

The background of the slide is a dark blue gradient. On the right side, there are three vertical bars of increasing height and a color gradient from blue to green. The background also features a faint, glowing network diagram with circular nodes and connecting lines, and a close-up image of a metal padlock.

# Cisco Security Intelligence Operations Defense in Depth

Scott Simkin, Cisco® Security Product and Solutions Marketing

May 2013

# Agenda

Threat Evolution

Cisco Security Framework

Cisco® Security Intelligence Operations  
(SIO) Portal Overview

Breadth and Context

Cisco SIO Portal Defense

Threat Example

# Threat Landscape Evolution

Response

Host-based  
(antivirus)

2000

Network perimeter  
(IDS and IPS)

2005

Global reputation  
and sandboxing

2010

Intelligence  
and analytics

Tomorrow

Threats

Worms

Chat

Application

Wireless

Yahoo

Laptop

Spyware and rootkits

Adobe PDF

Google  
Chrome

USB

Firefox

Internet  
Explorer

Java

Flash

Server

Users

Application

Network

Advanced persistent threats  
(APTs) and cyberwar

Digg

VMWare

Newsvine

Flickr

Myspace

Youtube

Delicious

Netvibes

MobileMe

RSS

Reddit

Technorati

StumbleUpon

Facebook

Twitter

Increased attack surface  
(mobility and cloud)

Salesforce

Mac  
iOS

iCloud

Gmail

Nokia mobile

Blackberry  
mobile

Dropbox

Cisco WebEx

Box net

Amazon

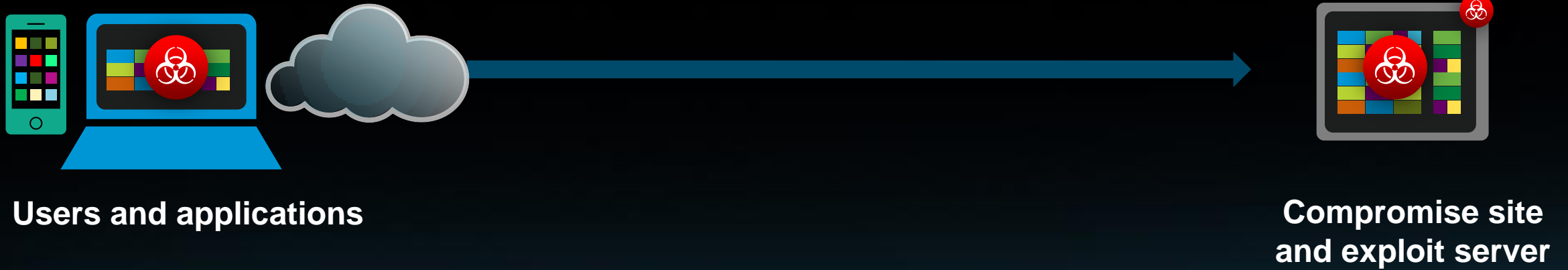
iphone

iPad

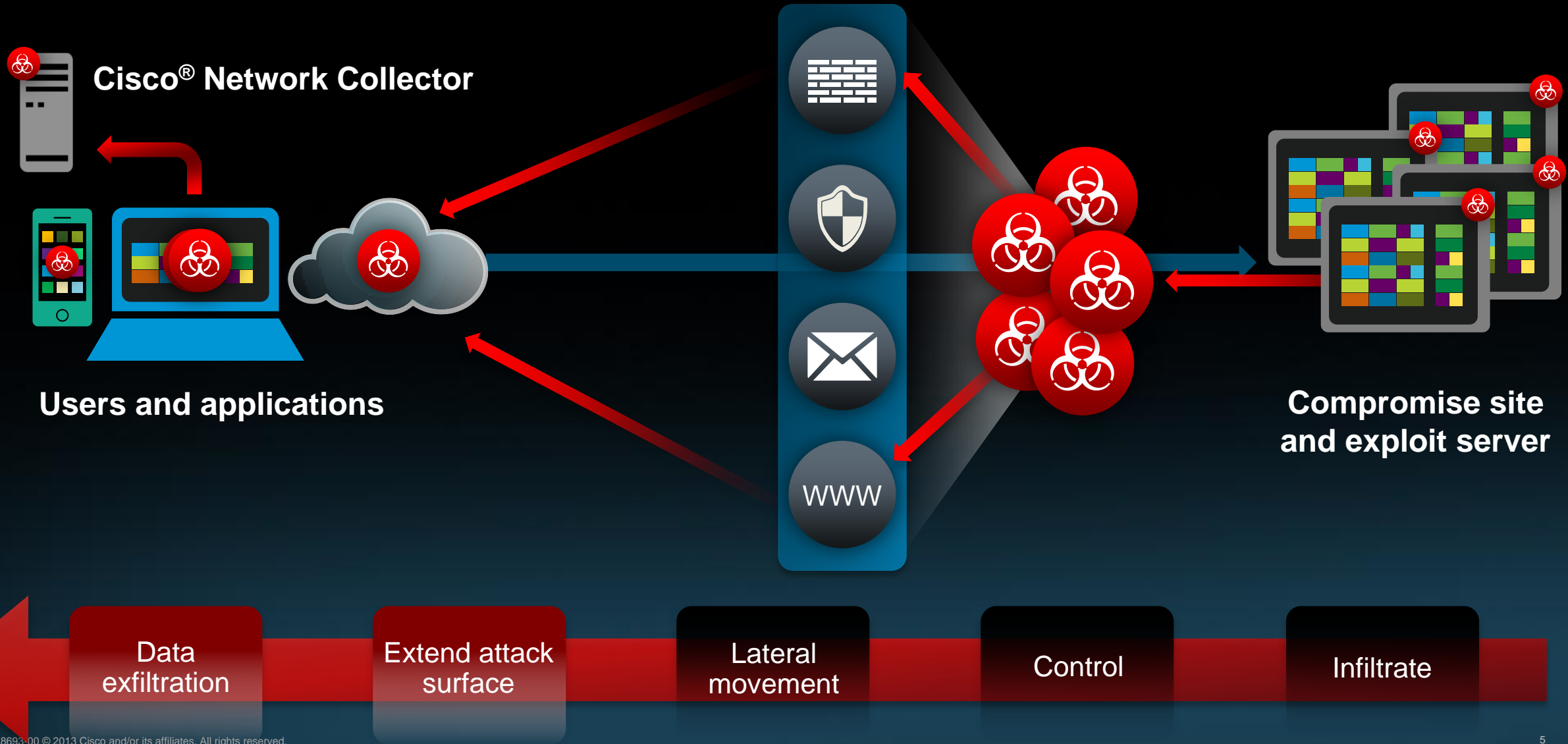
Android

Microsoft  
Office

# Advanced Cyber Threats



# Advanced Cyber Threats





## Cloud-based threat intelligence and defense

Attacks

Third-party feeds

Reputation And rules

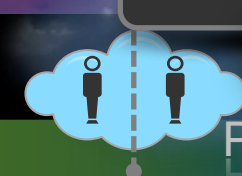
Malware analysis

Global

Local



Infrastructure



Public



Applications and services



Hybrid



Tenants



Workloads

Private



## Common policy, management, and context

Common management

Shared policy

Analytics

Compliance

Partner API

Identity

Application

Device

Location

Time

## Network-enforced policy

Access

Firewall

IPS

VPN

Web

Email

Appliances

Routers

Switches

Wireless

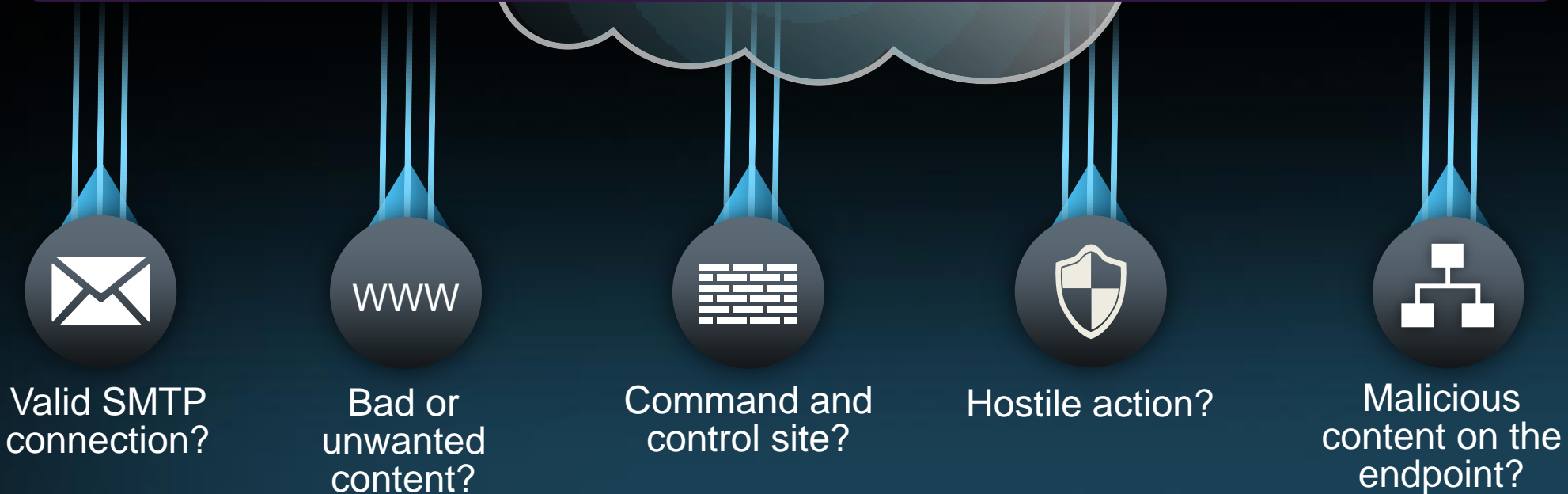
Virtual










# A More Integrated Approach

# Defend with Intelligence

## Cisco® Security Intelligence Operations



-  Blocklists and reputation
-  Spam traps, honeypots, and crawlers
-  Domain registration
-  Signatures
-  Content inspection
-  Third-party partnerships
-  Threat research

# Defend with Intelligence





Discovery with Breadth

100 TB  
of daily security intelligence

# Discovery with Breadth

**100 TB**  
of security  
intelligence

1.6 million  
deployed security devices

# Discovery with Breadth

**100 TB**

of security  
intelligence

**1.6**

**million**  
deployed  
devices

13 billion

daily web requests

# Discovery with Breadth

**100 TB**  
of security  
intelligence

**1.6  
million**  
deployed  
devices

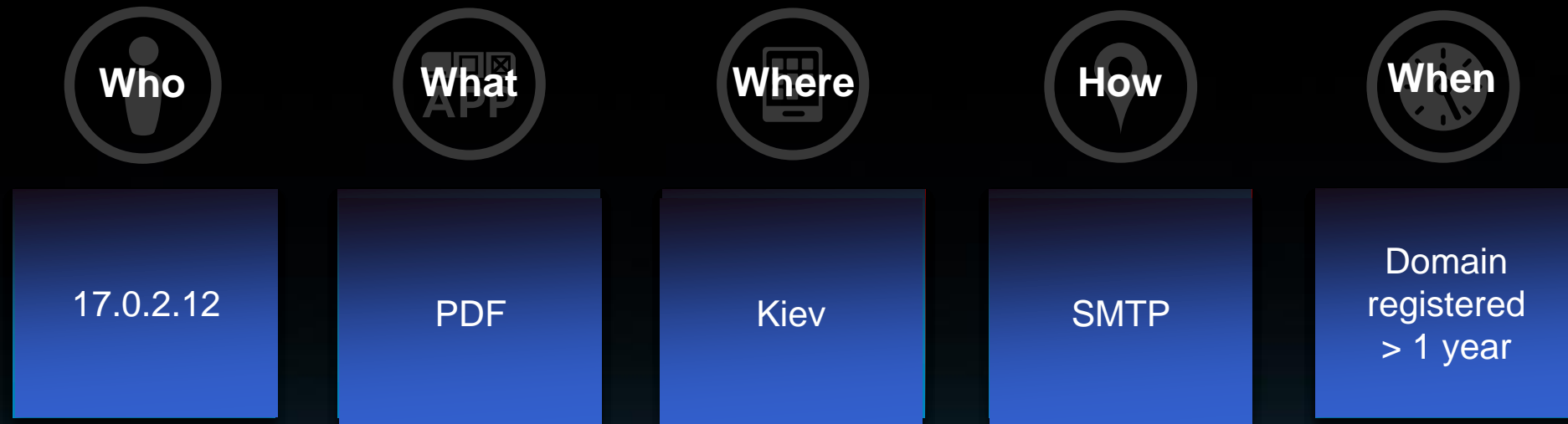
**13  
billion**  
web  
requests

150,000  
applications  
and micro-applications

<b>100 TB</b> of security intelligence	<b>150,000</b> micro-applications	<b>5500</b> IPS signatures	<b>5 billion</b> daily email connections
<b>1.6 million</b> deployed devices	<b>93 billion</b> daily email messages	<b>150 million</b> deployed endpoints	<b>1000</b> applications
<b>13 billion</b> web requests	<b>35%</b> enterprise email	<b>3 to 5-minute</b> updates	<b>4.5 billion</b> daily email blocks

Cisco® Security Intelligence  
Operations  
Broad visibility  
Global footprint  
Defense in depth

# Discovery with Context



# Discovery with Context



Suspicious  
domain  
owner



Poorly  
structured  
PDF



Server in  
high-risk  
location



Dynamic IP  
address



Domain  
registered  
< 1 minute



# Cisco SIO Defense Flow





# Cisco SIO Defense Flow

Example



# Microsoft Internet Explorer Zero-Day Vulnerability

**Day 0**  
Zero-day malware  
In the wild

**Day 16**  
First antivirus  
signature deployed

**Day 17**  
Second antivirus  
signature deployed

**Day 18**  
Third antivirus  
signature deployed

**Traditional response**

Security advisory  
issued

Microsoft IE  
patched

# Microsoft Internet Explorer Zero-Day Vulnerability

**Day 0**  
Zero-day malware  
blocked by Cisco

**Day 14**  
Cisco® IPS signature  
CNC server blocked

Cisco SIO Proactive Defense

Multiple attack vectors and multiple layers of defense

- **Cisco SIO cross-platform** intelligence
- **Blocked** zero-day threat
- **Blocked** 40+ “parked” domains
- **Blocked** exploit server and CNC
- **18-day** lead time

# Cisco SIO: Defense in Depth



# Learn more about Cisco Security Intelligence Operations



<http://cs.co/ciscosio4>



**CISCO**