

Thomas Swafford

Qualifications

Security:

- Firewalls, IDS/IPS (multiple vendors)
- Symantec/McAfee/Palo Alto Cortex /Carbon Black/CrowdStrike
- Web and DNS Security / Filtering
- Baseline security analysis/Vulnerability Assessment
- SIEM Solutions: Splunk/Syslog/Cortex
- MFA/2FA – multiple solutions

Server Applications:

- Microsoft Active Directory
- Novell NDS 6.x/8.5, NDS for NT
- Exchange 5.x/2000-2019, SMTP,POP3
- Microsoft SQL Server 7.0, 2000, 2005,2008/2012/2014/2019
- IIS 4 - 10, HTTP, FTP, SSL
- Backup Exec / ArcServe / BrightStor
- VMWare ESX, Server, Workstation
- Microsoft Virtual Server / Hyper-V
- Citrix Metaframe / XenApp

Operating Systems and Servers:

- Windows NT/2000-2022 Server
- Windows 3.x/9x/NT/2000/XP/7/8/10/11
- Linux: Red Hat, Ubuntu
- Novell Netware 3.x/4.x/5.x

Networking:

- TCP/IP, IPX, NetBEUI
- DHCP, DNS, WINS, NAT
- RAS, Client VPN, Site-to-Site VPN
- Cisco Routers, Switches, Wireless
- Ethernet and Fiber Optic Cabling

Applications:

- Office 4.x/95/97/2000-2021/365

Hardware:

- SCSI/SAS and RAID 0/1/5/10
- Fiber Channel, SAN, iSCSI
- Tape Backup: LTO/DAT/DLT/Library
- HP Compaq / IBM-Lenovo / Dell

Cloud:

- AWS/Azure/Microsoft 365

Education / Certifications

Degree	Bachelor of Science in Business Administration Concentration: Information Technology Colorado Technical University Graduate - GPA: 3.85
CISSP	Certified Information Systems Security Professional (ISC2)
CISM	Certified Information Security Manager (ISACA)
CLF-C01	AWS Cloud Practitioner
SAA-C03	AWS Solutions Architect Associate
AZ-900	Microsoft Certified: Azure Fundamentals
MCSE	Microsoft Certified Systems Engineer 4.0, 2000 and 2003
MCSA	Microsoft Certified Systems Administrator 2000 and 2003
CNE	Certified Novell Engineer Netware 5
CNA	Certified Novell Administrator 4.11 and 5.0
CCNA	Cisco Certified Network Associate (expired)
A+	A+ Certification
Network+	Network+ Certification
CFA-IF	CFA Investment Foundations
CCSK	Certificate of Cloud Security Knowledge V4

Career Experience

1/21 - Present	<u>Resolution Life US</u>	Atlanta, GA
	Head of Security Operations	1/21 – Present Permanent
<ul style="list-style-type: none">• Responsible for overseeing design, architecture and engineering of full greenfield platform and program buildout of all security capabilities with cloud-first, SaaS-first approach based upon AWS Compute, M365 Collaboration and SaaS capabilities. Successfully executed and oversaw projects to deploy 48+ new enterprise security capabilities at scale and transition to BAU operations.		

- Oversee and manage Identity Management Platform Engineering/Operations: Active Directory/ Azure AD/EntraID, Okta, BeyondTrust, LastPass, MFA Everywhere.
- Oversee and manage Security Platform Operations: Splunk Cloud, Proofpoint Email Security, Palo Alto Networks NGFW, Prisma Access, GlobalProtect VPN, Data Security with M365 Defender and Purview.
- Oversee and Manage SOC and Incident Response operations.

6/15 – 12/20

Voya Financial

Atlanta, GA

Reorganized from Voya Investment Management in June 2015

AVP, IT Security

3/20 – 12/20

Permanent

IT Security Director

1/17 – 3/20

Permanent

- Responsible for managing the Security Engineering and Platform Operations team overseeing platform tooling covering Security Monitoring (Splunk, Syslog, Guardium), Endpoint Security (Symantec Endpoint, Symantec DLP, Bit9, Encase, Tanium) and eDiscovery/Forensics (Relativity). Manage a team of up to 10 FTE plus up to 40 managed service provider staff at various points during tenure.
- January 2019- Added responsibility for managing Cloud Security Engineering function for various cloud related projects along with Azure and AWS.
- Managed Identity Management Platform Engineering/Operations (OIM/OIA, Cyber-Ark, NPUM, NePiS, ESSO) from 1/2017 – 3/2019.
- Helped lead the effort to reorganize manage security services from one provider to another as well as restructuring internal support and engineering in late 2018.
- Supported effort to execute outsourcing of operations and maintenance of security platforms to outsourcing provider in late 2017.
- Successfully executed and oversaw projects to replace multiple disparate solutions with unified enterprise applications across multiple IT organizations: zScaler for Web Security and Exchange Online Protection of Office 365 for eMail security.
- Acted as lead for departmental participation and execution of data center migration and various pre and post migration activities.

AVP, Information Security Officer

6/15 – 12/16

Permanent

- Responsible for managing the information security programs including security operations monitoring, CIRT response, patch/vulnerability management, and technical implementation, enforcement and compliance validation of IT security related internal policies and external regulations for the Voya Investment Management business unit. Manage and coordinate the activities of internal and outsourced security operations team and various information security related systems, applications and technology initiatives from design through implementation and support.
- Execute and oversee project to consolidate and integrate disparate business unit IT Security staff, technologies and processes into the broader Voya Financial IT Security program.

4/07 – 6/15

Voya Investment Management

Atlanta, GA

Formerly ING Investment Management – Rebranded May 2014

AVP, Information Security Officer

4/14 – 6/15

Permanent

Senior IT Security Analyst

4/12 – 4/14

Permanent

Chief IT Security Analyst

4/10 – 4/12

Permanent

Senior IT Security Analyst

4/07 – 4/10

Permanent

- Responsible for managing and executing the information security programs including security operations monitoring, CIRT response, patch/vulnerability management, and technical

implementation, enforcement and compliance validation of IT security related internal policies and external regulations. Manage and coordinate the activities of internal and outsourced security operations team and various information security related systems, applications and technology initiatives from design through implementation and support. Security systems include: nCircle/TripWire, Websense, Cyber-Ark, Guardium, IDS/IPS, and Endpoint security systems from Symantec and Lumension. Coordination with Risk Management, IT Management and IT Controls/Governance teams to ensure that audit and regulatory assurance activities are appropriately addressed..

10/06 – 4/07

ING Investment Management

Atlanta, GA

Senior Server Engineer

Contract

- Responsible for administration and troubleshooting of over 400 servers across three data centers and remote satellite offices. Work with Active Directory issues such as: logon failures, account lockouts, network connectivity, DNS and WINS name resolution, authentication problems, DFS links and replication issues, folder and printer permissioning, etc. Advanced troubleshooting of issues such as Active Directory and FRS/DFS replication issues, application memory leaks, Kerberos ticket size, etc. Server builds using HP Proliant hardware consisting of DL380, DL385 and DL580 models with local storage or connection to either an HP or NetApp SAN. Administration of a 26 server Citrix server farm and providing user support for various issues including profile and printing issues. Management of VMWare ESX farm with 10 ESX servers. Responsible for migration of Microsoft Virtual Servers and VMWare GSX servers to ESX platform. Responsible for Websense administration and maintenance.

8/03-2/04 8/04-10/06

Echostar Satellite, L.L.C.

Suwanee, GA

Regional Support Engineer

Permanent

- Responsible for Network, Server, Desktop, PBX support for the Southeast region of 26 locations, 71 servers and approx 1200 users. Management and administration of Enterprise Windows 2003 Active Directory infrastructure with over 30,000 objects. Daily phone and on-site support of end users covering any IT related issue including: application issues, hardware problems, operating system issues, network connectivity over Cisco switches and routers, Cisco VoIP and Lucent/Avaya phone system, etc. Provide IT related support for Production Lines and warehouse operations covering Unix connectivity, bar code scanners and label printer functionality. Application support includes: Office XP/2003, Windows 2000/XP/2003, Kronos, Clarify, HP Openview Service Desk, CSG, Siebel, Sharepoint, SMS 2003, Rumba, McAfee, iPass, Cisco VPN, Mappoint, Exchange 2003, Cisco Wireless, Client Firewalls, Enterprise PKI and Client Digital Certificates, Oracle Client, etc.

3/04 – 8/04

Microsoft Corporation

Charlotte, NC

Directory Services Support Engineer

Contract

- Provide support for all Microsoft customers with Active Directory issues, planning, design and disaster recovery. Also support all other distributed technologies such as DNS, WINS, Group Policies, Enterprise PKI, Digital Certificates, Terminal Services, File Replication Service/DFS, Exchange, SQL, etc. Provide server and client support for all issues such as: logon failures, account lockout, network connectivity, DNS and name resolution, authentication problems, etc. Number One Responsibility: Provide the absolute best support for all issues and 24/7 troubleshooting until problem resolution.

11/00 – 12/02

After Hours Formalwear

Norcross, GA

Network Administrator

Permanent

- Responsible for Nationwide Administration, support and troubleshooting of Netware 5.x and Windows NT 4.0/2000 Network Operating Systems on 28 IBM Servers. Design and Maintenance of Novell NDS8 and Microsoft Active Directory. Management and administration of Exchange 5.5 e-mail system with 600 users. Manage Tape Backups of all servers with Veritas Backup Exec using DLT Library and/or DAT Tape. Configure and manage corporate network security, Dial-In and VPN access utilizing Checkpoint Firewall, Shiva and RSA ACE/Server. Provide third level support for Help Desk Team. Design and implement Gigabit Ethernet in corporate network backbone. Configure, manage, and support Cisco 1600/1720/2600/3600 Routers and 3500 series switches as well as Bay and 3Com Routers, Switches and Hubs. Support large T1/Frame Relay/ISDN WAN.

Support AS/400 clients and connectivity troubleshooting. Develop and implement desktop imaging procedures. Develop and implement immediate solutions for common server and LAN/WAN problems: low disk space, user permissions, file restores, TCP/IP address and/or Name conflicts, Troubleshooting LAN/WAN Backbone connectivity and trouble reporting, User Lockout, Server Software/Hardware failures, etc. Develop and test Disaster Recovery procedures for network servers including recovery from total network destruction. Provide 24/7 On-Call Support.

6/97 – 9/00 **Business Equipment Center Of Atl** Atlanta, GA
Systems Engineer / Field Engineer Permanent – Career Growth

- Both In-house and On-Customer-Site installation, administration, support and troubleshooting of Novell Netware 3.x/ 4.x/5.0 and Windows NT 4.0, Windows 2000 Server Network Operating Systems. Supporting Workstations and printing under Novell and Windows NT Server Networks. Hardware support, troubleshooting, upgrading and consultation on Servers and workstations. Support Cisco and 3Com Routers and multiple T1/Frame Relay/ISDN WANs. Software support, troubleshooting, upgrading, and consultation covering Windows 3.x, Windows 95, Windows 98, Windows NT 4.0 and Windows 2000 Server / Workstation, Novell Netware 3.x/4.x/5.0, Microsoft Office 95/97/2000, WordPerfect 5.1-8.0, and various other software packages. 24/7 On Call

8/99 - Present **Commodity Marketing Company** Alpharetta, GA
Network/IT Consultant Part Time - Contract

- Responsible for all IT Operations. Design and implement multi-server Windows 2000 Active Directory / Exchange 2000 / SQL 2000 environment based on Dell hardware to replace Netware 4.11 server. Since upgraded to Windows 2003 Active Directory / Exchange 2003, then to Windows 2008 Active Directory / Exchange 2010 and now Windows 2016 Active Directory / Exchange 2016 on HP DL380p Gen8 Hardware. Redeploy all workstations with HP EliteDesk hardware and Windows 7 / Office 2010. Design and implement TMG Firewall/VPN solution with Client-to-Site and Site-to-Site 128bit VPNs. Move all web, mail and ftp servers in-house. Provide on-call support for all network related issues. Design and implement disaster recovery backup plan.

References

- | | |
|----------------------------------|--|
| Edmond Mack
(860) 573-1129 | - VP, IT Security Engineering and Operations at Voya Financial
- 1 Orange Way, Windsor, CT 06095 |
| Ray Rascher
(770) 690-5963 | - SVP, Head of Technology Management at Voya Investment Management
- 5780 Powers Ferry Road NW, Atlanta, GA 30327 |
| Cindy Fowler
(508) 930-5207 | - VP, IT Application Development and Support at Voya Financial
- 1 Orange Way, Windsor, CT 06095 |
| Janet Bonds
(404) 542-9890 | - Former Head of Security and Controls at Voya Investment Management |
| Vince Connolly
(678) 566-7820 | - Owner/President of Commodity Marketing Company.
- 8480 Holcomb Bridge Rd, Alpharetta, GA 30022 |