

Protecting Sensitive Data in Transit



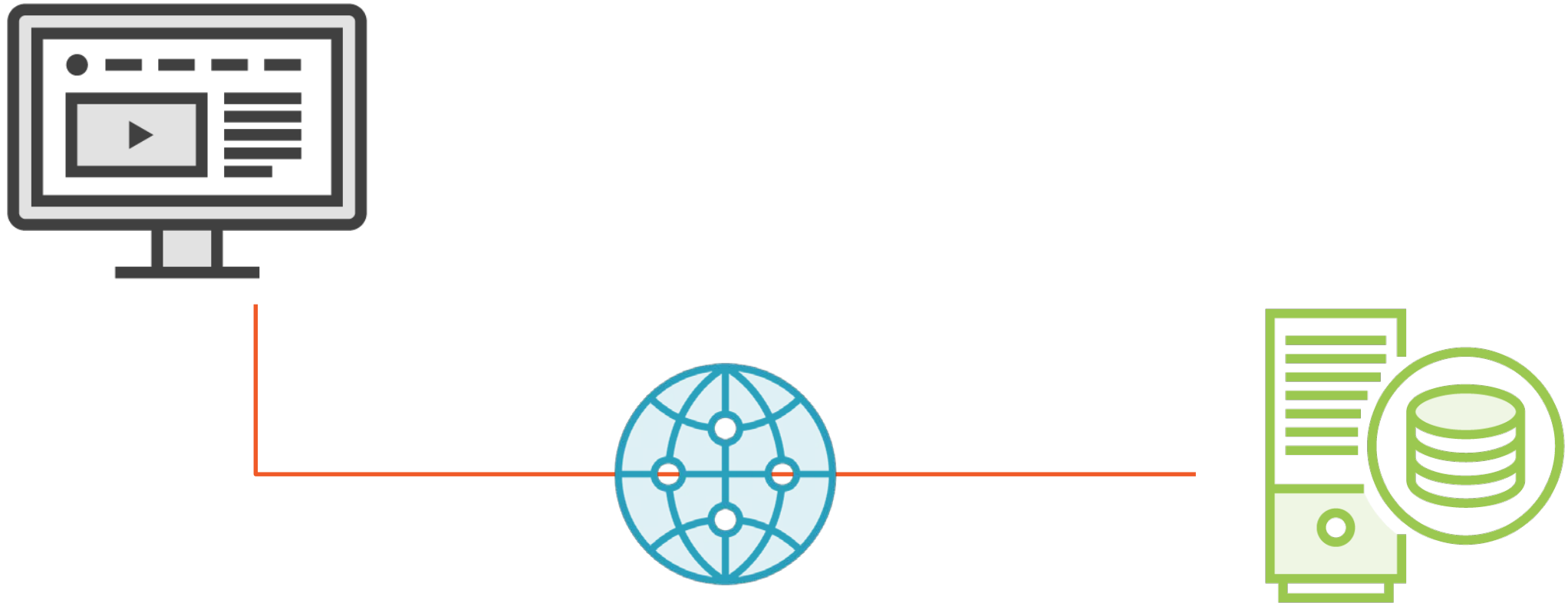
Russ Thomas

DATABASE MANAGER

@sqljudo www.sqljudo.com



SQL Server Data in Transit



Network Conversations

- All Traffic
- Other Traffic
- IPv4 (10.111.111.111 - 10.0.0.1) C

Display Filter

Apply Remove History Load Filter

Save Filter Clear Text

Frame Summary

Find

Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Source	Destination	Protocol Name	Description
1	6:18:37 PM 4/27/2009	0.0000000	10.111.111.111	10.0.0.1	TDS	TDS:SQLBatch, Version = 7.300000(No version information available, using the default version), SPID
2	6:18:37 PM 4/27/2009	0.0003430	10.0.0.1	10.111.111.111	TDS	TDS:Response, Version = 7.300000(No version information available, using the default version), SPID
3	6:18:37 PM 4/27/2009	0.0306380	10.111.111.111	10.0.0.1	TDS	TDS:RPCRequest, Version = 7.300000(No version information available, using the default version), SP
4	6:18:38 PM 4/27/2009	0.1410290	10.0.0.1	10.111.111.111	TDS	TDS:Response, Version = 7.300000(No version information available, using the default version), SPID

Frame Details

Frame: Number = 3, Captured Frame Length = 358, MediaType = ETHER
Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-0C-29
IPv4: Src = 10.111.111.111, Dest = 10.0.0.1, Next Protocol = TCP,
Tcp: Flags=...AP..., SrcPort=1111, DstPort=1433, PayloadLen=292,
Tds: RPCRequest, Version = 7.300000(No version information availa





Hex Details

Decode As	Width	Prot Off: 0 (0x00)	Frame Off: 0 (0x00)	Sel Bytes: 0
0079	34 00 40 00 50 00 30 00 20 00 6E 4.	@.P.O.	.n	
0084	00 76 00 61 00 72 00 63 00 68 00	.v.a.r.c.h.		
008F	61 00 72 00 28 00 34 00 30 00 30	a.r.(.4.0.0		
009A	00 30 00 29 00 2C 00 40 00 50 00	.0.)..@.P.		
00A5	31 00 20 00 69 00 6E 00 74 00 00	1..i.n.t..		
00B0	00 E7 40 1F 09 04 D0 00 34 90 00	.ç@...Đ.4		
00BB	73 00 65 00 6C 00 65 00 63 00 74	s.e.l.e.c.t		
00C6	00 20 00 2A 00 20 00 66 00 72 00	.*. .f.r.		
00D1	6F 00 6D 00 20 00 74 00 65 00 73	o.m. .t.e.s		
00DC	00 74 00 5F 00 74 00 61 00 62 00	.t._.t.a.b.		
00E7	6C 00 65 00 5F 00 31 00 20 00 77	l.e._.l. .w		
00F2	00 68 00 65 00 72 00 65 00 20 00	.h.e.r.e. .		
00FD	6E 00 61 00 6D 00 65 00 20 00 3D	n.a.m.e. .		
0108	00 20 00 40 00 50 00 30 00 20 00	.@.P.O. .		
0113	61 00 6E 00 64 00 20 00 69 00 64	a.n.d. .i.d		
011E	00 20 00 3D 00 20 00 40 00 50 00	. .=. .@.P.		
0129	31 00 20 00 20 00 20 00 20 00 20	1. . . .		

Frame Comments

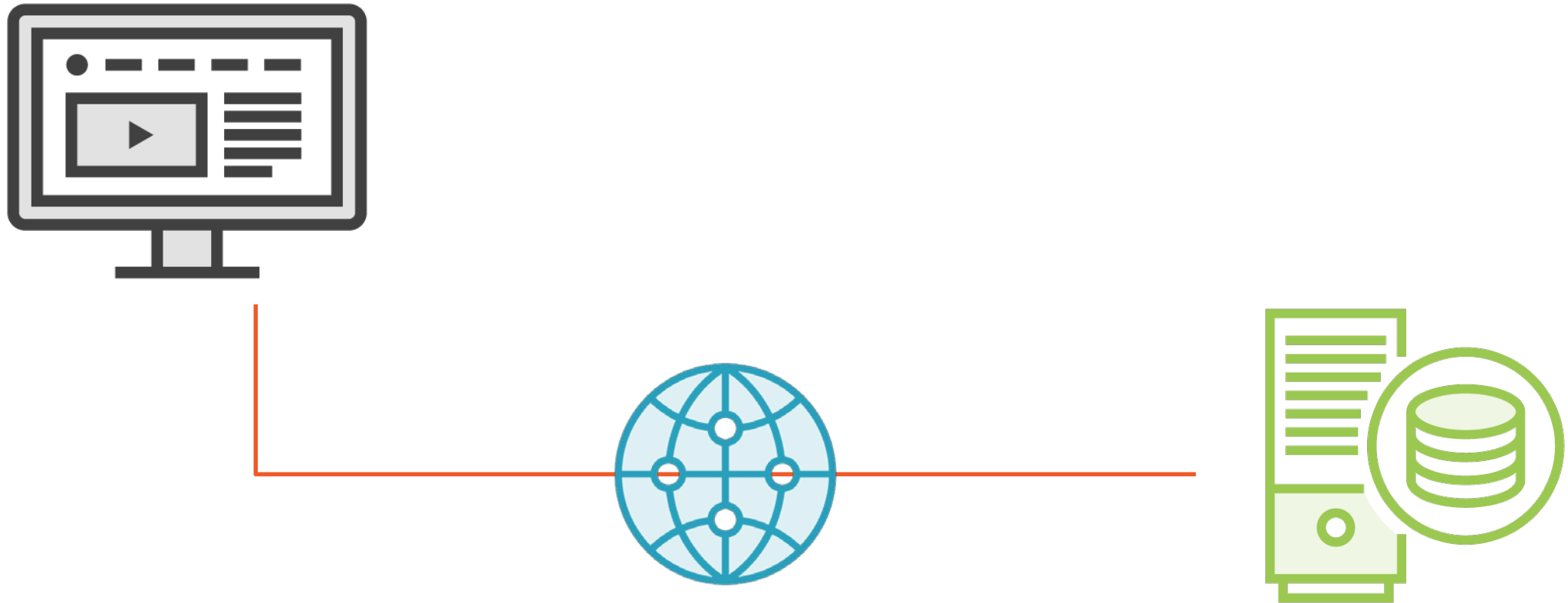
Hex Details

SQL Server Data in Transit

Hex Details													X
 Decode As	 Width	Prot Off: 0 (0x00)				Frame Off: 0 (0x00)				Sel Bytes: 0			
0079	34	00	40	00	50	00	30	00	20	00	6E	4. @. P. 0. . n	^
0084	00	76	00	61	00	72	00	63	00	68	00	. v. a. r. c. h.	
008F	61	00	72	00	28	00	34	00	30	00	30	a. r. (. 4. 0. 0	
009A	00	30	00	29	00	2C	00	40	00	50	00	. 0.) . , . @. P.	
00A5	31	00	20	00	69	00	6E	00	74	00	00	1. . i. n. t. .	
00B0	00	E7	40	1F	09	04	D0	00	34	90	00	. ç@ . . . ð. 4 .	
00BB	73	00	65	00	6C	00	65	00	63	00	74	s. e. l. e. c. t	
00C6	00	20	00	2A	00	20	00	66	00	72	00	. . * . . f. r.	
00D1	6F	00	6D	00	20	00	74	00	65	00	73	o. m. . t. e. s	
00DC	00	74	00	5F	00	74	00	61	00	62	00	. t. _ . t. a. b.	
00E7	6C	00	65	00	5F	00	31	00	20	00	77	l. e. _ . 1. . w	
00F2	00	68	00	65	00	72	00	65	00	20	00	. h. e. r. e. .	
00FD	6E	00	61	00	6D	00	65	00	20	00	3D	n. a. m. e. . =	
0108	00	20	00	40	00	50	00	30	00	20	00	. . @. P. 0. .	
0113	61	00	6E	00	64	00	20	00	69	00	64	a. n. d. . i. d	
011E	00	20	00	3D	00	20	00	40	00	50	00	. . =. . @. P.	
0129	31	00	20	00	20	00	20	00	20	00	20	1.	▼
 Frame Comments													 Hex Details
Displayed: 38				Captured: 38				Focused: 3				Selected: 1	



SQL Server Data in Transit



Module 5



Encrypting data at the application

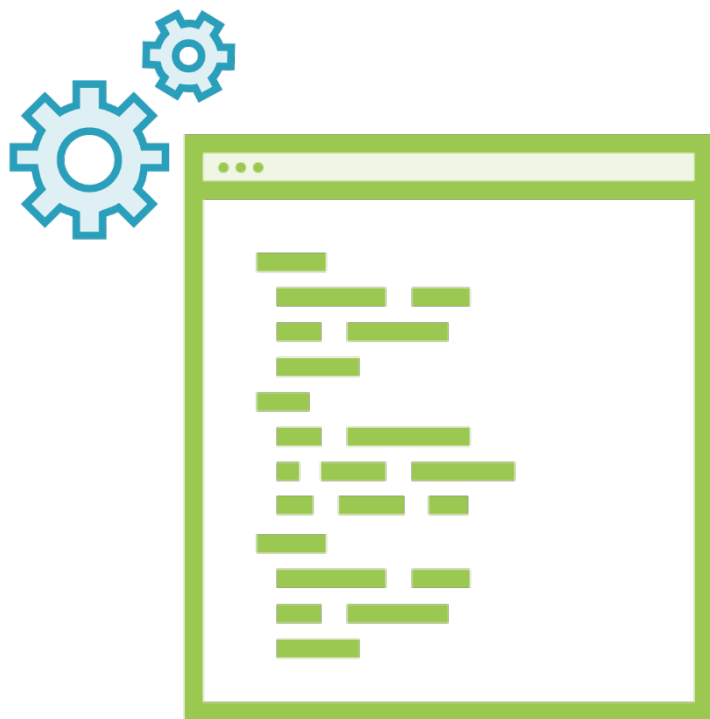
SSL encryption

- Self Signed Certificates
- Verified Certificates

SQL Server 2016 Always Encrypted



Encrypting at the Application





Developer responsibilities tend to pile up

Security typically requires more effort than a single sprint item or after thought

A team can be very effective if given the bandwidth and resources to succeed



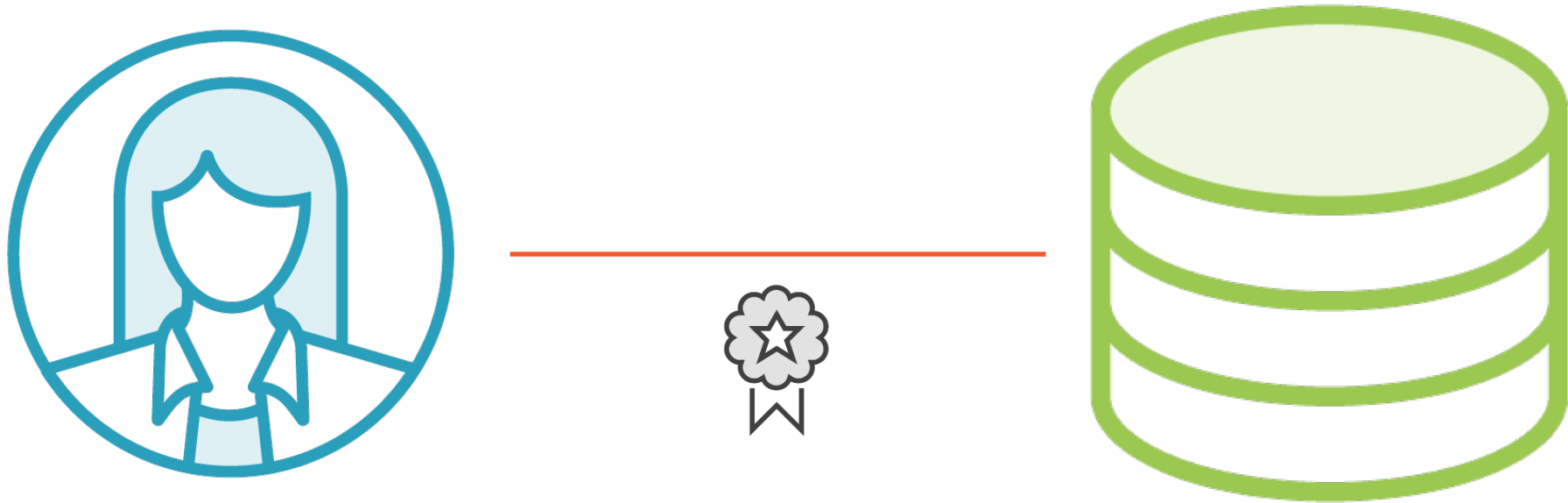
Single Entry Point for Sensitive Data



Requiring SSL Connections to SQL Server



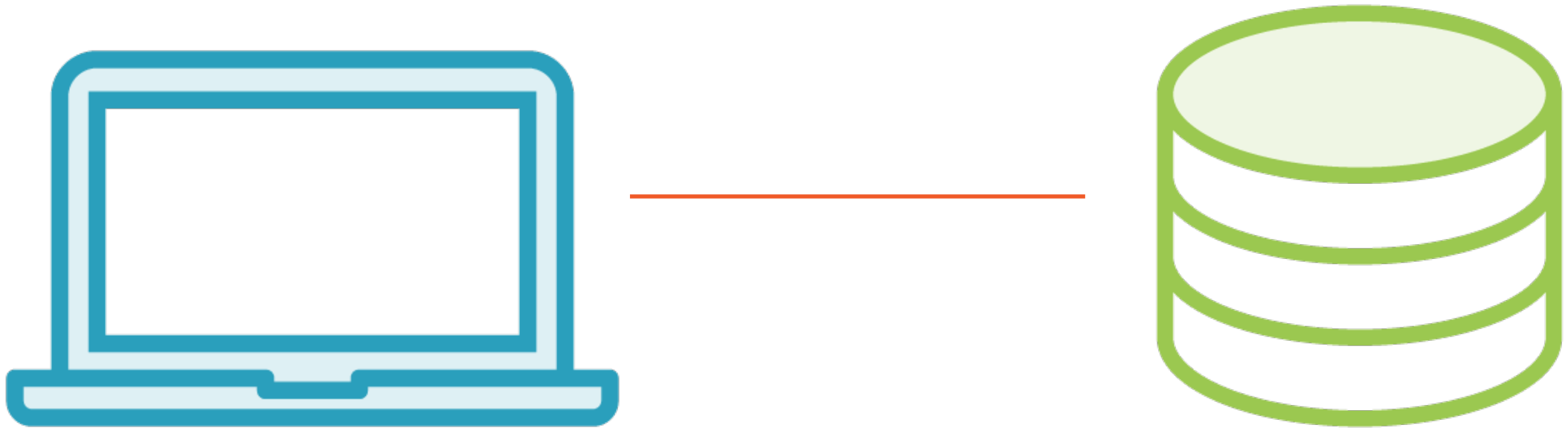
Encryption During Login



Requiring SSL Connections to SQL Server



SQL Session Encryption





Basics of Certificate Management

- <http://bit.ly/2d4a46l>

Windows Server Certificate Services

2008 / 2008 R2

- <http://bit.ly/2cqVvHn>

2012 / 2014

- <http://bit.ly/2cYfPnY>



Requirement Summary

- Trusted, current, valid
- Certificate for server authentication (supports **Enhanced Key Usage**)
- Identify FQDN of SQL Server

SQL Server SSL Full Documentation

- <http://bit.ly/2cqxxRp>

SQL Server Session Encryption With SSL

What it does

Protects Network Packets in Transit

What it doesn't do

Protect Data at Rest on SQL Server

Protect Data in Memory on SQL Server

Protect Data Once it Reaches the Client



Up Next



Real World Demo

**Protecting Data in Transit with
SQL Server 2016 Always Encrypted**

