

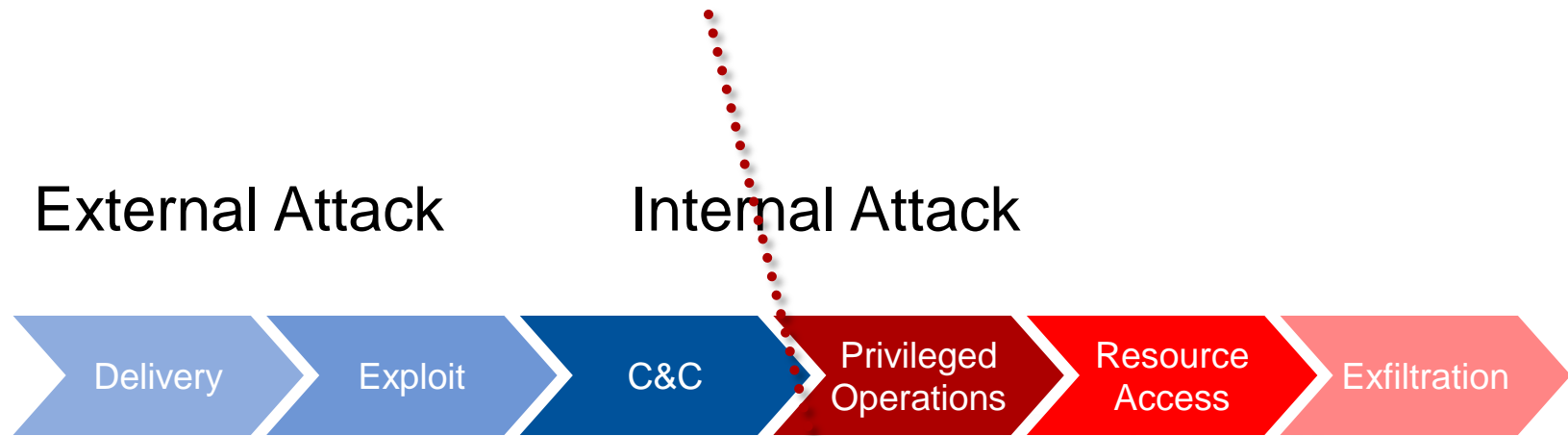
The Cyber Threat Landscape

Oliver Rochford
Research Director

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the [Usage Guidelines for Gartner Services](#) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "[Guiding Principles on Independence and Objectivity](#)."

Gartner[®]

First You See Me ...



... Then You Don't!

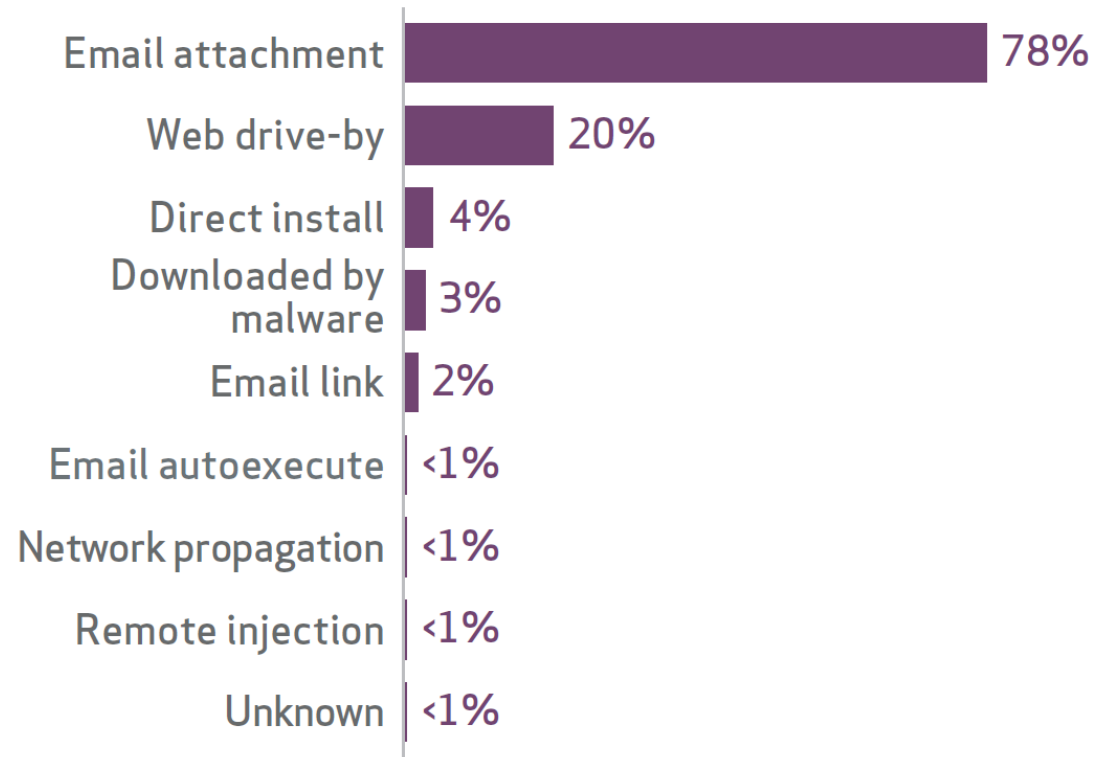


Key Issues

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?

Spear Phishing Still Works

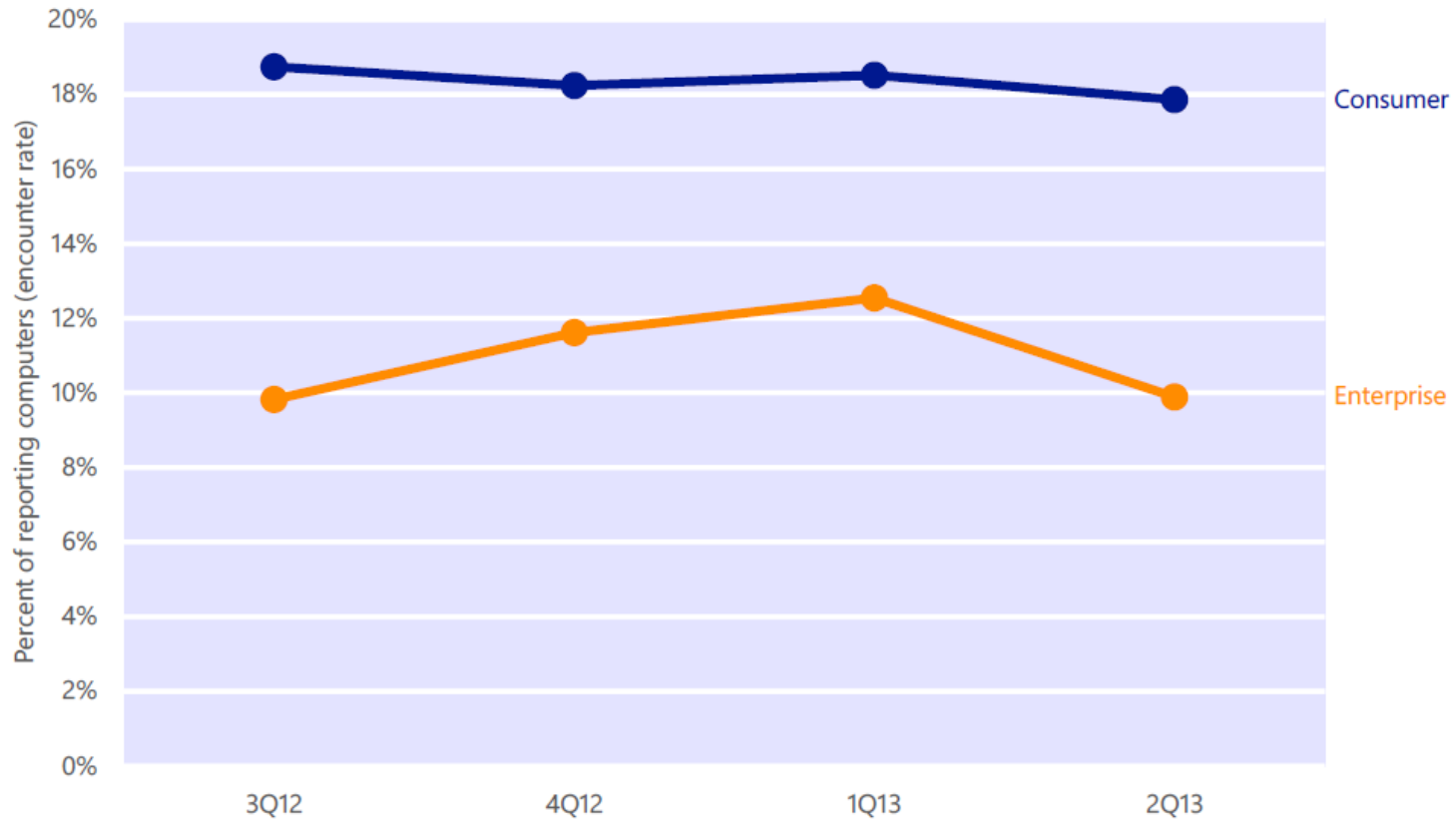
Vector for malware actions within cyber-espionage



n = 329

Malware Rates: Consumers Outpace Enterprises Nearly 2x

A Challenge for BYOD



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

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.

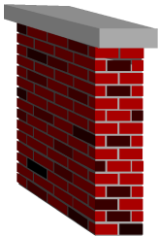
Off-network Traffic Grows to 25% by 2018

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

We Call Them "Advanced" Threats ...

Because they bypass traditional defenses:

Firewall



**Intrusion
Prevention**



**Endpoint
Protection**



**Secure
Web
Gateway**



**Secure
Email
Gateway**



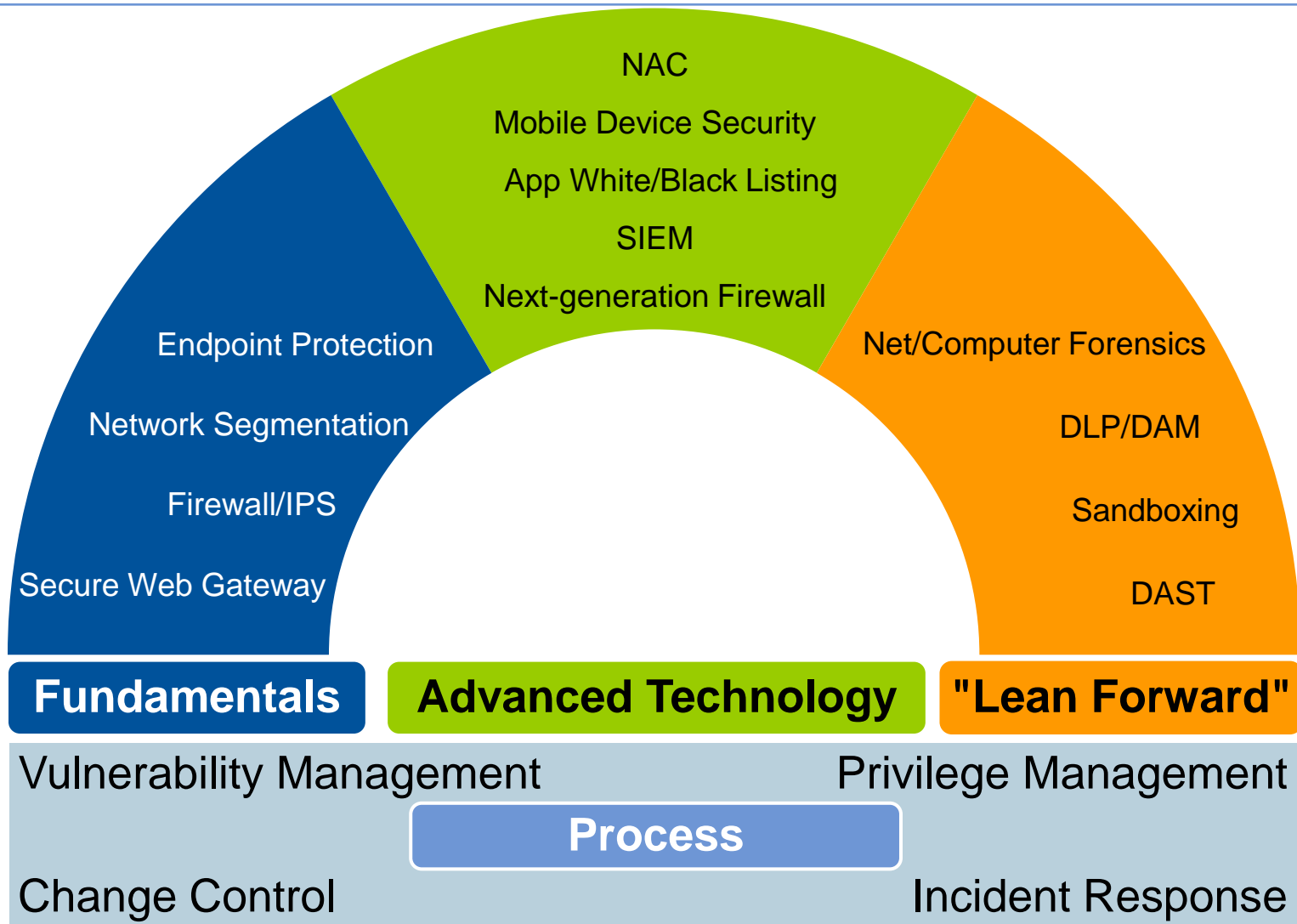
Traditional defense-in-depth components are still necessary, but are no longer sufficient.

Cyberattack on German Steel Plant

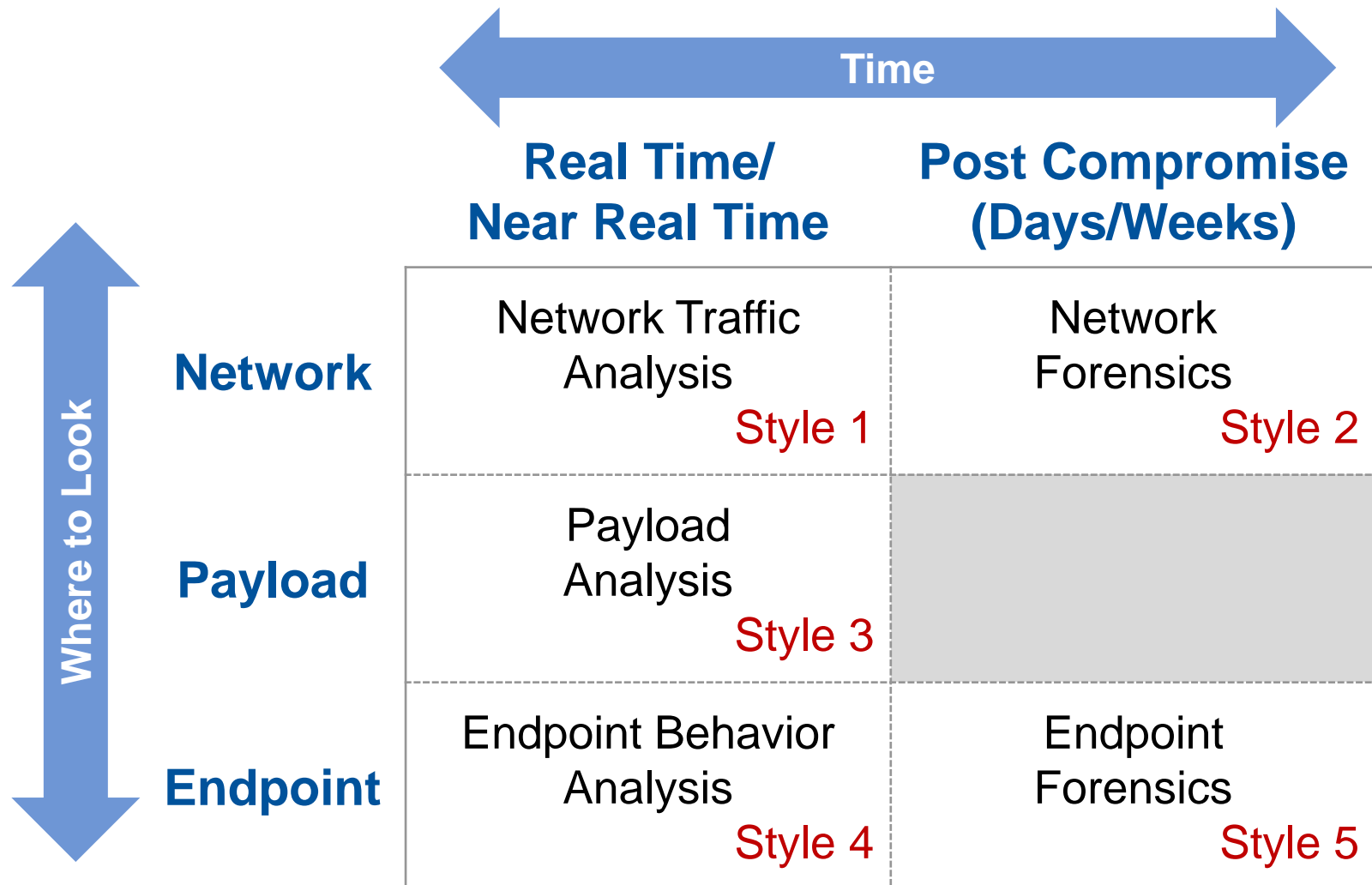
- Unnamed steelplant targeted in Germany
- Multistage persistent attack, initiated via spearphishing
- Control components were manipulated, leading to damage to a blast furnace
- Germanys Federal Agency for Information Security (BSI) stated the attackers possessed advanced technical knowledge of OT

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

Defending Against Targeted Attacks



Five Styles of Advanced Threat Defense



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, Triumphant, IBM (Trusteer)

Network Traffic Analysis	Network Forensics
Payload Analysis	
Endpoint Behavior Analysis	Endpoint Forensics

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

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.

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.

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)