Market Connections
Research you can act on.

CONTINUOUS MONITORING

Managing the Unpredictable Human Element of Cybersecurity

A WHITE PAPER PRESENTED BY:

solarwinds

May 2014

PREPARED BY

MARKET CONNECTIONS, INC. 14555 AVION PARKWAY, SUITE 125 | CHANTILLY, VA 20151

T703.378.2318 | F703.378.2025 |WWW.MARKETCONNECTIONSINC.COM

CONTINUOUS MONITORING

Managing the Unpredictable Human Element of Cybersecurity

"If it weren't for the people in my agency, my IT would be more secure."
– All IT Ops/InfoSec professionals at every federal agency

Whether through human error or malicious intent, people are an unpredictable component of your agency's cybersecurity defense. Continuous monitoring tools can significantly reduce the threats people pose by putting checks and balances in place to keep your organization secure.

Executive Summary

IT Operations (IT Ops) and Information Security (InfoSec) teams at federal agencies face cyber threats every day—situations such as the hackers who breached Federal Reserve Bank servers, stealing and publishing personal information on more than 4,000 U.S. bank executives; the Federal Reserve staffer who accidentally emailed the Federal Open Market Committee's meeting minutes before their scheduled release, giving major financial companies access to potentially market-moving information; and the contractor who disclosed thousands of classified documents that revealed operational details of global surveillance programs run by the NSA and five other governments.

SolarWinds commissioned Market Connections to discover the primary cybersecurity threats facing federal agencies, the extent of cybersecurity readiness, and obstacles agencies face. The study revealed the top-of-mind concerns and to what extent continuous monitoring is seen as a solution to those concerns.

Whether the threats are malicious or simply human error, there is no escaping the fact that people are an unpredictable element in any agency's cybersecurity defense. It's impossible to change human nature, but with continuous monitoring it is possible to put checks and balances in place to significantly reduce the threats people pose.

Continuous monitoring is the ability to automatically collect data and report on the performance, availability, and security posture of IT infrastructure, applications, and, most importantly, the critical/sensitive data they hold. IT Ops has used continuous monitoring for decades, focusing on availability and performance of IT systems. Now InfoSec is accelerating its rollout of continuous monitoring technology for compliance and security purposes.

SolarWinds commissioned a study to learn about the primary cybersecurity threats facing federal agencies, the degree of cybersecurity readiness within agencies, obstacles agencies face, and the extent to which continuous monitoring tools facilitate their response.

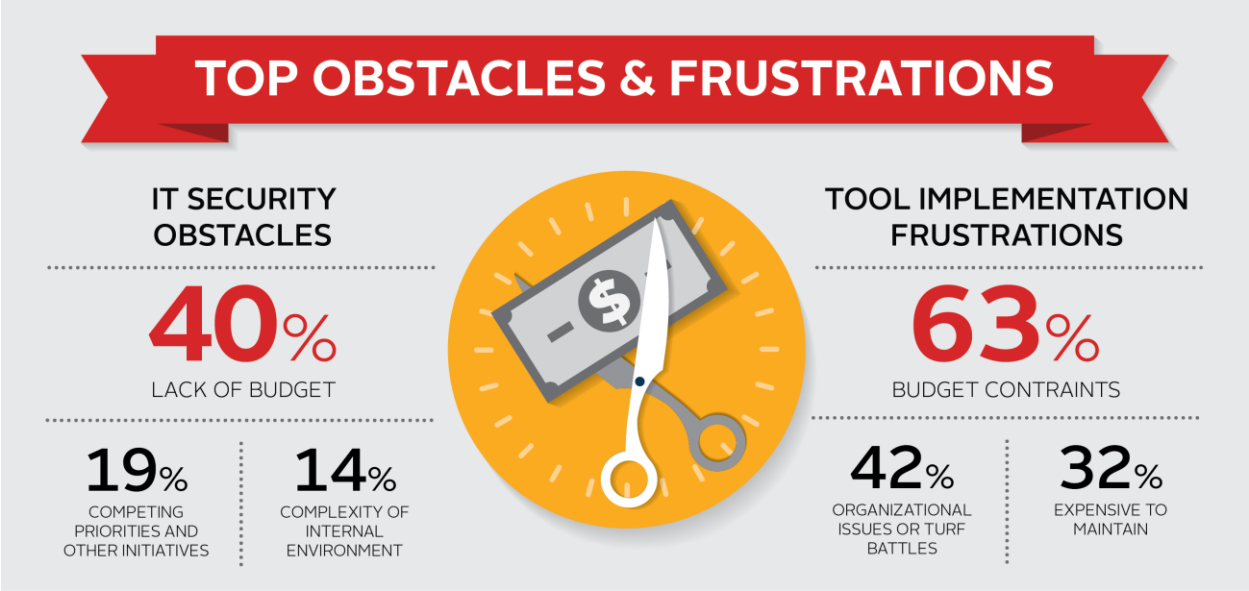
The study by Market Connections, Inc. revealed the top-of-mind cybersecurity concerns federal agencies are facing and to what extent continuous monitoring is seen as a solution to those concerns—what they are prepared for, what they are not prepared for, and how they can become better prepared to address the unpredictable human component of cybersecurity defense.

MOST PRESSING CYBERSECURITY CONCERNS

Operations

With budgets tightening throughout the federal government, it is no surprise that 40% of respondents consider budget constraints the single most significant high-level obstacle to maintain or improve IT security, followed by competing priorities (19%) and complexity of their internal environment (14%).

When it comes to the frustrations associated with implementing cybersecurity tools, the importance of budget and the complexity of the internal environment rises even higher. Budget is the primary frustration for 63% of respondents. Organizational issues or turf battles shoot up to almost half (42%), likely in part because IT Ops and InfoSec have sometimes seen each other as adversaries rather than allies. Although there is strong evidence that any adversarial relationship is rapidly disappearing.



IT Ops knows that continuously monitoring their infrastructure is critical to their success, and have been doing it for years with performance monitoring, availability monitoring, and change management tools. More recently InfoSec has been driving the use of automated tools for their success: compliance monitoring, security monitoring, change monitoring, and log monitoring tools. The challenge for cybersecurity is that InfoSec often has the budget for automated tools, but limited budget for actually operating the tools.

People

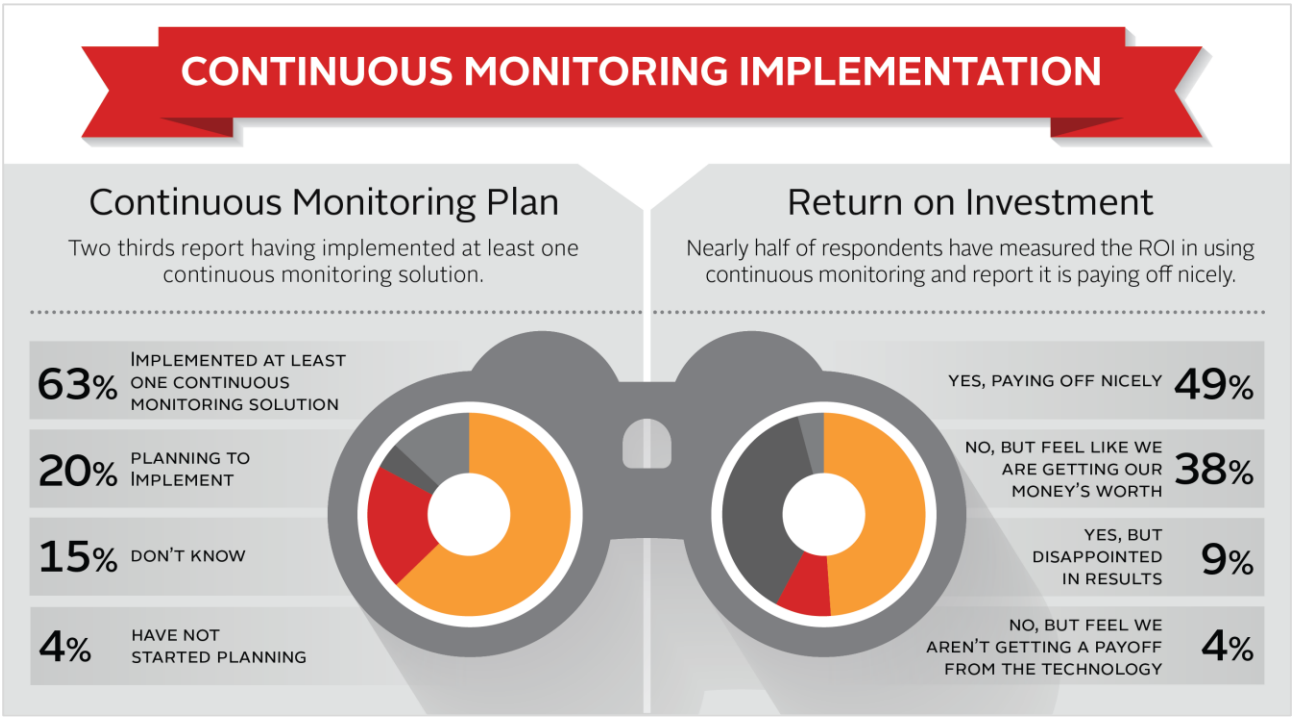
Whether cybersecurity threats come from the general hacking community (47% of total respondents) or careless or untrained insiders (42% of total respondents), people are the largest source of security threats at agencies. While civilian agencies are more concerned about external threats, defense agencies see threats coming from the inside. External hacking (50%) and malware (46%) are the overall top cybersecurity concerns plaguing agencies and nearly one-third (29%) also cite insider data leakage/theft as a threat.

How can federal agencies address these threats? By implementing continuous monitoring.

USING CONTINUOUS MONITORING TOOLS

Most agencies realize continuous monitoring tools help address threats—two-thirds of respondents have implemented at least one continuous monitoring tool (63%). And this decision is paying off. Half of those who are measuring the return on investment (ROI) (49%), and 38% of those who are not actively measuring ROI, say the investment is paying off for their agency.

Of the one-third of respondents who do not have continuous monitoring in place, 86% cite budget constraints as the primary reason. Lack of manpower (43%) and competing priorities (29%) also impact the decision to put off planning. Only 20% of this group is currently planning to implement continuous monitoring, while 18% either are not, or do not know, if it's in their plans.



Lack of executive buy-in on the importance of complicance is significantly more frustrating for current non-users versus users (29% versus 14%). However, it's not surprising that agencies where compliance is not a high priority would tend not to invest in compliance tools such as continuous monitoring.

The Benefits of Continuous Monitoring

"There are always people who don't think the rules apply to them. Securing your environment is about making sure people aren't breaking the rules. Continuous monitoring technology flags this activity as it happens."

CHRIS LAPOINT
VP PRODUCT MANAGEMENT, SOLARWINDS

While the majority of respondents describe their agency's overall cybersecurity readiness as good or excellent, a significantly greater proportion of respondents that use continuous monitoring tools rate their readiness as excellent (54% vs. 28%). This is no surprise considering continuous monitoring tools can change reaction times from days, weeks or months, to minutes or hours and uncover vulnerabilities that may typically only be found during a quarterly or annual manual audit of security configurations. While the nature of security requires reactive response, agencies using continuous monitoring can react faster, saving vital time in containing a breach and minimizing damage. From sophisticated attacks to simple mistakes, continuous montioring tools get the job done.

For example, a targeted attack originating at the perimeter implants new malware on a system, compromising user accounts and leading to data theft from multiple systems. Continuous monitoring would correlate events from the network, systems, and applications and identify the suspicious activity, allowing InfoSec to respond quickly.

Another example is as simple as denying account access to users identified during routine log data examination as using accounts to access data they do not have permission to access.

True continuous monitoring requires automation and the capabilities to intelligently analyze and act on the information in as near real-time as possible. A variety of tools meet this criteria, most of which can serve a dual purpose for IT Ops and InfoSec. Types of tools include network and firewall configuration and change management, server and application monitoring, network performance monitoring, endpoint tracking, log and event management.

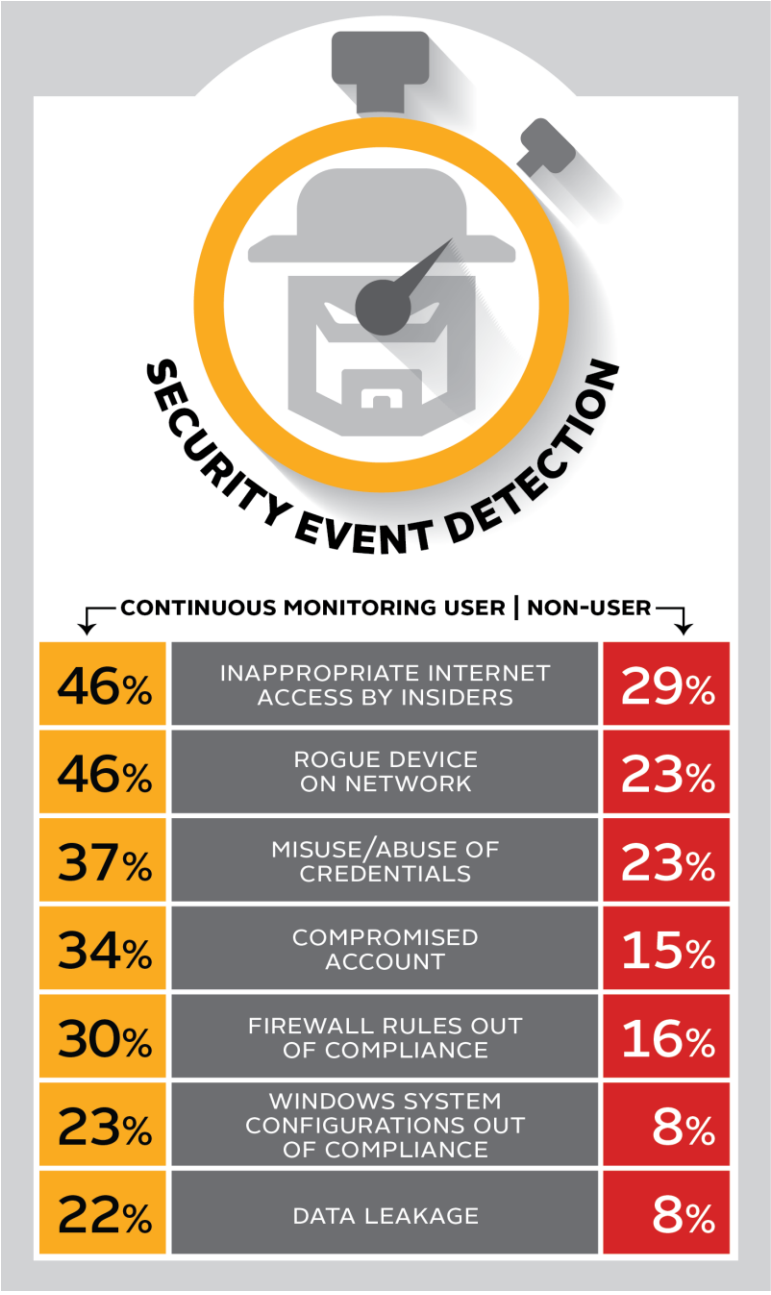
USING CONTINUOUS MONITORING TO ADDRESS THE THREATS

One of the primary ways continuous monitoring addresses the people threat is through timely awareness of real-time vulnerabilities—a benefit 69% of respondents recognize as important.

For example, by monitoring user logs, IT Ops or InfoSec could spot a breach as it is happening and stop it. This real-time threat detection over-rides the internal procedures that can sometimes slow response times between departments.

Despite an acknowledgment that speed is imperative when addressing cybersecurity threats, almost half of the respondents have slow response times to their biggest threats. It takes *one day or more* to detect inappropriate access from insiders (42%), misuse/abuse of credentials (46%), a compromised account (49%), inappropriate sharing of documents (64%), or an external data breach (46%). Malware detection (47%), compliance issues (50% and higher), and firewall rules (53%) present similar challenges. By the time these threats are detected, the damage has been done. Continuous monitoring tools can detect those threats in minutes, if not moments.

In addition to the real-time security detection, continuous monitoring can leverage integrative tools that help bridge teams—thus addressing the frustrations of turf issues. The fact is IT Ops and InfoSec are often studying the



same data, they're simply looking at it from different perspectives.

By using the same tools, they can not only reduce their teams' costs, they can each get a more holistic picture of what is happening throughout the organization.

CONCLUSIONS

Continuous monitoring is bridging the gap between the teams responsible for managing the unpredictable human component of cybersecurity. By working together, they significantly reduce the risks—and costs—of security breaches.

- Agencies that place a focus on continuous monitoring have higher levels of security and compliance, and are better situated to address cyber threats.
- Despite historical arguments from InfoSec that IT Ops isn't concerned about security, the data shows that IT Ops does care about cybersecurity and their role in implementing plans—in fact, the two groups had nearly identical responses to the survey questions. As both IT Ops and InfoSec realize they are working toward the same end, continuous monitoring tools can help to diminish the organizational turf battles—easing at least one of the concerns agencies face.
- While budget is a primary barrier to implementing continuous monitoring, for many tasks, continuous monitoring tools can collect the data both teams need, giving them the opportunity to extend their budgets by consolidating tools rather than duplicating efforts. In fact, agencies don't necessarily need big security frameworks or expensive tools. Many are already monitoring the data. For example, an agency might already have a configuration management tool in place that can provide the data for identifying unauthorized configuration changes on a continuous basis. It's about working together.
- Continuous Monitoring helps both defense and civilian agencies keep up with the latest vulnerabilities and respond faster to the primary threats against their agencies.

"Any time an incident occurs, the first question is 'is it an IT issue or a security issue?' Continuous monitoring tools provide a central collaboration point between IT Ops and InfoSec that helps put an end to the inefficient and dangerous siloed operations of the past."

Chris LaPoint
VP Product Management,
SolarWinds

From network and firewall configuration to application performance monitoring, continuous monitoring helps make the unpredictable manageable—and that makes your agency ready to address any cyber threat.

ABOUT THE STUDY

The SolarWinds 2014 Cybersecurity Online Survey explores the greatest cybersecurity threats federal agencies face, their levels of readiness, the obstacles they face in addressing them, and the extent to which continuous monitoring tools prove beneficial. The blind online survey reached 200 IT decision makers and influencers, of which 56% were federal, civilian, or independent government agencies; 40% were defense; and 4% were other agencies. One-third were IT Ops or InfoSec staff, and almost half (47%) had 15+ years of tenure in their position. More than half (51%) are on a team that makes decisions regarding IT security and/or IT operations and management

solutions and 41% manage or implement IT security and/or IT operations and management solutions.

ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to nearly every civilian agency, DoD branch and intelligence agencies. In all market areas, the SolarWinds approach is consistent—focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Each solution is rooted in the company's deep connection to their user base, which interacts in an online community, thwack®, to solve problems, share technology and best practices, and directly participate in the product development process.

SolarWinds provides IT management and monitoring solutions to numerous common public sector IT challenges including continuous monitoring, cybersecurity, network operations, compliance, data center consolidation, cloud computing, mobile workforce and devices, and scaling to the enterprise. SolarWinds software is available on the U.S. General Services Administration (GSA) Schedule, Department of Defense ESI and numerous other contract vehicles. For more information and fully functional free trials visit: http://www.solarwinds.com/federal.

ABOUT MARKET CONNECTIONS, INC.

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education. For more information visit: www.marketconnectionsinc.com.

Managing the Unpredictable Human Element of Cybersecurity

Market Connections
Research you can act on.

solarwinds

CONTINUOUS MONITORING USER		NON-USER
46%	INAPPROPRIATE INTERNET ACCESS BY INSIDERS	29%
46%	ROGUE DEVICE ON NETWORK	23%
37%	MISUSE/ABUSE OF CREDENTIALS	23%
34%	COMPROMISED ACCOUNT	15%
30%	FIREWALL RULES OUT OF COMPLIANCE	16%
23%	WINDOWS SYSTEM CONFIGURATIONS OUT OF COMPLIANCE	8%
22%	DATA LEAKAGE	8%

CONTINUOUS MONITORING IMPLEMENTATION

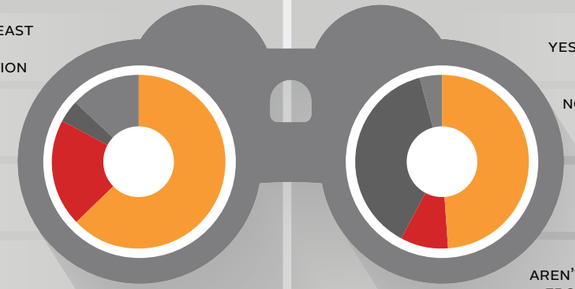
Continuous Monitoring Plan

Two thirds report having implemented at least one continuous monitoring solution.

- 63% IMPLEMENTED AT LEAST ONE CONTINUOUS MONITORING SOLUTION
- 20% PLANNING TO IMPLEMENT
- 15% DON'T KNOW
- 4% HAVE NOT STARTED PLANNING

Return on Investment

Nearly half of respondents have measured the ROI in using continuous monitoring and report it is paying off nicely.



- YES, PAYING OFF NICELY 49%
- NO, BUT FEEL LIKE WE ARE GETTING OUR MONEY'S WORTH 38%
- YES, BUT DISAPPOINTED IN RESULTS 9%
- NO, BUT FEEL WE AREN'T GETTING A PAYOFF FROM THE TECHNOLOGY 4%

TOP OBSTACLES & FRUSTRATIONS

IT SECURITY OBSTACLES

40% LACK OF BUDGET

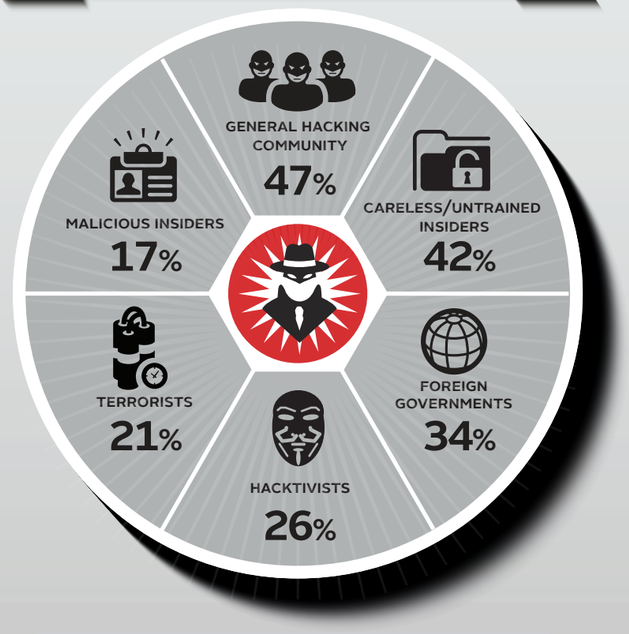
- 19% COMPETING PRIORITIES AND OTHER INITIATIVES
- 14% COMPLEXITY OF INTERNAL ENVIRONMENT

TOOL IMPLEMENTATION FRUSTRATIONS

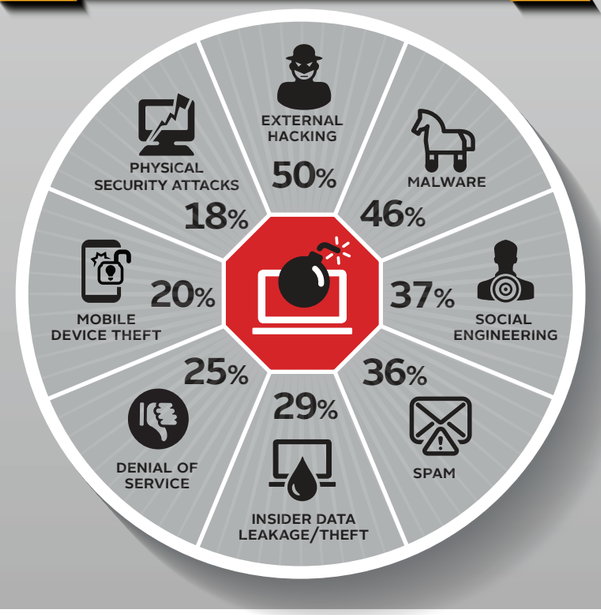
63% BUDGET CONTRAINTS

- 42% ORGANIZATIONAL ISSUES OR TURF BATTLES
- 32% EXPENSIVE TO MAINTAIN

SECURITY THREAT SOURCES



CYBERSECURITY THREATS



SolarWinds.com/Federal | 877.946.3751