solarwinds government

Leveraging Network, Systems, and Log Monitoring Tools to Help Improve Security and Compliance

CyberUSA Conference Presentation

January 16, 2020

This presentation contains forward-looking statements regarding future product plans and development efforts. SolarWinds considers various features and functionality prior to any final generally available release. Information in this presentation regarding future features and functionality is not and should not be interpreted as a commitment from SolarWinds that it will deliver any specific feature or functionality in the future or, if it delivers such feature or functionality, any time frame when that feature or functionality will be delivered. All information is based upon current product interests, and product plans and priorities can change at any time. SolarWinds undertakes no obligation to update any forward-looking statements regarding future product plans and development efforts if product plans or priorities change.

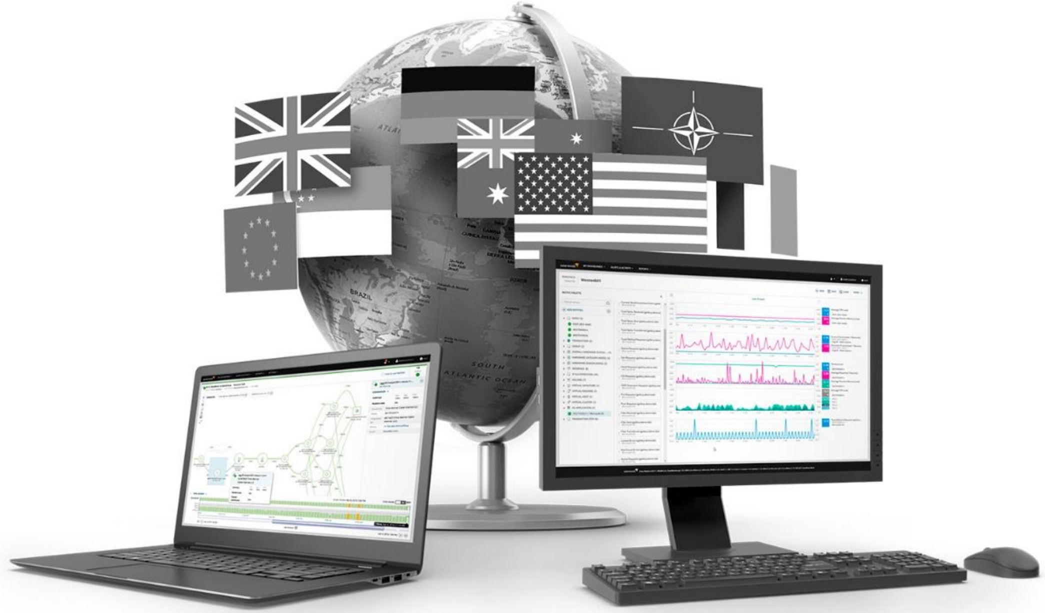
Speaker Introduction

Rich Roberts

Senior Federal Sales Engineer

richard.roberts@solarwinds.com

703.386.2650 (office)



© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Agenda

- IT compliance overview and challenges
- Improving security and compliance
- SolarWinds® solutions
- Demonstrations
- Resources
- Q&A

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Improving Security and Compliance

We can learn a lot from federal IT security compliance regulations:

They provide guidance for asset management and categorization

They provide frameworks for improving security, implementing security controls, and hardening systems

They provide guidance on encrypting data and establish privacy standards

Leverage controls and benchmarks from the Center for Internet Security (CIS).

Follow best practices for cybersecurity:

Discover and monitor infrastructure to discover potential threats

Leverage continuous monitoring to detect and mitigate suspicious activities

Patch systems/apps and configure networks to manage vulnerabilities

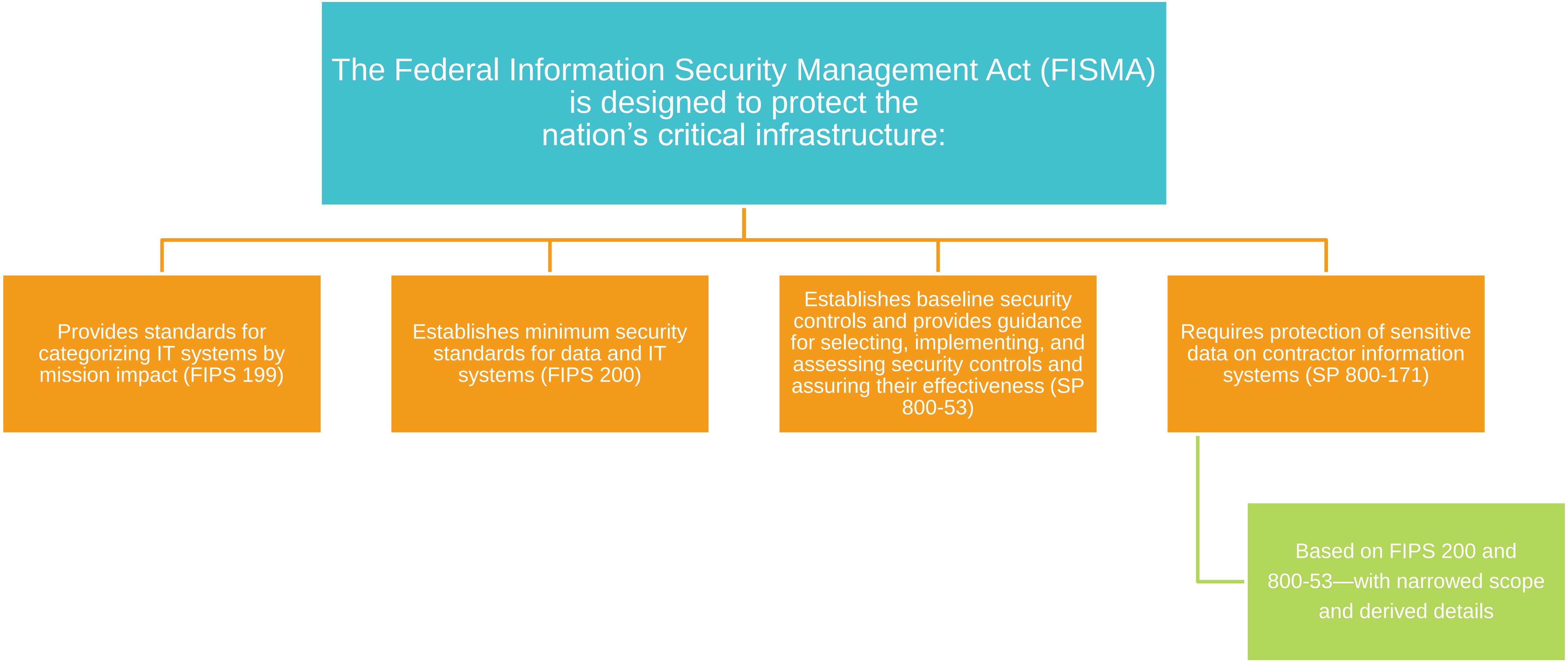
© 2020 SolarWinds Worldwide, LLC. All rights reserved.

IT Compliance Overview and CIS Controls

- Making Sense of Federal Regulations
  - FISMA
  - FIPS 199 and 200
  - RMF
  - DISA STIGs
  - HIPAA
  - PCI DSS
- CIS Controls® and CIS Benchmarks™ are global standards and recognized best practices for securing IT systems and data against the most pervasive attacks

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

FISMA Overview



The Federal Information Security Management Act (FISMA) is designed to protect the nation’s critical infrastructure:

Provides standards for categorizing IT systems by mission impact (FIPS 199)

Establishes minimum security standards for data and IT systems (FIPS 200)

Establishes baseline security controls and provides guidance for selecting, implementing, and assessing security controls and assuring their effectiveness (SP 800-53)

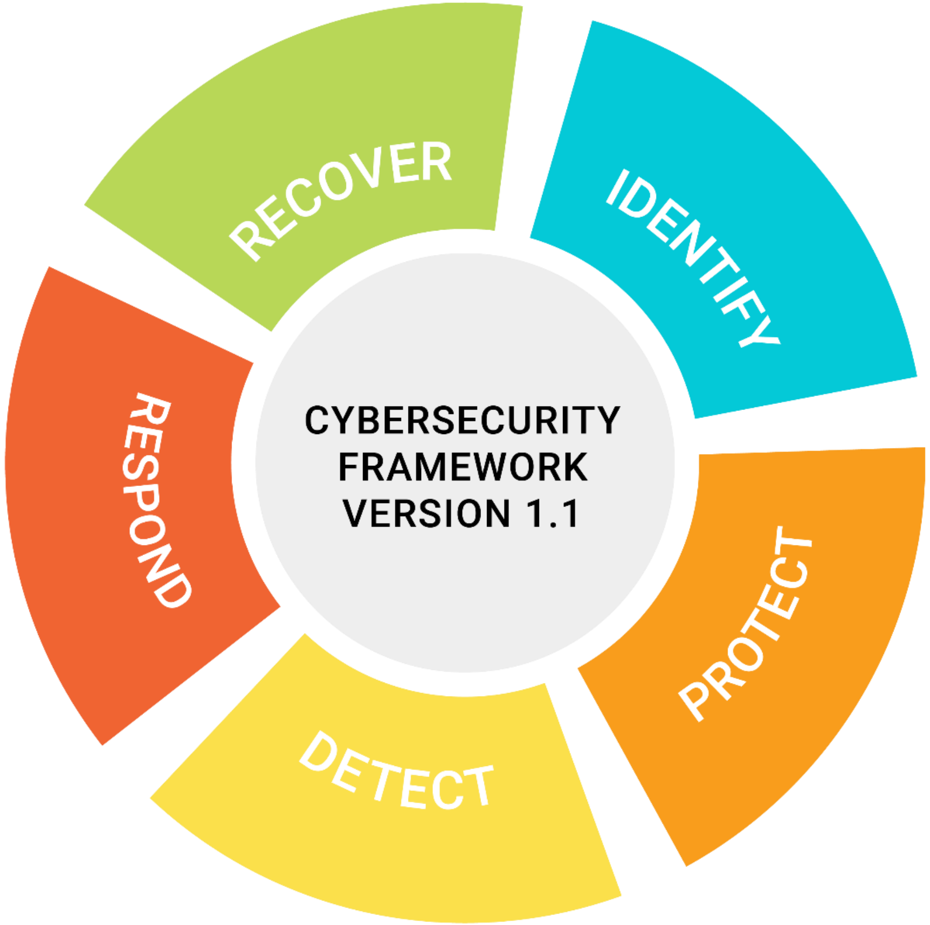
Requires protection of sensitive data on contractor information systems (SP 800-171)

Based on FIPS 200 and 800-53—with narrowed scope and derived details

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

NIST Cybersecurity Framework

Recovery planning
Learning and improvement
System restoration
Communications



Asset management
Business environment
Governance
Risk assessment
Risk-management strategy

Response planning
Incident response
Communications
Analysis
Mitigations

Access control
Awareness training
Data and security protection
Processes and procedures
Patch management
Vulnerability assessment

Anomalies and events
Continuous security monitoring

"Framework Resources," NIST. https://www.nist.gov/image/framework-01png (Accessed March 2019)

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

FISMA Compliance Cyberintelligence Best Practices

- Maintain an inventory of IT systems
- Categorize data and systems according to risk level
- Maintain a system security plan
- Utilize security controls
- Conduct risk assessments
- Certification and accreditation
- Conduct continuous monitoring

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

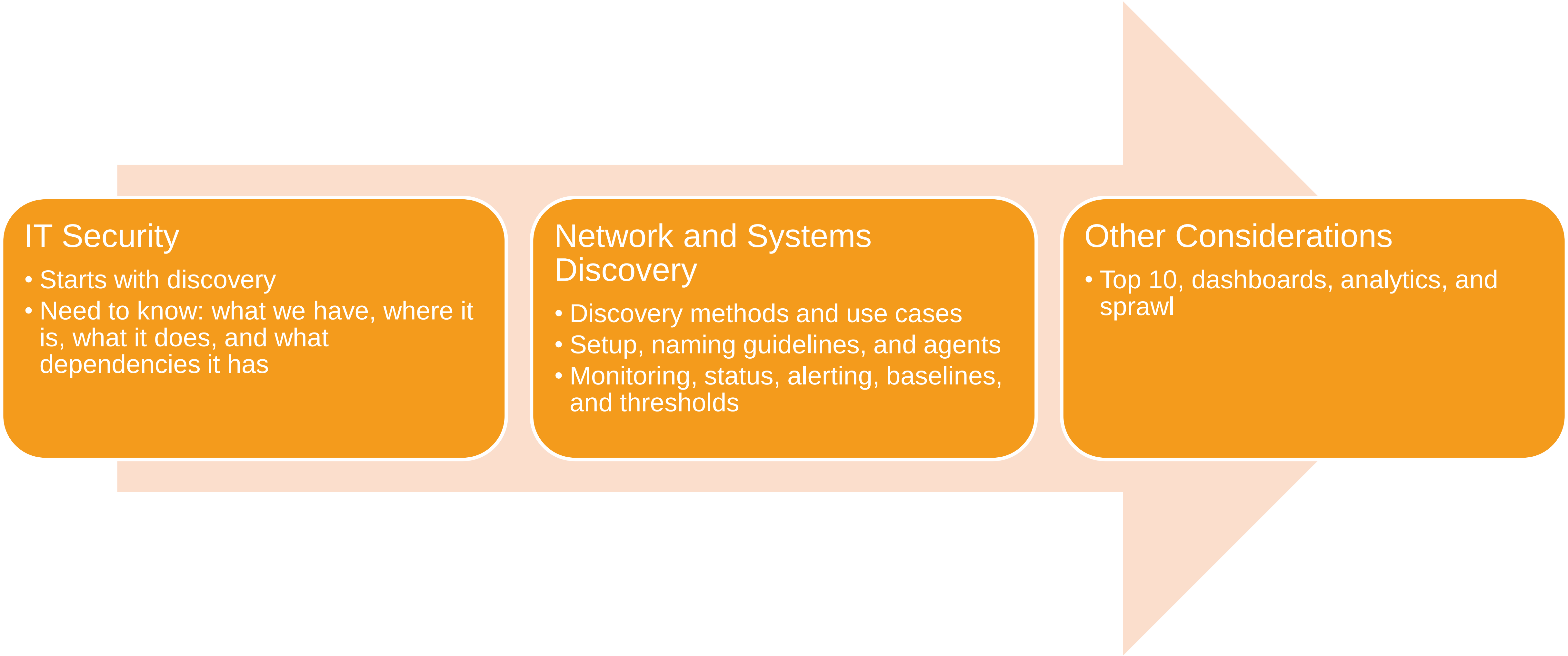
Improving Security and Compliance

Leveraging Network, Systems, and Log Monitoring Tools

- Get an inventory of your network
- Establish baselines and thresholds
- Monitor network and system performance
- Validate devices are correctly configured
- Validate system and application patches are applied across your system
- Monitor system logs
- Block or quarantine malicious and suspicious activity
- Proactively manage and monitor your access rights

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Asset Discovery



IT Security

- Starts with discovery
- Need to know: what we have, where it is, what it does, and what dependencies it has

Network and Systems Discovery

- Discovery methods and use cases
- Setup, naming guidelines, and agents
- Monitoring, status, alerting, baselines, and thresholds

Other Considerations

- Top 10, dashboards, analytics, and sprawl

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Gather Device, Utilization, and Dependency Data

Tools to Use

- Network performance
- Network traffic analysis
- Network configuration
- System management
- Device and IP address tracking
- Visualization

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Implement Strong Security Controls

- Agencies with evidence of strong IT controls are more likely to possess the hallmarks of strong infosec environments[1]
- Security controls are used to avoid, detect, counteract, or minimize security risks
    - General controls
    - Application controls
- Network monitoring and management tools
- Requires a deep level of visibility into your organization’s IT infrastructure

[1] “SolarWinds Federal Cybersecurity Survey Summary Report 2017,” Market Connections, Inc. https://www.solarwinds.com/resources/survey/solarwinds-federal-cybersecurity-survey-summary-report-2017 (Accessed December 2019).

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Continuous Monitoring

- Helps determine if an asset is achieving the anticipated target
- Deviation could mean a potential threat or attack
- Can help alert organizations to abnormal activities (e.g., failed logins or file transfers)
- Security information and event management (SIEM) tools detect suspicious activities

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

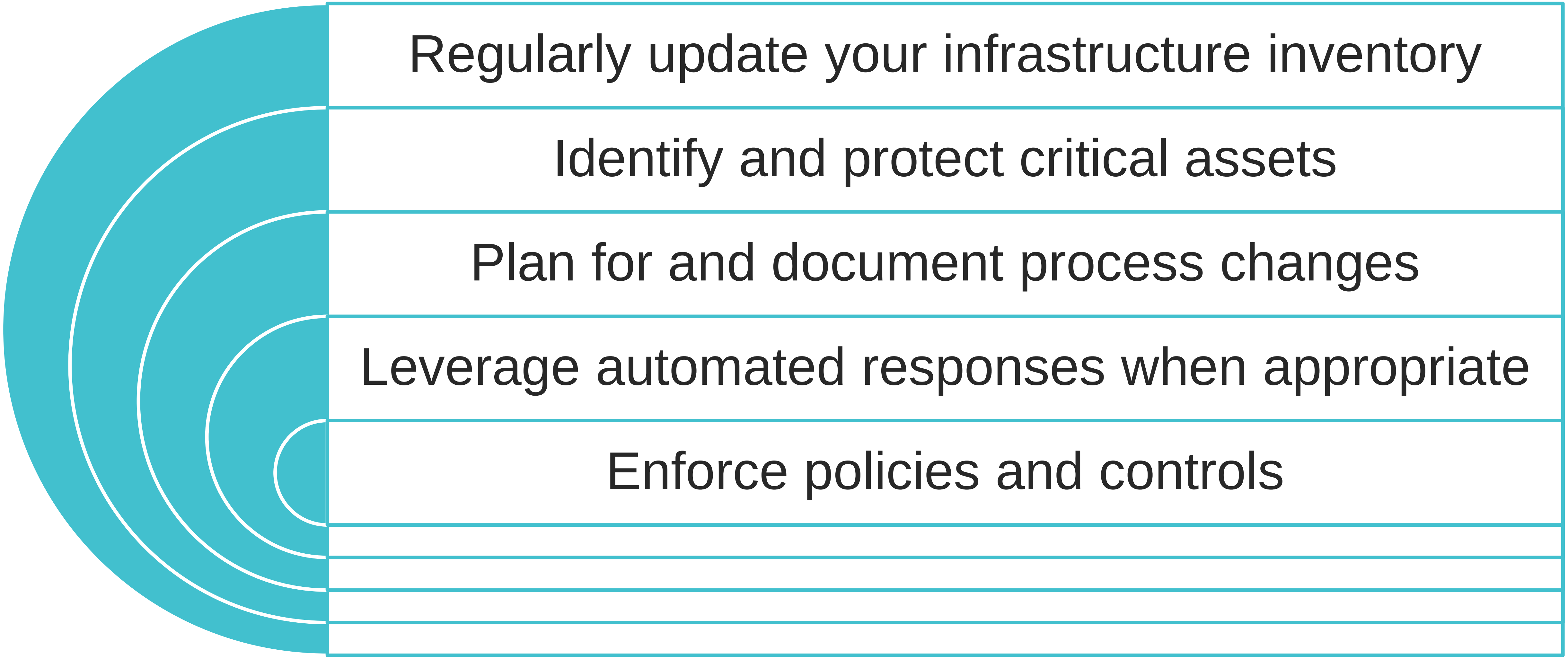
Managing Access Rights Across Your Infrastructure

- Identify, understand, and monitor high-risk access and accounts
- Visualize file server permissions
- Identify who has access
- Provision and deprovision accounts quickly and accurately
- Generate audit-ready reports

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Additional Steps to Improve Your Security Posture

And Help Protect Against Ransomware Attacks



Regularly update your infrastructure inventory

Identify and protect critical assets

Plan for and document process changes

Leverage automated responses when appropriate

Enforce policies and controls

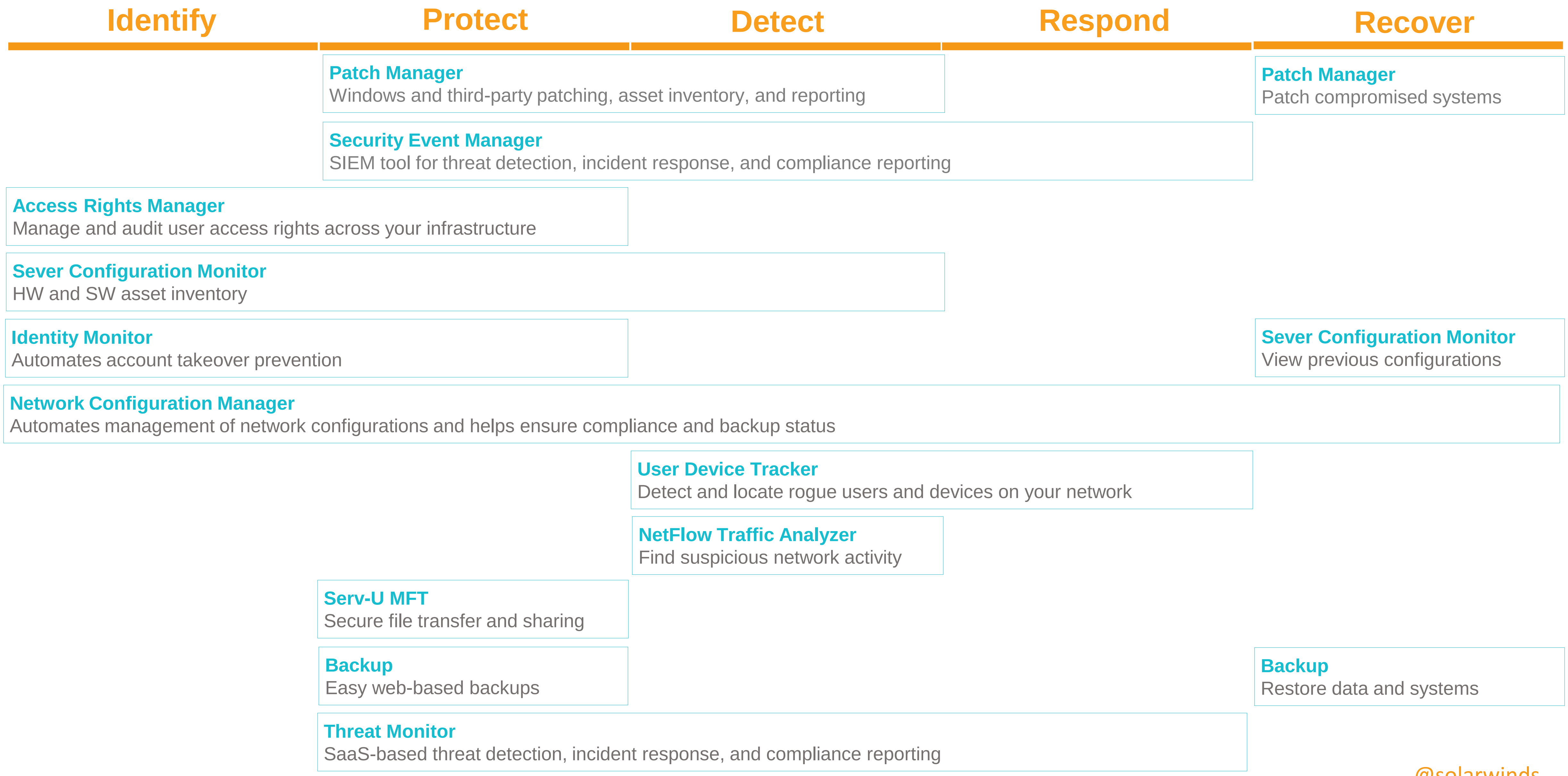
© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Build Security into Your Community

- Embed security practices and conversations about good security habits within your daily office environment
    - Gamify security training
    - Document and test your security policies
    - Conduct annual security awareness training
    - Leverage cybersecurity certification training (e.g., DOD 8570)
    - Document security incident reporting procedures (e.g., wallet cards, desk references, etc.)
    - Utilize multi-factor authentication

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

SolarWinds Security Products Overview



Identify | Protect | Detect | Respond | Recover

Patch Manager
Windows and third-party patching, asset inventory, and reporting

Patch Manager
Patch compromised systems

Security Event Manager
SIEM tool for threat detection, incident response, and compliance reporting

Access Rights Manager
Manage and audit user access rights across your infrastructure

Sever Configuration Monitor
HW and SW asset inventory

Identity Monitor
Automates account takeover prevention

Sever Configuration Monitor
View previous configurations

Network Configuration Manager
Automates management of network configurations and helps ensure compliance and backup status

User Device Tracker
Detect and locate rogue users and devices on your network

NetFlow Traffic Analyzer
Find suspicious network activity

Serv-U MFT
Secure file transfer and sharing

Backup
Easy web-based backups

Backup
Restore data and systems

Threat Monitor
SaaS-based threat detection, incident response, and compliance reporting

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

SolarWinds Compliance Features

Network Configuration Manager

- Inventory network device configurations, assess configurations for compliance, and automate change and configuration management
- Implement configuration of security controls and help ensure effectiveness
- Produce FISMA and DISA STIGs reports from configuration templates
- Produce audit documentation and reports

Security Event Manager

- Configure correlation rules to help assure effectiveness of security controls
- Conduct real-time and continuous monitoring of security controls
- Produce FISMA and DISA STIGs compliance reports from templates
- Support DISA STIGs requirements for configuration auditing, log analysis, and broader network security
- Track and report suspicious activities/attacks to provide auditing support

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

SolarWinds Compliance Features

Patch Manager

- Automate patching of Microsoft and third-party applications to help improve compliance
- Schedule patches for minimum downtime
- Inventory software and physical components per server or workstation

Network Performance Monitor

- Trend utilization for capacity planning
- Track multicast or firewall port discards
- Monitor network health and availability
- Identify protocol latency delays
- Produce audit documentation and reports

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

SolarWinds Compliance Features

Access Rights Manager

- Improve security posture and mitigate insider threats
- Demonstrate compliance
- Easily manage user permissions
- Enhance productivity

Server Configuration Monitor

- Track system and application changes, even if they were made offline
- Create configuration baselines and compare configurations over time
- View and report on hardware and software inventories

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Compliance Resources

- **Review** a blog on FISMA requirements: https://www.solarwinds.com/federal-government/solution/fisma-compliance-requirements
- **Review** a blog on how SolarWinds software can help with CIS controls: https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2017/08/18/solarwinds-and-cis-critical-security-controls
- **Review** a blog on how SolarWinds software can help with NIST FISMA/RMF compliance: https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2015/08/01/fisma-nist-800-53-compliance-with-solarwinds-products
- **Review** a blog on how SolarWinds software can help with DISA STIGS compliance: https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2011/09/07/disa-stig-compliance-with-log-event-manager
- **Watch** a federal security compliance video: http://www.solarwinds.com/resources/videos/solarwinds-federal-security-compliance.html
- **Download** a compliance white paper: https://go.solarwinds.com/Ultimate_Guide_Federal_IT_Compliance
- **Download** a continuous monitoring white paper: http://go.solarwinds.com/fedcyberWP?=70150000000Plgf

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Q&A

Come visit our table on the exhibit floor for more information or a demo.

Call government sales:

877.946.3751

Contact federal sales: federalsales@solarwinds.com

Contact state and local government sales: governmentsales@solarwinds.com

Contact education sales: educationsales@solarwinds.com

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

Contact Us

Let Us Know How We Can Help You

- Visit our THWACK government group: http://thwack.com/government
- Watch a short demo video: http://demo.solarwinds.com/sedemo/
- Download a free trial: http://www.solarwinds.com/downloads/
- Visit our government website: http://www.solarwinds.com/government
- Email SolarWinds federal government sales: federalsales@solarwinds.com
- Email SolarWinds state and local government sales: governmentsales@solarwinds.com
- Email SolarWinds education sales: educationsales@solarwinds.com
- Follow us on LinkedIn®: https://www.linkedin.com/company/solarwinds-government

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

SolarWinds at a Glance

Founded in 1999

More than 3,100 employees globally

Austin, TX headquarters
Herndon, VA, government office
30+ offices globally

#1 in network management[1]

#3 in systems management[2]

55+ IT management products

Growing security portfolio

Leader in remote monitoring and management

150,000+ registered members of THWACK®, our global IT community

300,000+ customers in 190 countries [3]

499 of Fortune 500®

Serving 22,000+ MSPs and 450,000+ organizations

Every branch of the DoD, and nearly every civilian and intelligence agency

1. IDC defined Network Management Software functional market, IDC's Worldwide Semiannual Software Tracker, April 2019.
2. Gartner, Market Share Analysis: ITOM: Performance Analysis Software, Worldwide, 2018. June 11, 2019. (AIOps/ITIM/Other Monitoring Tools Software Market). SolarWinds term, Systems Management, refers to the AIOps/ITIM/Other Monitoring Tools Software Market Taxonomy referenced in the Gartner report. All statements in this report attributable to Gartner represent SolarWinds interpretation of data, research opinion, or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation). The opinions expressed in Gartner publications are not representations of fact and are subject to change without notice.
3. Customers are defined as individuals or entities that have an active subscription for our subscription products or that have purchased one or more of our perpetual license products since our inception under a unique customer identification number. We may have multiple purchasers of our products within a single organization, each of which may be assigned a unique customer identification number and deemed a separate customer.

© 2020 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.