Datacenter Security Automation

NANJGEL Solutions

Modern datacenter security components

Privileged User Management

Next Generation Security mechanism

Threat Intelligence

Security, privacy and compliance

NANJGEL Solutions

Privileged User Management

NANJGEL Solutions

Privileged Accounts

Everywhere In the Enterprise

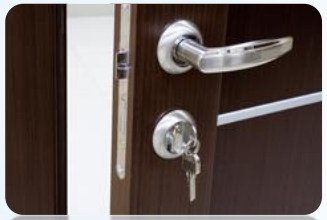
- Servers & Workstations
  - Every hardware platform
  - Every operating system
- Datacenter Appliances
  - Routers and switches
  - Application accelerators
  - Security appliances
- Applications
  - Line-of-business
  - Web services
  - Database and middleware
  - Backup services
  - Identity and access management
  - Systems management




Privileged Accounts

What Are The Risks?

- **Do we know where all of our privileged accounts are?**
- **Do the wrong people have access to sensitive data?**
- **Who is sharing credentials? Who is accountable?**
- **Are inconsistent & invisible access policies inviting abuse?**
- **Will our passwords fail to withstand dictionary and social attacks?**
- **Where are developer “back doors”?**
- **Does lack of automation make it impractical to comply with policies?**
- **Are manual processes wasting resources & leaving security holes?**
- **Will manual account changes lead to application failure & downtime?**
- **Are privileged accounts being used for tasks that don’t require them?**
- **If one IT asset is compromised, will others be exploited as a result?**
- **Will we fail our next IT audit?**

Mitigating the Risks

1. ***Identify*** and document critical IT assets, their privileged accounts and interdependencies.
2. ***Delegate*** so that only appropriate personnel can access privileged accounts in a timely manner, using the least privilege required, with documented purpose, during designated times.
3. ***Enforce*** rules for password strength, uniqueness and change frequency, synchronizing changes across dependencies.
4. ***Audit*** and alert so that the requesters, purpose and requested duration are documented and management is made aware of unusual access and other events.



Customer Value

Executive Management (CISO / CIO)

- Protect corporate assets
- Comply with regulatory requirements
- Improve corporate agility against new security threats

IT Director

- Increase operational efficiency
- Prove that policies and IT processes are aligned
- Reduce the risk of planned changes and unplanned events

Administrator

- Automate tedious, error-prone tasks
- Mitigate security threats in a changing environment
- Eliminate security monitoring and compliance uncertainty

User Activity Monitoring

NANJGEL Solutions

69%

OF REPORTED BREACHES INVOLVE
A TRUSTED USER

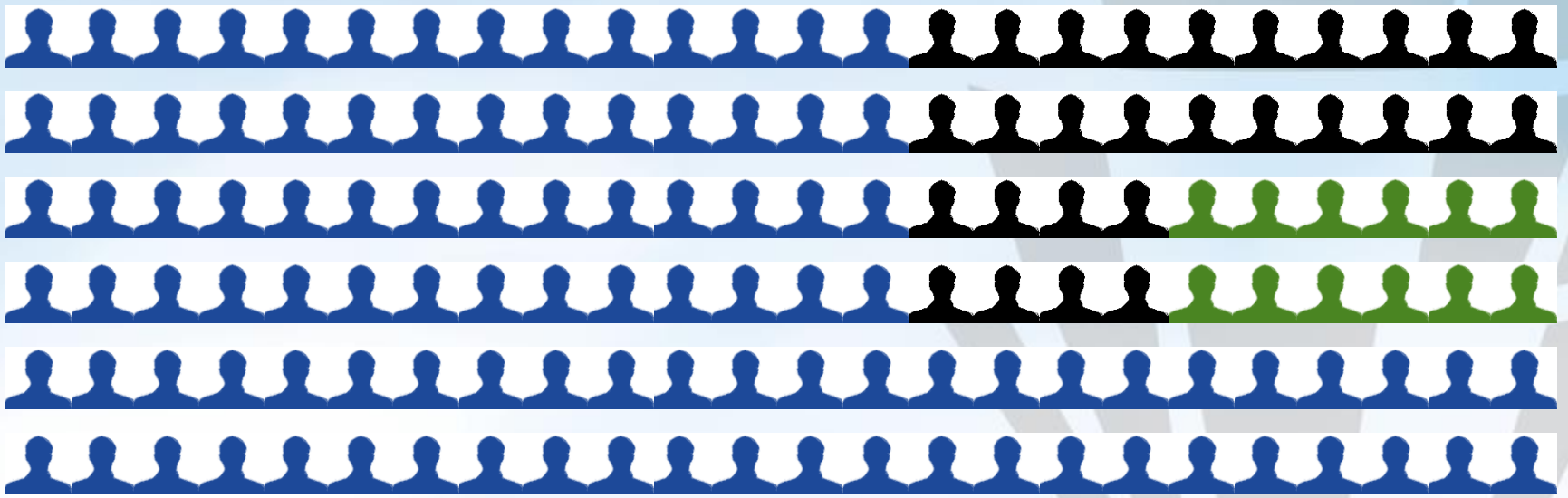
76%

of data breaches involve

Accounts with Access to Sensitive Data

Source: Data Breach Investigations Report Verizon

Do you know Your Risky Users?



Business Users

84% of Insider based breaches involve users with no admin rights[2]

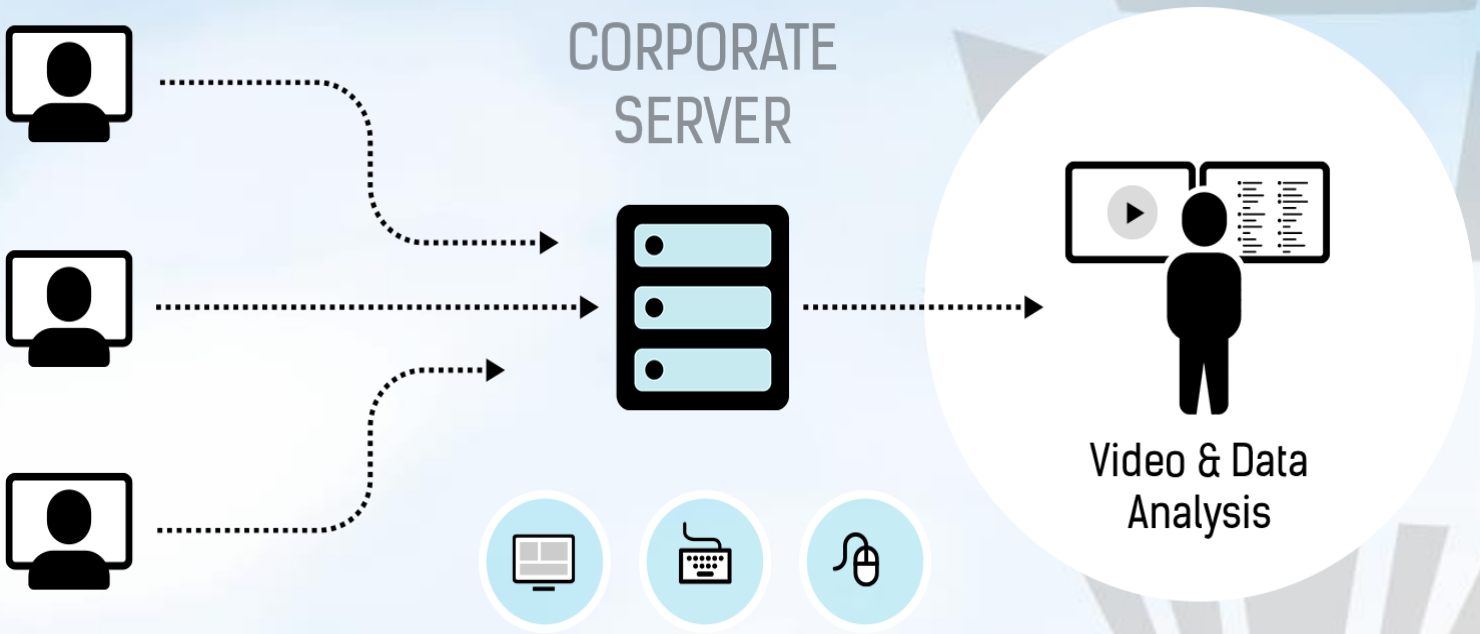
IT Users

62% of admin-caused breaches due to human error[3]

Contractors

NANJGEL Solutions

Find out Who's Doing what?



Identify and Manage User-based Risks

- Monitor all user activity
- Real-time and historical reporting
- User behavior analysis and alerting
- Integrates with SIEM & IAM

NANJGEL Solutions

USER RISK MITIGATION

Monitoring, Detection & Rapid Incident Response

Analyze
Monitor and baseline user activity

Detect
Instantly detect changes in actual user behavior that warrant investigation

Respond
Isolate users, systems and data in real-time and historically with detailed forensic data

NANJGEL Solutions

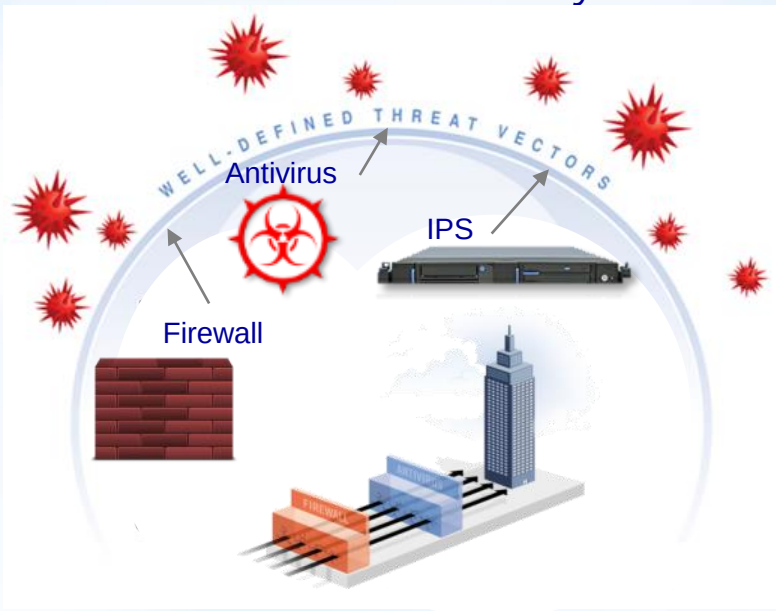
Database Security

The Security Landscape is changing rapidly

Data Explosion | Consumerization of IT | Everything is Everywhere | Attack Sophistication

Extending the perimeter; focus shifts to protecting the DATA

Moving from traditional perimeter-based security…



NANJGEL Solutions

*Continuously monitor access to sensitive **DATA** including databases, data warehouses, big data environments and file shares to...*

1 **Prevent data breaches**

- Prevent disclosure or leakages of sensitive data

2 **Ensure the integrity of sensitive data**

- Prevent unauthorized changes to data, database structures, configuration files and logs

3 **Reduce cost of compliance**

- Automate and centralize controls
- Simplify the audit review processes

4 **Protect Data in an efficient, scalable, and cost effective way**

Increase operational efficiency

✓Automate & centralize internal controls
✓Across heterogeneous & distributed environments
✓Identify and help resolve performance issues & application errors
✓Highly-scalable platform, proven in most demanding data center environments worldwide

No degradation of infrastructure or business processes

✓Non-invasive architecture
✓No changes required to applications or databases

NANJGEL Solutions

Data Security Solution

Data at Rest

Discovery
Classification

Masking
Encryption

Configuration

Vulnerability
Assessment

Entitlements
Reporting

Data in Motion

Activity
Monitoring

Blocking
Quarantine

Dynamic Data
Masking

Discover — *Where is the sensitive data?*

How to protect sensitive data?

- Security Policies
- Dormant Data
- Dormant Entitlements

Harden — *How to secure the repository?*

Who should have access?

Monitor — *What is actually happening?*

- Compliance Reporting
- Security Alerts / Enforcement

Protect — *How to protect sensitive data to reduce risk?*

How to prevent unauthorized activities?

NANJGEL Solutions

Data Security solutions protect structured and unstructured sensitive data

Discovery
Classification

Masking
Encryption

Vulnerability
Assessment

Entitlements
Reporting

Activity
Monitoring

Blocking
Quarantine

Discover

"Base Product"

- ✓ DB and Data Discovery
- ✓ Data Classification
- ✓ Enterprise Integrator
- ✓ Entitlement Reporting
- ✓ Queries & Reports
- ✓ Threshold Alerts
- ✓ Compliance Workflow
- ✓ Group Management
- ✓ Security Integrations
- ✓ IT Integrations
- ✓ Data Level Security
- ✓ Incident Management
- ✓ User/Roles Management
- ✓ HR Integrations
- ✓ Portal Management
- ✓ Self Monitoring
- ✓ Data Export Options
- ✓ Data Imports Options

Harden

Vulnerability Assessment

- ✓Assessment reports
- ✓Data Protection Subscription
- ✓Configuration Changes

Data Encryption

- ✓File-level encryption
- ✓Role-based access control
- ✓File access auditing

Static Data Masking

- ✓Static masking
- ✓Semantic and format preserving

Monitor

Standard DAM

- ✓Data Activity Monitoring
- ✓Real-time alerts
- ✓App end-user identification
- ✓Normalized audit creation
- ✓Compliance reporting
- ✓Compliance workflow
- ✓Federate large deployment
- ✓Central control
- ✓Central audit collection

Protect

Advanced DAM

- ✓ Blocking access
- ✓ Masking sensitive data
- ✓ Users Quarantine

Data Redaction

- ✓ Redact sensitive documents

Masking for Applications

- ✓ Masking on the browser

NANJGEL Solutions

Application Security

Securing Applications is a Challenge

Your Application Portfolio
Different Types & Sources


Financial


HR


Logistics


Intranet


Outsource


In-house


Legacy


Open Src

Your Policies
- Data Privacy
- Regulatory Compliance
- Accountability

Your SDLC Processes

- Large and diverse application portfolios
- Mobile applications
- In-house and outsource development
- External & internal regulatory pressure
- Pockets of security expertise
- Yet another task for developers

Need an efficient, scalable, automated way to

develop and deliver secure applications…

NANJGEL Solutions

Threat Intelligence & Analysis

Provides Specific Analysis of:

- Vulnerabilities and exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

Most comprehensive vulnerability database in the world

- Entries date back to the 1990's

Event Name	2012 Rank	Trend	2011 Rank	Trend	2010 Rank	Trend
SQL_Injection	1	Up	1	Up	2	Down
SQL_SSRP_Slammer_Worm	2	Slightly Down	3	Slightly Down	1	Down
PsExec_Service_Accessed	3	Slightly Up			3	Slightly Up
HTTP_GET_DotDot_Data	4	Up	5	Up		
Cross_Site_Scripting	5	Slightly Up	6	Slightly Up		
SNMP_Crack	6	Down	4	Down		
SSH_Brute_Force	7	Slightly Up	7	Slightly Up	4	Slightly Up
HTTP_Unix_Passwords	8	Up	8	Up	6	Slightly Up
Shell_Command_Injection	9	Slightly Up	9	Up		
JavaScript_Shellcode_Detected	10	Up				

Table 1: Top MSS High Volume Signatures and Trend Line - 2012 H1

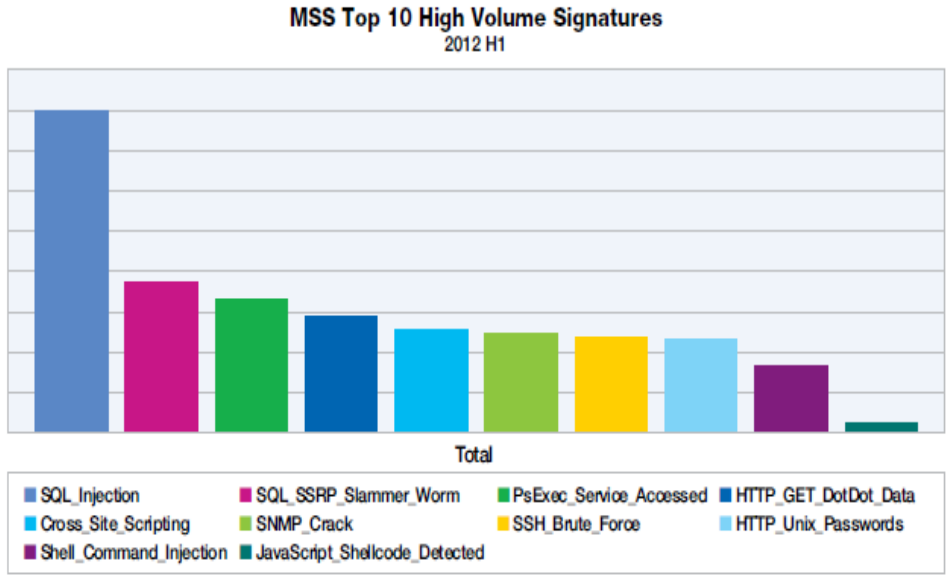


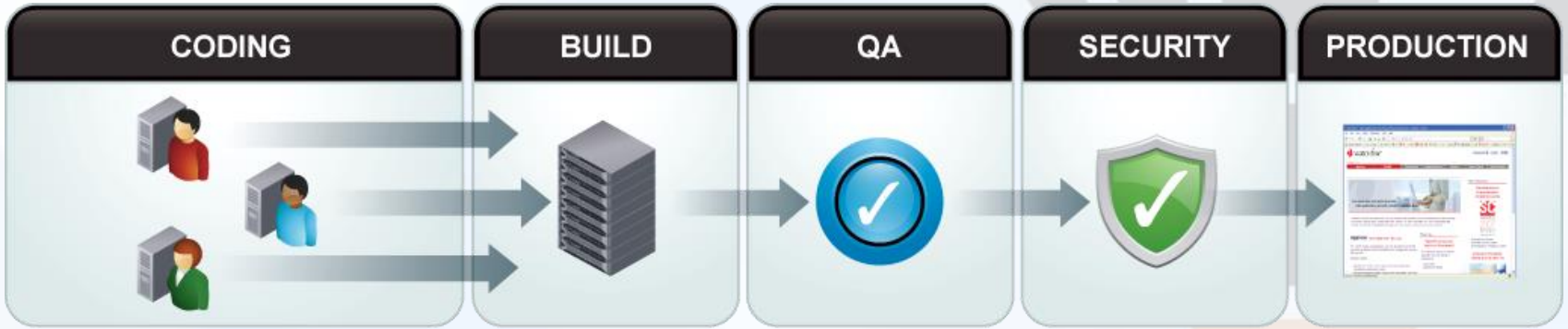
Figure 3: MSS Top 10 High Volume Signatures - 2012 H1

NANJGEL Solutions

Adopt a **Secure by Design** approach to enable you to design, deliver and manage smarter software and services

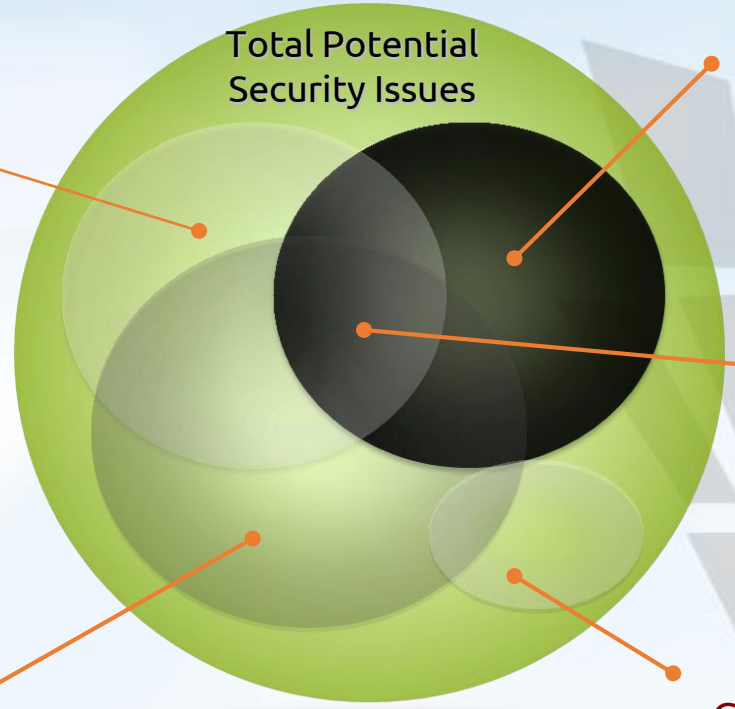
- Build security into your application development process
- Efficiently and effectively address security defects **before deployment**
- Collaborate effectively between Security and Development
- Provide Management visibility

Deliver New Services Faster | Innovate Securely | Reduce Costs



Proactively address vulnerabilities early in the development process

App Scan helps finding more vulnerabilities using advanced techniques



Static Analysis

- Analyze Source Code
- Use during development
- Uses Taint Analysis / Pattern Matching

Dynamic Analysis

- Analyze Live Web Application
- Use during testing
- Uses HTTP tampering

Hybrid Analysis

- Correlate Dynamic and Static results
- Assists remediation by identification of line of code

Run-Time Analysis

- Combines Dynamic Analysis with run-time agent
- More results, better accuracy

Client-Side Analysis

- Analyze downloaded Javascript code which runs in client
- Unique in the industry

Next- Gen Prevention Mechanisms

NANJGEL Solutions

WHAT'S CHANGED?

THE EVOLUTION OF THE **ATTACK**

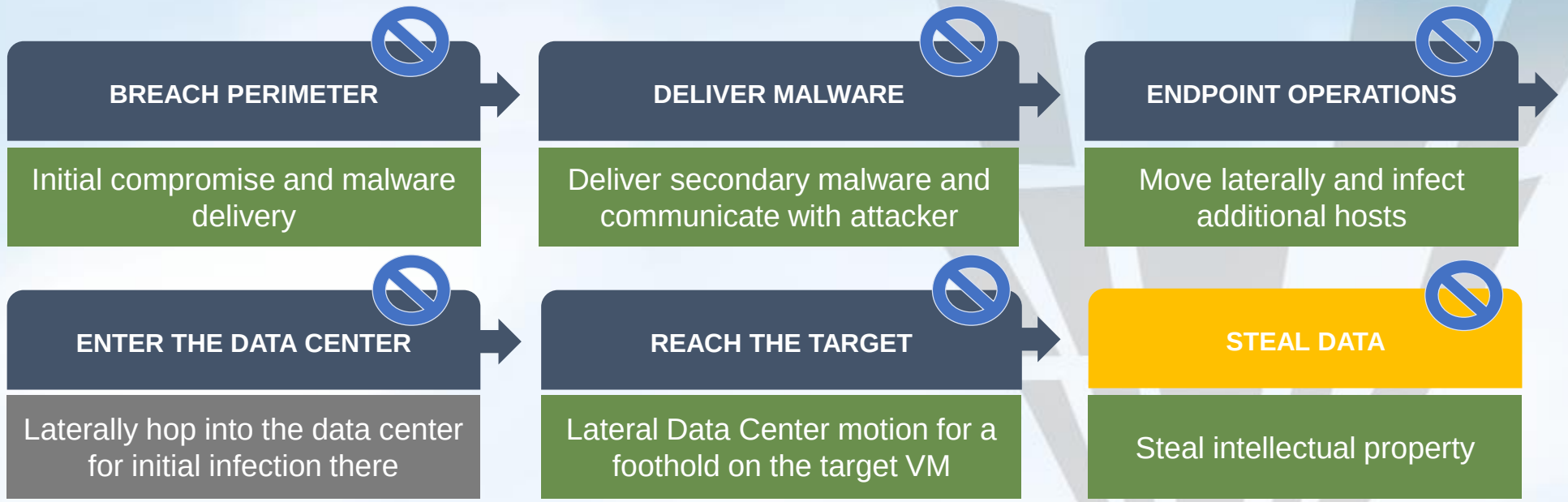
Common traits for breached networks

1. A port based firewall
2. A static IPS
3. Zero Day Malware used to manipulate platforms in the network
4. Identity credentials hijacked

NANJGEL Solutions

Understanding the Attack Kill-chain

Attack kill-chain

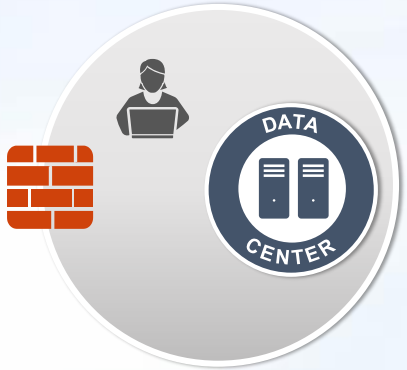


Prevent attacks by stopping one step in the kill-chain

REQUIREMENTS FOR THE FUTURE

DETECT **AND** PREVENT THREATS AT EVERY POINT ACROSS THE ORGANIZATION

At the mobile device



At the internet edge

Between employees and devices within the LAN

At the data center edge, and between VM's

Within private, public and hybrid clouds

NANJGEL Solutions

Requirements for Security in todays Threat Landscape

1. Application based security rules
   - Including the ability to decrypt flows
2. Rules based on User Identity/User Groups
3. Sandbox Technology to detect unknown malware
4. Threat Prevention updates to enable dynamic prevention signatures for malware
5. URL Technology to enable dynamic prevention of malware Command & Control

NANJGEL Solutions

Security Information & Event Management

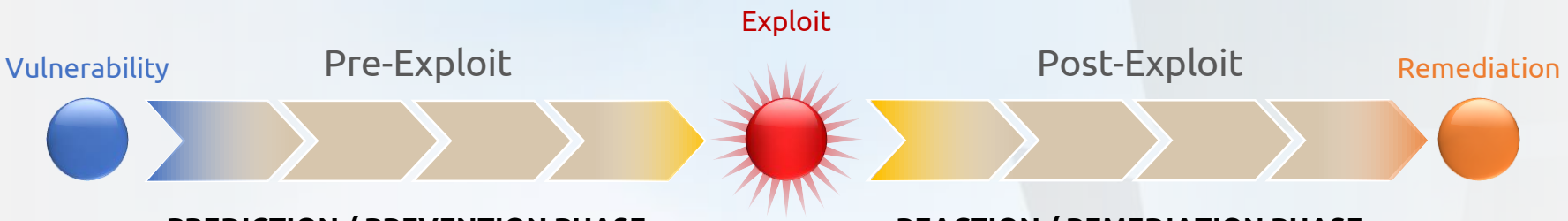
NANJGEL Solutions

What are the major risks and vulnerabilities?

Are we configured to protect against advanced threats?

What security incidents are happening right now?

What was the impact to the organization?



PREDICTION / PREVENTION PHASE

- Gain visibility over the organization's security posture and identity security gaps
- Detect deviations from the norm that indicate early warnings of APTs
- Prioritize vulnerabilities to optimize remediation processes and close critical exposures before exploit

REACTION / REMEDIATION PHASE

- Automatically detect threats with prioritized workflow to quickly analyze impact
- Gather full situational awareness through advanced security analytics
- Perform forensic investigation reducing time to find root-cause; use results to drive faster remediation

Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

NANJGEL Solutions

Providing actionable intelligence

INTELLIGENT

Correlation, analysis and massive data reduction

AUTOMATED

Driving simplicity and accelerating time-to-value

INTEGRATED

Unified architecture delivered in a single console

Embedded intelligence offers automated offense identification

Extensive Data Sources

- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Application activity
- Configuration information
- Vulnerabilities and threats
- Users and identities
- Global threat intelligence

Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

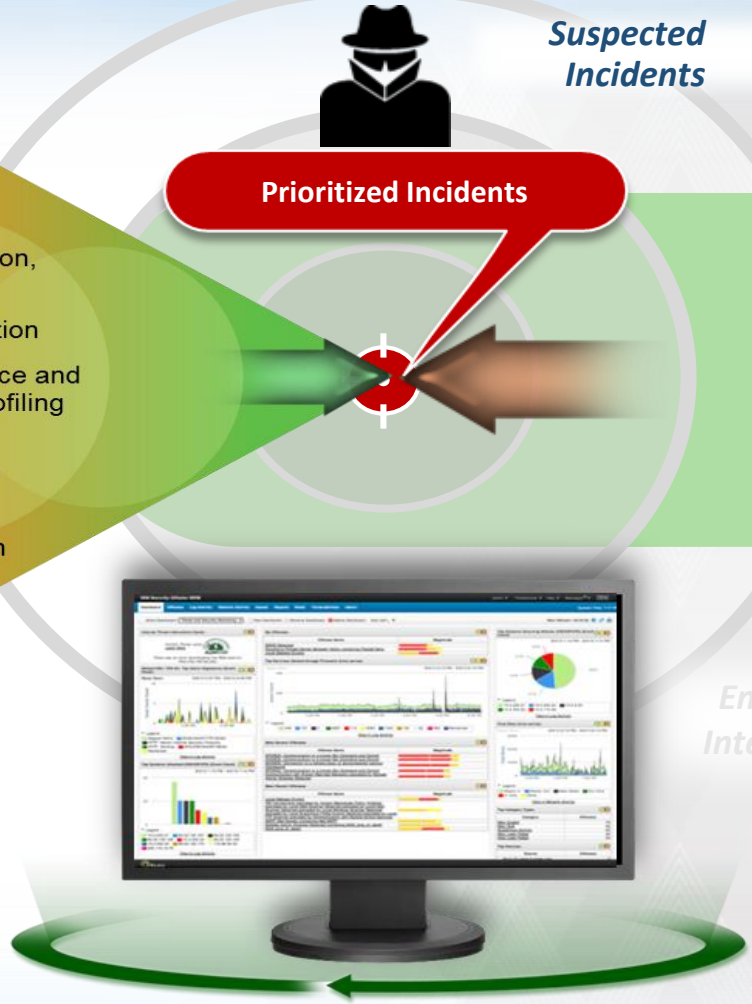
Embedded Intelligence

NANJGEL Solutions

Extend clarity around incidents with in-depth forensics data

Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box



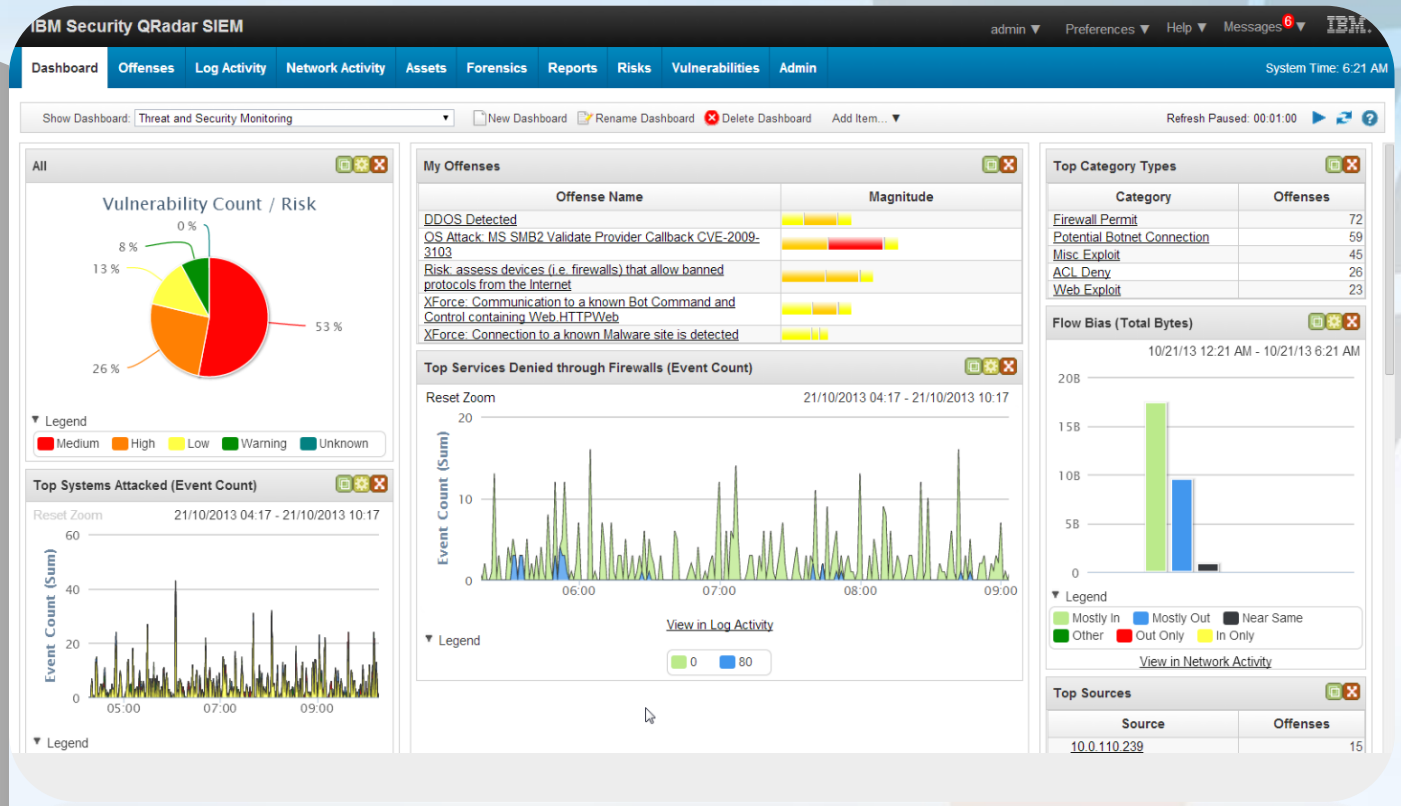
Directed Forensics Investigations

- Rapidly reduce time to resolution through intuitive forensic workflow
- Use intuition more than technical training
- Determine root cause and prevent re-occurrences

NANJGEL Solutions

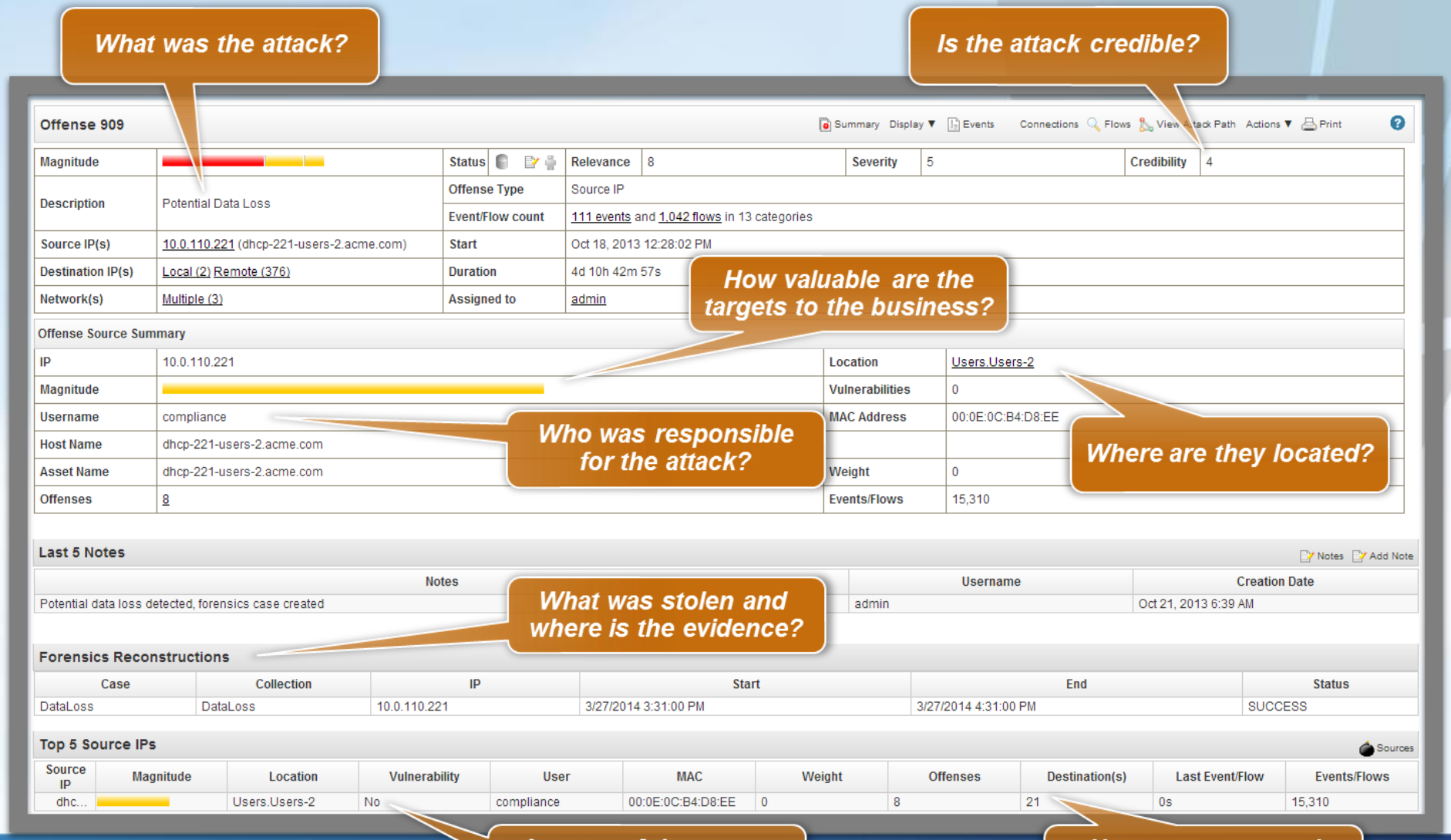
An integrated, unified architecture in a single appliance

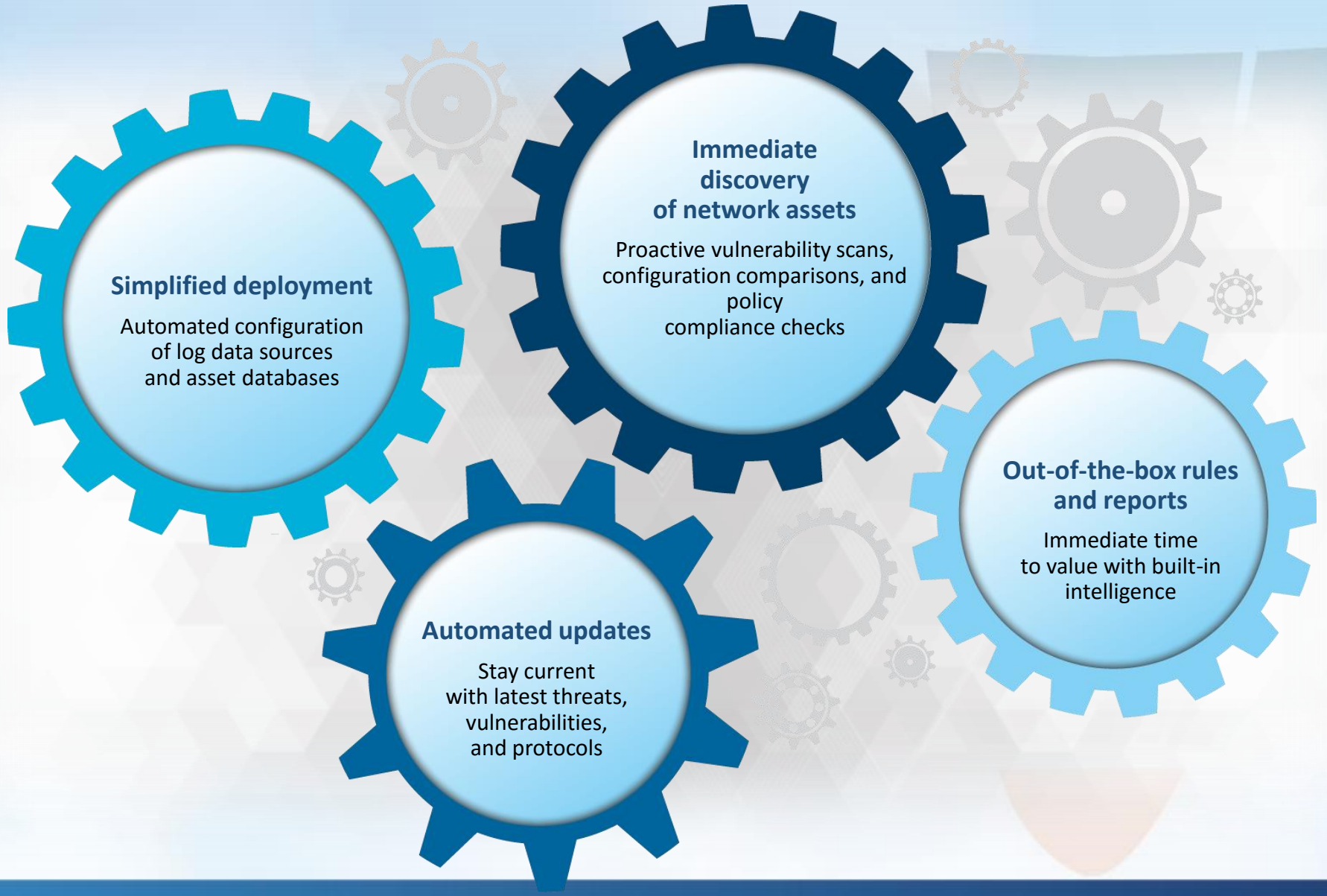
- Log Management
- Security Intelligence
- Network Activity Monitoring
- Risk Management
- Vulnerability Management
- Network Forensics



NANJGEL Solutions

Answering questions to help prevent and remediate attacks





Identify and quickly remediate

Deploy comprehensive security intelligence and incident forensics

Address regulation mandates

Automate data collection and configuration audits

Detect insider fraud

Adopt next-generation SIEM with identity correlation

Consolidate data silos

Collect, correlate and report on data in one integrated solution

Better predict business risks

Engage entire lifecycle of risk management for network and security infrastructures

NANJGEL Solutions

Consolidation and integration help reduce costs and increase visibility

Traditional SIEM

6 products from 6 vendors are needed

Flows	ARBOR NETWORKS, Lancope, riverbed Think fast.
Packets	EMC² RSA, SOLERA NETWORKS
Vulnerabilities	QUALYS, RAPID7, tenable network security
Configurations	algosec FIREMON, skybox security, tufin, REDSEAL NETWORKS
Logs	loglogic, splunk>
Events	ArcSight, McAfee, EMC² RSA

Security

Intelligence and Analytics

An integrated, unified architecture in a single web-based console

NANJGEL Solutions