What Is Your Mobile Content Policy? A Checklist for Content Risk Mitigation

Sponsored by SAP

What Is Your Mobile Content Policy?
A Checklist for Content Risk Mitigation

November 2012

A SANS Whitepaper

Written by: Barbara Filkins

Introduction

We are living in a world that only 20 years ago was the realm of science fiction. Devices once just barely imaginable have become common consumer items, carried casually in pockets and purses, with constantly growing capabilities. Our smartphones are becoming extensions of ourselves. With a world of content at our fingertips, we embed ourselves in a near constant stream of "conversations" and rich media including images, audio, video and voice.

By the end of 2012, there are likely to be more smartphones on the planet than humans, according to the October 2012 Cisco Global Cloud Index study.[1] The rapid growth of mobile device usage is accompanied by significant growth in cloud data transmission and storage. The study also predicts that global cloud application traffic will reach 355 exabytes per month by the end of 2016, or more than four zettabytes annually, with a compound annual growth rate (CAGR) of 44 percent from 2011 to 2016. By 2016, global cloud application traffic is expected to account for nearly two-thirds of total data center traffic.

Flowing through this traffic is critical content once managed within the confines of the enterprise. However, with today's user-driven demand for mobile access, and the obvious cost benefits therein, content protection calls for new policies. Unfortunately, these policies are lacking, according to the SANS Survey on Mobility/BYOD Policies and Practices, also released in October 2012. In it, more than 95 percent of the 650-plus respondents stated that policy is a critical protection that needs to be integrated into an all-encompassing security risk management scheme. Yet 38 percent do not have the policies they feel are necessary, and many rely primarily on user education and agreements without implementing Mobile Device Management (MDM) as part of their security strategy.[2]

Content management tools must now adapt to and embrace mobile users accessing systems and content, including content processed in the cloud. To scale to this brave new world, protection policies must focus on the content being accessed and processed, as well as the context in which it is used. Policies also need to validate compliance, which may not be fully achievable at this time. Tools and techniques that support these unique content protection needs are evolving, along with the changing landscape of mobile and cloud computing.

1 www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.html

2 www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

Content Management: Enablers and Challenges

Content management technologies descend from the standalone electronic document management systems (EDMS) introduced in the late 1980s and early 1990s. Those evolved to become Enterprise Content Management (ECM) platforms, supporting networked EDMS solutions such as PCDocs and Documentum. By 2006, ECM was gaining widespread acceptance as an integral part of online business, and the acceptance of Microsoft SharePoint changed the way that many viewed online collaboration.[3] Today, the line between social media and online collaboration has blurred the rules around secure content management, especially when users access business content from a personal or corporate mobile device.

Several enablers drive the evolution of secure enterprise content management, including the following:

1. **Bandwidth and content acceleration.** Cheap bandwidth is virtually everywhere, or at least where a vast majority of business is conducted, allowing the delivery of high-quality video and voice at low cost and delivery of multimedia-rich content at the point of use. Organizations grapple with increasing amounts and diversity of content—documents, scanned images, web content, rich media, e-mail, corporate records, blogs, wikis, e-forms, audio and video—each with its own editing process and workflow requirements.
2. **Mobile device power.** A mobile phone is no longer just a device to talk on. Smartphones and tablets are true computing platforms that connect users to a world of content in the cloud, both for social and business benefits. Device management tools have also evolved, acting as gatekeepers for content. A decade ago, management was about the network, the servers, and the applications: What passed for content management was usually limited to device backups and screening for hostile content. Today, mobile platforms have basic manageability baked in; corporate IT can remotely wipe devices that leave the device usable while selectively removing company-owned data.
3. **User expectations and demands.** Today, people expect to share content, whether a family photo, a business document, a patent application, or a radiographic image for medical diagnosis, no matter where they are. They expect to communicate conveniently via voicemail, e-mail, or instant messaging wherever they go. Today's expectations will become tomorrow's demands. As the complexity and richness of content increases, so will user demands that this content be seamlessly delivered to their mobile devices.

In this environment, just what are the threats to an enterprise's content? Perhaps the greatest is that mobile devices are potential hostiles, having an average of 41 installed apps,[4] not all of which may be under a company's control. A great deal of the content on these devices uses the cloud—from e-mail, to hosted financial and workforce applications, to collaborative applications like Box.

3 www.mhprofessional.com/downloads/products/0071743677/0071743677_chap01.pdf, page 3.

4 thenextweb.com/insider/2012/05/16/nielsen-us-smartphones-have-an-average-of-41-apps-installed-up-from-32-last-year/

In 2008, Tim O'Reilly said at that year's Web 2.0 Summit, "Everything we think of as a computer today is really just a device that connects to the big computer that we are all collectively building."[5] Content delivery and management need to adapt to this reality. Along the same lines, access to content and services should be consistent across multiple platforms—whether smartphone, tablet, or workstation.

To develop security rules for content protections in this open and potentially hostile environment, the context of the content becomes just as critical as the content itself. Industry-specific regulatory and compliance statutes require knowledge of the how, where, and when content is used and managed. Rules for access should be based on user role, the device being used, the content being accessed and the user's geographical location, among other information.

5 Joyent, (2008) video, www.youtube.com/watch?v=6PNuQHUiV3Q

Creating a Secure Content Policy

The October 2012 SANS Mobility Survey notes that organizations are experiencing significant confusion about what content controls to adopt. In the survey, less than 10 percent of respondents confirmed that their organizations fingerprint sensitive data or employ device-level encryption, despite the clear value of these technologies.[6] More respondents, but still not enough, are deploying or considering Mobile Device Management (MDM). Overall, the survey shows much confusion around the use of such tools as exist today, so organizations are falling back to relying mostly on user education and use agreements, despite their ineffectiveness.

Policy for protecting content across services depends on the nature of the platforms used to consume, manage and deliver various types of information. Each presents its own problem: e-mail and instant messaging support limited file exchange and, along with secure FTP, lack versioning capabilities. Social media tools raise concerns over privacy and ownership, and content in the cloud puts management and visibility outside the realm of current controls. These shortcomings within platforms are vulnerabilities, and they must be considered when developing content-aware policy to traverse cloud and mobile devices.

Start by looking at protection from the infrastructure outward. Basic assumptions for such protection should include the following:

- ✔ Secure distribution across multiple platforms, with controls for content ownership equal to or better than those for traditional clients
- ✔ Protection of content at both company-owned and employee-owned endpoints, with an assumption of hostile applications installed and vulnerable services enabled
- ✔ Seamless file access, synchronization and transfer, with robust identity management and the ability for real-time revocation of permissions throughout the enterprise
- ✔ An established basis (i.e., a reference architecture) for building other apps (such as context awareness) that support data in the cloud, on-premises storage or a hybrid approach

To help visualize the problem, let's consider some simple building blocks for secure ECM in the cloud, as listed in Table 1.

6 www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

Building Block	Definition	Cloud Model
Content	The object of secure content management—information, data, business rules, policy documents, data-driven services and applications. Content has embedded properties or characteristics that dictate its behavior in a specific context. Active content should be of special concern as it "can carry out or trigger actions automatically without an individual directly or knowingly invoking the actions."[7]	SaaS
Integration and Management	Manages the processes and technologies at the heart of an ECM platform—collection, management and publishing of digital information in any form or medium—as well as providing content management services that enforce policies and security that addresses the use of content. This layer binds these elements to the underlying infrastructure processes and tools needed to enforce that security. Today, this may include using the enterprise Active Directory as an identity manager for the ECM tools, with manual review of ECM logs. In the future, robust services should know how to act on characteristics embedded in content, given the context of how, when and by whom the content is sought. Auditing will provide a rich set of events with information from the ECM, MDM, Identity Management (IdM), and Security Information Event Management (SIEM) tools, allowing an end-to-end understanding of the events relating to individual content items.	PaaS
Infrastructure and Mechanics	Virtual or physical computing resources, storage, and network services. This layer, being dependent on third parties, such as carriers and other service providers, will not be completely under enterprise control and, therefore, cannot always be fully trusted. Direct access to its services may be achievable only through the ECM integration layer services.	IaaS

Table 1. ECM Building Blocks for the Cloud

Figure 1 presents a reference architecture that demonstrates how these building blocks relate to one another in a cloud-based environment.

7 http://csrc.nist.gov/publications/nistpubs/800-28-ver2/SP800-28v2.pdf

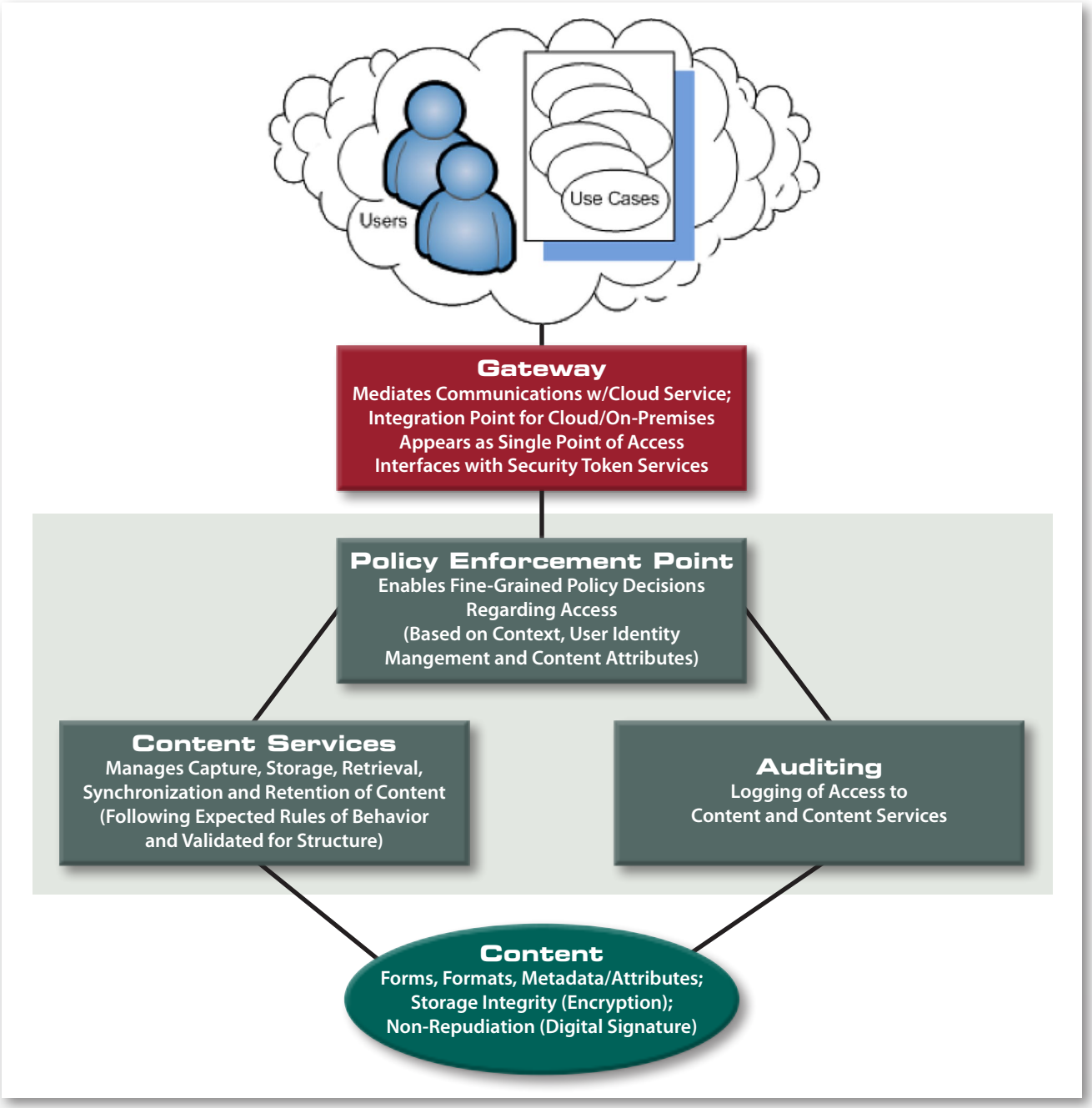

Figure 1. Content Management Reference Architecture for Mobile/Cloud Environments

The architecture depicts the content layer converging with the integration services and the infrastructure, bearing in mind that, in a cloud-enabled implementation, the physical layers are a given, if not irrelevant. Users and their use cases, based on actual scenarios, determine the context for how content is accessed, consumed and managed, whether from fixed workstations or mobile devices. Users access content services through a gateway, which mediates communication to and from cloud services, and which provides an integration point for cloud-based content with on-premises services and mobile devices. Users see this gateway as a single access point—perhaps as a page of the corporate intranet site—that to them is just another black box in the IT infrastructure.

21st Century Content Management: A Checklist

Enterprises must navigate a maze of decisions when implementing cloud-based content management for mobile users. Start by quantifying business needs, followed by assessing typical content usage in order to detect atypical content behaviors. Also, consider how to enable user expectations and demands, while ensuring that access and data encryption are seamless throughout the user experience. Monitoring access, usage and content sharing is a problem for organizations unused to coping with content that can't be stored in a file cabinet, and it may require specialist input during the adoption phase.

The following checklist should help enterprises navigate the set of decisions they face in implementing a strategy for cloud-based ECM. Many are decisions enterprises should have already faced when defining their management policies for on-premises content use.

Step 1: Objectives—Understand Your Business Needs, Processes and Requirements.

- ✔ Identify key content users within your enterprise, and target those who can describe existing needs, policies, processes and systems.
- ✔ Build a simple work plan and timeline, assigning resources as necessary to accomplish the work in a timely manner.
- ✔ Develop a questionnaire to capture relevant information from your targeted users consistently. Sample questions could include the following:
  - What are the use cases and workflows your content management capabilities need to address? Are these structured workflows, such as accounts receivable or accounts payable; *ad hoc* ones, such as working on a presentation; or both?
  - Do you need group collaboration on documents, presentations or analysis?
  - What sensitive content and applications are the mobile workforce accessing now and in the future?
  - Where is the content distributed (on-premises, mobile, cloud)?
  - What are the current and foreseeable future regulatory demands around content, including retention?
  - What are typical user roles? What are common access and sharing requirements for each user role? Where are users most likely to access content?
  - Are users aware of the risks of mixing personal and business data on their devices? Have you been able to enforce your mobile policies?
  - What are current user concerns related to usability, access to applications and content? What is the current authentication process? Can it be made easier?
- ✔ Document your use cases and extract the common features and/or rules around content management. These may be simple rules such as "80 percent of our employees access SharePoint from mobile devices," or "Executives have broad access to resources X, Y and Z, regardless of their need to see the content."

Step 2: Assessment—Know Your Content.

Best practices dictate that you locate your data, map its usage, examine the potential risks and then build protection policies and controls around it. To do this, perform the following:

- ✔ Develop a data map and inventory of content and content usage, including where content flows and to what devices.
- ✔ Review content policies, schemas for access, content and governance.
- ✔ Determine both the types and formats of content you are currently managing, as well as what content you seek to manage.
- ✔ Have the necessary associated metadata to enable enforcement of privacy and security policy rules via that metadata.

Step 3: Requirements—Match Technology to the Need.

Match your technical options to your functional needs. For example, if cloud-based collaboration over employee-owned devices is a requirement, would a cloud-based service or an on-premises content-centric platform be more secure?

- ✔ Ask the nuts-and-bolts questions that will shape your requirements, such as the following:
  - What enterprise content needs to be accessed, and what technologies will be used (e.g., social networking, cloud or on-premises collaboration)?
  - What security features do a given device and its access scheme support? (Options may include remote wipe, two-factor authentication, self-service password reset, device encryption, application sandboxing and automated OS patch management.)
  - Are existing data classification policies enforceable on the selected platforms?
  - What applications—both professional and personal—will be used?
  - What sensitive content is associated with those applications, and what are the associated rules and regulations for that content?
  - How can the organization achieve regulatory compliance?
  - How will the organization provision and revoke access?
  - How will the organization enable monitoring and logging capabilities?

- ✔ Organize requirements into broad categories or feature sets such as the following:
  - **Architecture.** If regulatory compliance is one of the biggest drivers, as indicated in the preliminary results of the 2012 SANS Application Security Survey (to be published in December 2012),[8] the architecture must support a level of monitoring that ensures sensitive content is not leaking through mobile devices or the cloud.
  - **Authentication and access.** Multifactor authentication, secure connectivity, and other controls must apply to the growing segment of BYOD workers as much as they do to users of company-issued devices. What approaches can make access easier and more consistent for users and their applications, whether the data lives in the cloud, on-premises, both or either?
  - **Support for business rules.** Rules around content management should take into consideration factors such as time of day and device location. What full access to content would be granted if the device were in, say, Cambodia, trying to access content at 3 a.m. local time?
- ✔ Identify current gaps in protections. Look to the security management tools you have available—Data Loss Prevention (DLP), firewalls, Intrusion Detection Systems (IDS), MDM—to identify potential gaps in configuration that could result in vulnerabilities. If you found gaps, it's possible someone outside the organization has done the same. So, be sure to close them as part of your overall security upgrade to support mobile/cloud content management.

Step 4: Implementation—Identify Tools and Techniques that Support Security Requirements.

- ✔ Identify tools and techniques specific to each ECM layer, using the requirements from Step 3 as your guide.
- ✔ Conduct a risk analysis to maintain a cost-effective balance between administrative and technical controls. For example, an MDM implementation might involve putting a software agent on employee-owned devices, so the organization would need to incorporate employee consent to monitoring as part of the internal service agreement.

8 The survey is expected to be available on December 15, 2012, at: www.sans.org/reading_room/analysts_program

Table 2 associates potential techniques and technologies, with the ECM building blocks described previously. Not all these technologies may be available for a mobile or cloud ECM solution, but consider those that are important to the organization and build them into a technology roadmap as discussed in Step 5.

Building Block	Techniques (e.g., Policies)	Technologies (e.g., Tools)
Content	Metadata standards	Policy editors
	Data maps	Digital rights
	Data classification policy	Encryption (for data at rest)
Integration and Management	Identify proofing procedures	Digital signature (for non-repudiation)
	Acceptable use policy	Data Loss Prevention (DLP)
	Retention policy and procedures	Identity Management Systems (IdM)
	Auditing policy and procedures	Geo-fencing[9]
	Sanction policy	Record locator services
Infrastructure and Mechanics	Performance and capacity plans	Auditing
	Quota management	Gateway services / Single sign-on
	Network design	Cloud-based IdM
		Database management
		MDM/MAM
		Proof of storage
		SIEM

Table 2: ECM Building Blocks, Techniques and Technologies

9 Geo-fencing is the process of setting and enforcing a virtual perimeter around data based on access location, usually accomplished through SIEM-related technologies.

Step 5: Future Proofing—Build a Technology Roadmap for ECM.

Outline a strategy based on today's user needs and consider future requirements as adoption of mobile devices continues to grow.

- Try to identify tools based on industry standards, and align techniques with accepted best practices.
- Work with vendors that have established a roadmap that guides their product development, growth and change in concert with market trends and direction. Continue to involve the business units, users, and vendors that were part of the initial needs and content analysis. Base your roadmap on a two-year event horizon, as suggested in a Gartner research report published in September 2012.[10] (Conveniently, this period coincides with the customary term for major carriers' service contracts.)
- Include a risk review to help manage your organization's risk profile and any threats introduced by these changes, especially for any new use case involving content and mobile users.
- Finally, don't forget to involve your stakeholders in communicating changes to your roadmap.

10 Redman, P. "The Cloud Is Expanding to Address the Challenges of the Mobile Enterprise," Gartner Research Note, published Sept. 19, 2012.

Conclusion

To meet the demand for mobility in an increasingly cloud-based working environment, business is driving toward a security model that is content-centric and context-aware. Traditional protections need to scale virtually as well as physically, while new and innovative defenses need to be developed and enabled.

Policies that provide rules of use around sensitive content and how it is managed already exist; they simply need to be updated for a mobile business world. The old adage, "Don't put in policy what you can't enforce," is even truer in today's distributed computing environment with employee-owned devices. The majority of respondents to recent SANS surveys on mobile devices and BYOD agree that data protections are important, but few are implementing the basics, such as encryption, let alone implementing the more sophisticated security controls, such as MDM, that are necessary for today's world of mobile and cloud computing.

Secure content delivery can be achieved. The first step is understanding the challenges of the mobile and cloud computing models. Policies and practices around content must carry with them the metadata or enablers for protection and implement policies and processes that establish trust in an environment no longer based on absolutes. Access and context around access become critical in this environment, as well as protecting content from potentially hostile devices. Visibility into cloud-based content usage and compliance is also a consideration when sensitive data is involved.

By taking the right steps to secure their infrastructures and applications, as well as content, organizations can safely embrace the mobility and cloud explosion.

About the Author

Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls "policy, process, platforms, pipes AND people." Most recently, she's been involved with HIPAA security issues in the health and human services industry, with clients from federal agencies (DoD and VA), municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system lifecycle as well as its relation to many of the issues faced by a modern society dependent on automation—privacy, identity theft, exposure to fraud and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold) and GCIH (Gold), and the GHSC.

SANS would like to thank its sponsor:

Last Updated: May 26th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Thailand 2017	Bangkok, TH	Jun 12, 2017 - Jun 30, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced