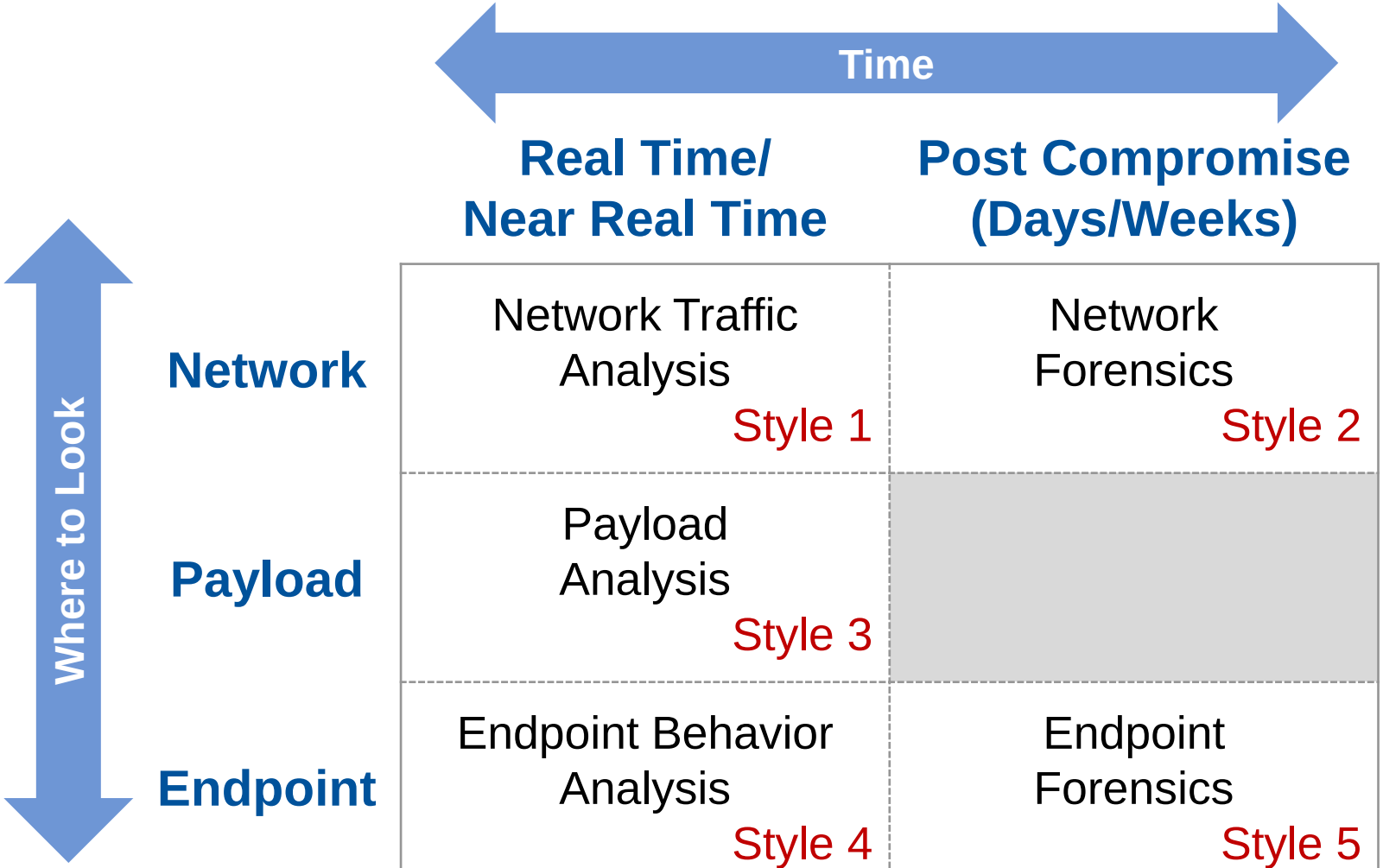
Gartner

Defending Against Targeted Attacks



Gartner

Five Styles of Advanced Threat Defense



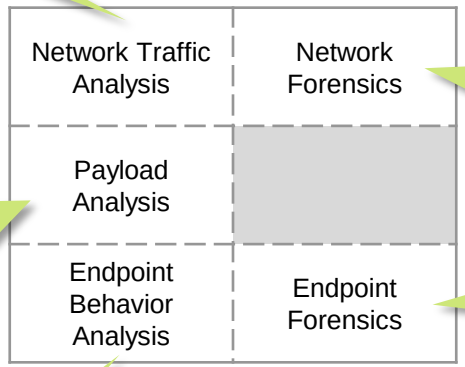
Gartner

Five Styles — Sample Vendors

Arbor Networks, Damballa, Lancope, Fidelis, Cisco (Sourcefire), Vectra

AhnLab, Cyphort, FireEye, Lastline, Blue Coat (Norman Shark), Cisco (ThreatGRID), Fortinet, McAfee, Trend Micro, Check Point Software Technologies, Palo Alto Networks, Proofpoint, Websense, Zscaler

Bromium, CounterTack, Invincea, Palo Alto Networks (Cyvera), ManTech, RSA, The Security Division of EMC, Triumfant, IBM (Trusteer)



Arbor Networks, IBM (QRadar), LogRhythm, FireEye (nPulse) RSA NetWitness, Blue Coat (Solera Networks)

Bit9 (Carbon Black), Guidance Software, FireEye (Mandiant), ManTech

Sample vendors — not an exhaustive list

Gartner

Recommendations

- ✓ Update your layered defense strategy:
  - Adopt "lean forward" technologies.
  - Use five-styles framework.
- ✓ Protect mobile workers:
  - 25% of traffic will bypass traditional security defenses.
  - Consider cloud security services.
- ✓ Present a hard target — focus on fundamentals:
  - Vulnerability management, change management, incident response and others.
  - Develop mature processes.

Gartner

Recommended Gartner Research

- **Five Styles of Advanced Threat Defense**
  Lawrence Orans and Jeremy D'Hoinne (G00253559)
- **Using SIEM for Targeted Attack Detection**
  Oliver Rochford and Kelly Kavanagh (G00260253)
- **Leverage Your Network Design to Mitigate DDoS Attacks**
  Andrew Lerner and Lawrence Orans (G00253330)
- **Adapting Vulnerability Management to Advanced Threats**
  Mark Nicolett (G00227901)

For more information, stop by Gartner Research Zone.

Gartner