BowBlack Ninja base system:Compliance and Security
Questions and Answers Knowledgebase

"…Does BowBlack Ninja base system have any certifications for compliance regulations such as PCI or HIPAA, or against frameworks like ISO27001, NEN7510, or ISAE3400/3402?…"

Certifications

As of November 2020, The Ninja base system has the following certifications.

Regulation/Certification	Details/Comments	Status
SOC 2 [American Institute of CPAs (AICPA)'s ***S***ervice ***O***rganization ***C***ontrol reporting platform]	"…Developed by the American Institute of CPAs (AICPA), SOC 2 is specifically designed for service providers using the cloud to store customer data, inclusive of nearly every SaaS company…" "…The Service Organization Control (SOC) 2…certification is among the most coveted and hard to obtain information-security certification. It demonstrates that an expertly trained independent accounting and auditing firm has examined an organization's non-financial reporting control objectives and activities, and has actually tested those controls over time to ensure that they are operating effectively…" BowBlack Ninja base system. bases their SOC 2 controls on the following well-tested, industry-validated, and widely-accepted guidelines: 1) The ***NIST Cyber Security Framework*** – "…The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework, or CSF) was originally published in February 2014 in response to Presidential Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity'…" *[As an AWS Enterprise client, both Ninja base system and AWS are focused on bringing security to cloud. AWS has a writeup on the CSF adoption.*	Ninja base system has received AICPA SOC2 certification from accredited audit firm Schellman & Company. The most recent audit was performed in Q1 (Jan-Mar) 2020. The report following this audit was completed in Q2 (April) 2020. Full SOC 2 Certification validates that Ninja base system has exceeded the requirements of HIPAA, PCI-DSS, GDPR, and CCPA.

	2) The ***NIST Special Publication # 800-171*** – "...NIST 800-171...was developed after FISMA (Federal Information Security Management Act) was passed in 2003...to improve cybersecurity [controls of NIST 800-53]...after numerous well-documented [U.S. federal government agencies were breached]...including [the]...U.S. Postal Service...and [the] National Oceanic and Atmospheric Administration]. ..[the] National Institute of Standards and Technology Special Publication 800-171.. [is] a set of standards that define how to safeguard ..information that is sensitive and relevant to the interests of the United States. " ***3)*** The ***NIST Special Publication # 800-53*** – ". [NIST 800-53] guidelines were created to heighten the security of the information systems used within the federal government. [and] provides a catalog of controls that support the development of secure and resilient federal information systems. "	
HIPAA [***H***ealth ***I***nsurance ***P***ortability and ***A***ccountability ***A***ct]	SOC 2 Certification exceeds requirements of HIPAA Act	Ninja base system's controls already meet, and for some controls exceed, the requirements of HIPAA.
HITECH [***H***ealth ***I***nformation ***T***echnology for ***E***conomic and ***C***linical ***H***ealth Act]	Supports HIPAA, "…created to promote and expand the adoption of health information technology, specifically, the use of electronic health records (EHRs) by healthcare providers…"	Ninja base system's controls already meet, and for some controls exceed, the requirements of HITECH.
PCI-DSS [***P***ayment ***C***ard ***I***ndustry ***D***ata ***S***ecurity ***S***tandard]	SOC 2 Certification exceeds requirements of PCI-DSS	Ninja base system's controls already meet, and for some controls exceed, the requirements of PCI-DSS.
GDPR [EU ***G***eneral ***D***ata ***P***rotection ***R***egulation]	SOC 2 Certification exceeds requirements of EU GDPR	Ninja base system's controls already meet, and for some controls

		exceed, the requirements of GDPR.
EU-US Privacy Shield	Supports EU GDPR Compliance	Certification obtained February 2020
Swiss-US Privacy Shield	Supports EU GDPR Compliance	Certification obtained February 2020
CCPA [***C***alifornia ***C***onsumer ***P***rivacy ***A***ct]	SOC 2 Certification exceeds requirements of CCPA	Ninja base system's controls already meet, and for some controls exceed, the requirements of CCPA.

Compliance & Security Initiative

Ninja initiated a compliance and security project in Q2 of 2019 that includes:

- ◊ Collaboration with ***Illumant, LLC*** [ran from Q2 2019 through to Q4 2019], with objectives that include:
  - ♦ Aligning Ninja base system controls against the following baseline frameworks:
    - NIST SP 800-171r1* / NIST SP 800-53r4* **Note: Both NIST SP 800-171r1 and NIS SP 800-53r4 contain controls that map to equivalent ISO/IEC 27001 controls, andISO/IEC 27002:2013 controls*
    - US Department of Defense's DFARS 252.204-7012
  - ♦ Security and vulnerability assessments around:
    - Business Risk
    - Perimeter Security
    - Web Application Security
    - Code Development Security
    - Security Controls
    - Regulatory Compliance
    - SOC Type 2 examination readiness
  - ♦ Illumant's clients include:
    - Ellie Mae
    - EMC
    - Duke
    - Cornell
    - Stanford
    - Juniper
    - Brocade

        - Adobe
        - Synaptics
        - Bloomberg
        - eBay
        - Panasonic
        - Tyco
    - Continued vulnerability assessments with Illumant since the initial collaboration regarding our compliance and security program.
- SOC Type 2 examination with ***Schellman & Company, LLC*** [formerly *BrightLine CPAs and Associates, Inc.*] in Q1 of 2020:
    - Schellman's clients include:
        - Hess
        - Ellie Mae
        - Salesforce
        - Microsoft/Azure/Office365
        - Iron Mountain
        - Oracle
        - VMware
        - Equinix
        - SentinelOne
        - CrowdStrike
        - Savvis/CenturyLink
        - Virtustream/Dell
        - Sumo Logic
        - InfoSight
        - RSA/Dell
        - Threat Stack
        - BetterCloud
        - ThousandEyes
        - Acquia
        - Mozy/Carbonite
        - HubSpot
        - Salesloft
        - FireEye
        - Business Wire
- SOC Type 2 certification and report from ***Schellman & Company, LLC*** in Q1/Q2 of 2020

"…Are you Cyber Essentials Plus certified, and if not, are you working towards doing so?..."

No, we are not certified against the UK Government's 2014 Cyber Essentials.

No, we are not working towards it. We are SOC 2 certified against the:

- 2020 NIST 800-171 Revision 2
- 2018 NIST Cyber Security Framework Revision 1.1
- 2017 US Department of Defense DFARS 252.204-7012 https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf
- 2017 NIST 800-53 Revision 5

Because of the above compliance of NIST 800-171 r2 + NIST Cyber Security Framework r1.1 + US DoD DFARS 252.202-7012, we also meet the compliance requirements of the US Department of Defense Cybersecurity Maturity Model Certification Level 3 https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20200203.pdf

The security controls, frameworks, and certification we have chosen exceeds the UK Cyber Essentials Certification - so there is no need to go after it.

"…Has the Ninja base system had any risk assessments performed, and if so, what were the results?..."

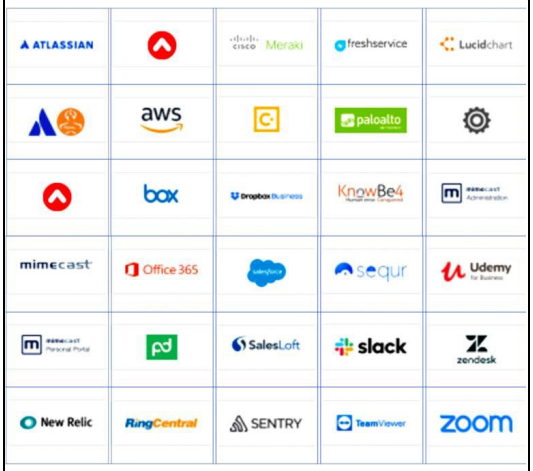
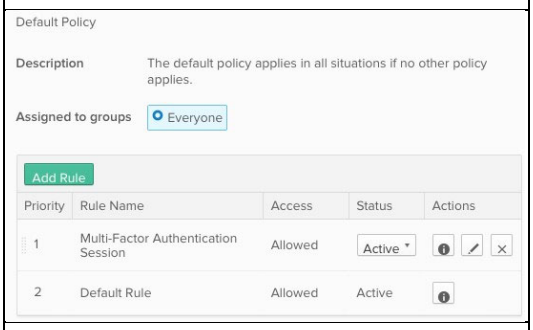
Risk & Vulnerability Assessments

Current as of ***December 2020***, the Ninja base system has received the following certifications and security vulnerability assessment scores:

- 2019 Security Vulnerability Assessments from Illumant
    - Network and Perimeter – *HIGHLY SECURE*
    - Ninja Web Service – *HIGHLY SECURE*
    - Ninja Web App – *HIGHLY SECURE*
    - Ninja Agent Code – *HIGHLY SECURE*
    - Ninja NMS Code – *HIGHLY SECURE*
- 2020 SOC 2 Certification from AICPA Accredited Schellman & Company [for 2019 year lookback]
    - First year audit and examination of the Ninja base system's security controls, as based upon these frameworks:
        - NIST Cyber Security Framework
        - U.S. Department of Defense DFARS 252.204-712
        - NIST Special Publication 800-171 Revision 1
        - NIST Special Publication 800-53 Revision 4
- 2020 Security Vulnerability Assessments from Illumant
    - Network and Perimeter – *HIGHLY SECURE*
    - Ninja Web Service – *In Progress*
    - Ninja Web App – *In Progress*
    - Ninja Agent Code – *In Progress*
    - Ninja NMS Code – *In Progress*
    - Ninja Mobile Code – *In Progress*
- 2021 SOC 2 Certification from AICPA Accredited Schellman & Company [for 2020 year lookback]
    - Currently in SOC 2 period

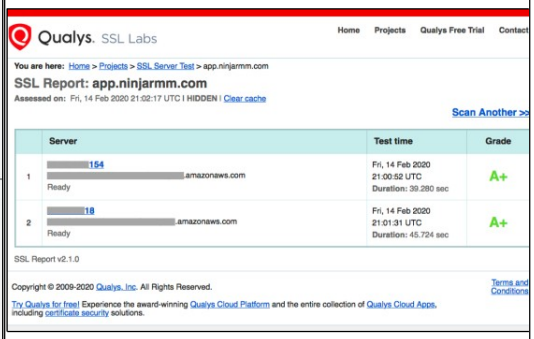
“…What security controls does the Ninja base system implement internally?…”

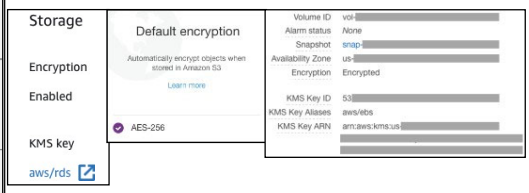
Security Controls & Implementations

<table>
<tr><th></th><th>Details/Comments</th><th>Status</th></tr>
<tr><td>SSO (Single Sign-On)</td><td>
<table>
<tr><th>NIST SP 800-171 REQUIREMENTS</th><th colspan="2">NIST SP 800-53 Relevant Security Controls</th></tr>
<tr><td colspan="3">3.5 IDENTIFICATION AND AUTHENTICATION</td></tr>
<tr><td colspan="3">Basic Security Requirements</td></tr>
<tr><td rowspan="2">3.5.1 Identify information system users, processes acting on behalf of users, or devices.
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.</td><td>IA-2</td><td>Identification and Authentication (Organizational Users)</td></tr>
<tr><td>IA-5</td><td>Authenticator Management</td></tr>
<tr><td colspan="3">Derived Security Requirements</td></tr>
<tr><td>3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.</td><td>IA-2(8)</td><td>Identification and Authentication (Organizational Users) Network Access to Privileged Accounts-Replay Resistant</td></tr>
<tr><td>IA-2(9)</td><td>Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts-Replay Resistant</td></tr>
</table>
</td><td> 
</td></tr>
<tr><td>MFA (Multi-Factor Authentication)</td><td>
<table>
<tr><th>NIST SP 800-171 REQUIREMENTS</th><th colspan="2">NIST SP 800-53 Relevant Security Controls</th></tr>
<tr><td colspan="3">3.5 IDENTIFICATION AND AUTHENTICATION</td></tr>
<tr><td colspan="3">Derived Security Requirements</td></tr>
<tr><td rowspan="3">3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.</td><td>IA-2(1)</td><td>Identification and Authentication (Organizational Users) Network Access to Privileged Accounts</td></tr>
<tr><td>IA-2(2)</td><td>Identification and Authentication (Organizational Users) Network Access to Non-Privileged Accounts</td></tr>
<tr><td>IA-2(3)</td><td>Identification and Authentication (Organizational Users) Local Access to Privileged Accounts</td></tr>
</table>
</td><td> 
</td></tr>
<tr><td>Password Complexity</td><td>
<table>
<tr><th>NIST SP 800-171 REQUIREMENTS</th><th colspan="2">NIST SP 800-53 Relevant Security Controls</th></tr>
<tr><td>3.5.6 Disable identifiers after a defined period of inactivity.</td><td>IA-4</td><td>Identifier Management</td></tr>
<tr><td>3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.</td><td>IA-5(1)</td><td>Authenticator Management Password-Based Authentication</td></tr>
</table>
</td><td> 
</td></tr>
</table>

Encryption at Rest & in Transit

NIST SP 800-171 REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*	
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	Remote Access *Protection of Confidentiality / Integrity Using Encryption*
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport *Cryptographic Protection*
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	SC-8	Transmission Confidentiality and Integrity
		SC-8(1)	Transmission Confidentiality and Integrity *Cryptographic or Alternate Physical Protection*
3.13.10	Establish and manage cryptographic keys for cryptography employed in the information system.	SC-12	Cryptographic Key Establishment and Management
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	Cryptographic Protection





"…What practices, methods, and technologies does the Ninja base system utilize to secure and protect the MSPs and the MSPs' clients?..."

Access

Ninja controls access, and segregates environments and networks with:

- ◊ a least-privilege access model
- ◊ the requirement of Multi-Factor Authentication for access authentication and authorization
- ◊ restrictions on access to source code
- ◊ restrictions on access to cloud environments
- ◊ restrictions on access to production services
- ◊ the requirement of VPN's for approved access
- ◊ logging, monitoring, auditing, and alerting of access

Remote Connectivity

Ninja further controls access by:

- ◊ limiting VPN access to only a handful of staff
- ◊ the VPN connection itself is:
  - o an IKE V2 tunnel
  - o that requires valid user/password credentials
  - o and requires a valid installation of our VPN SSL Certificate

Data Protection

Ninja protects data at rest and in transit with:

- ◊ application data transmittal encryption meeting FIPS 140-2 encryption requirements
- ◊ database/data storage encryption meeting FIPS 140-2 encryption requirements
- ◊ Ninja collects, monitors, audits, and alerts in realtime on:
  - o intrusions (whether by external origin, or internal)
  - o login failures
  - o configuration changes
  - o file alterations
  - o privilege elevations and privileged executions
  - o network connections (from undesirable sources, or to undesirable destinations)

Cloud Security

Ninja protects our cloud infrastructure with:

- ◊ Network ACLs
- ◊ Security Groups
- ◊ IP filtering and blocking on EC2 instances
- ◊ Threat Stack's Cloud Security Platform

- ◊ AWS' GuardDuty security service

"…Can you provide information regarding DDoS protection, penetration testing, network security, and source code security?..."

DDoS Protection

- The Ninja Application has been developed against the AWS Well-Architected framework and has been audited by AWS for adherence to the principles. Through the use of multiple Availability Zones and Regions, services maintain elasticity and require minimal downtime…"

- In building around the AWS Well-Architected framework, the Ninja base system follows and implements AWS best practices – including the AWS Best Practices for DDoS Resiliency whitepaper: https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.pdf

Penetration Testing

- In Q2 of 2019, Ninja base system submitted their company, corporate and cloud environments, applications, and webservices to Illumant, LLC for in-depth security and vulnerability testing. And with the major updates in 4.3 and 4.4, the Ninja base system resubmitted ourselves for security and vulnerability testing on our application code and webservices…"

- We adhere to the **AICPA SOC 2** security controls model, in which we must meet the requirements of:

    - CC4.1 - "…*COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning…"*

    - CC7.1 - "…*To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities…Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis…"*

- We comply with:

    - the **NIST 800-171** framework where:

        - *"…Requirement 3.11.2 specifies vulnerability scanning in organizational systems and applications periodically. Further, this publication also prescribes vulnerability scans when an organization identifies new vulnerabilities affecting its systems and applications…"*

        - *"…Requirement 3.12.1 specifies a periodical assessment of security controls in organizational systems for determining their effectiveness…"*
        - *"…Requirement 3.12.3 deals with continuous monitoring of security controls for ensuring the continued effectiveness of security controls…"*
        - *"…Requirement 3.14.1 focuses on identifying, reporting, and correcting system flaws in a timely manner…"*
    - the **NIST 800-53** framework where:
        - Requirement CA-8 (1) PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM – *"…The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components…"*

- We have a multi-year engagement with security firm Illumant LLC for multiple and varying penetration and security vulnerability tests/assessments throughout the year.

Network Security

- The following are several security implementations to lock down network connectivity:
    - Deploying network security devices at the perimeter of our offices that:
        - prevent unwanted ingress
        - block unnecessary egress
    - Blocking all direct backend cloud access through the use of:
        - physical firewalls
        - SDN (software-defined networking) ACLs
        - AWS Cloud-based Security Groups
        - VPN tunnels for approved backend cloud access
    - Requiring FIPS 140-2 compliant VPN tunnels for backend cloud access, where VPN credentials must:
        - be approved prior to the assignment of an account
        - use a complex password
        - include a valid Ninja base system VPN SSL certificate
    - Controlling cloud resource access by:

        - integrating authentication and authorization with a centrally administered authentication
        - and authorization system SSO backend
        - requiring Multi-Factor authentication
        - requiring complex passwords that expire
        - assigning individual API credentials that expire
        - requiring the rotation of API credentials
        - defining resource-specific policies with granular privileges
        - creating purpose-driven roles that will only include necessary policies, and denying all extraneous privileges
        - reviewing all credentials and access on a bi-annual basis
    - Blacklisting nearly 50,000 IP addresses of:
        - known malware sites
        - IP blocks affiliated with hacking organizations
        - Tor exit nodes
    - Deploying realtime monitoring, auditing, and alerting of:
        - network ingress
        - network egress
        - file alterations
        - configuration changes
        - successful and failed logins
        - command execution
        - application execution
        - privileged execution
        - OS vulnerabilities
        - software vulnerabilities

        - policy changes
        - all-new activity
        - atypical activity

- For protection of data (at rest and in transmission):
    - For data in transit - the system metrics, error logs, and other Event Log information - that is transferred between the Ninja base system Agent and the Ninja base system platform, FIPS 140- 2 compliant cryptographic modules are utilized in the TLS encryption. Specifically, the following cryptography is employed:
        - ECDHE RSA with AES128-GCM and SHA256
        - ECDHE RSA with AES128-CBC and SHA256
        - ECDHE RSA with AES128-CBC and SHA
        - ECDHE RSA with AES256-GCM and SHA384
        - ECDHE RSA with AES256-CBC and SHA384
        - ECDHE RSA with AES256-CBC and SHA

- And as per compliance with NIST CSF, NIST 800-171, and NIST 800-53 apply the following guidelines in our security controls:
    - NIST SP # 800-41, Guidelines on Firewalls and Firewall Policy
    - NIST SP # 800-44, Guidelines on Securing Public Web Servers
    - NIST SP # 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
    - NIST SP # 800-47, Security Guide for Interconnecting Information Technology Systems
    - NIST SP # 800-77, Guide to IPsec VPNs
    - NIST SP # 800-95, Guide to Secure Web Services
    - NIST SP # 800-123, Guide to General Server Security
    - NIST SP # 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise
    - NIST SP # 800-144, Guidelines on Security and Privacy in Public Cloud Computing
    - NIST SP # 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)

- NIST SP # 800-92, Guide to Computer Security Log Management
- NIST SP # 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP # 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

Source Code Security

- In Q2 of 2019, the Ninja base system submitted our company, corporate and cloud environments, applications, and webservices to Illumant, LLC for in-depth security and vulnerability testing. And with the major updates in 4.3 and 4.4, the Ninja base system resubmitted ourselves for security and vulnerability testing on our application code and webservices…
  - Allowing source code access only as defined by specific jobs duties and responsibilities within their job, e.g.
    - development and QA staff have access to user-interface code if they are working on the UI
    - development and QA staff have access to the server code if they are working on the server components
    - development and QA staff have access to the agent code if they are working on the agent components
  - Requiring executive approvals when source code access should be allowed for read-only purposes, e.g
    - for code review by an external security firm
    - for vulnerability assessment of components by an external security firm
    - for re-review or re-assessment by an external security firm
  - Revoking source code access immediately upon termination of an individual, project, or upon the conclusion of review/assessment by an external security firm
- And in compliance with the **NIST 800-53** framework:
  - Requirements:
    - SA-11 (1) DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS - The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

- SA-11 (2) DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES - The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

- SA-11 (3) DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE - The organization:

    - SA-11 (3)(a) Requires an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and

    - SA-11 (3)(b) Ensures that the independent agent is either provided with sufficient information to complete the verification process or granted the authority to obtain such information.

- SA-11 (4) DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS - The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques].

- SA-11 (5) DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING - The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [Assignment: organization-defined breadth/depth] and with [Assignment: organization-defined constraints].

- SA-11 (6) DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS - The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

- SA-11 (7) DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION - The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [Assignment: organization-defined depth of testing/evaluation].

- SA-11 (8) DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS - The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

- SA-15 (2) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS - The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

- SA-15 (3) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS - The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle].

- SA-15 (4) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS - The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [Assignment: organization-defined breadth/depth] that:

    i. SA-15 (4)(a) Uses [Assignment: organization-defined
. formation concerning impact, environment of operations, known or
. assumed threats, and acceptable risk levels];

    ii. SA-15 (4)(b) Employs [Assignment: organization-defined tools and methods]; and

    - SA-15 (4)(c) Produces evidence that meets [Assignment: organization-defined acceptance criteria].

- SA-15 (5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION - The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [Assignment: organization-defined thresholds].

- SA-15 (6) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT - The organization requires the developer of the information system, system component, or information system service

to implement an explicit process to continuously improve the development process.

- SA-15 (8) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION - The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

“…What information does the Ninja base system agent actively collect from the endpoints/systems?…”

Metrics

Health and troubleshooting information for endpoints and systems:

- ◊ CPU performance, load, and utilization
- ◊ Memory capacity, usage, and/or exhaustion
- ◊ Hard drive and I/O performance, parameters, and errors
- ◊ Network metrics, utilization, and errors
- ◊ Operating system notifications and events

Logs & Events

Troubleshooting information for software and applications:

- ◊ Error codes and messages
- ◊ Debug information
- ◊ Code snippets that are part of errors and debug information

Tickets & Requests

An end-user of an endpoint/system may be able to submit a support/helpdesk ticket to the Managed Service Provider leveraging Ninja base system services (it would not go to the Ninja base system), which would include this information as part of the ticket:

- ◊ For contact and follow-up via email: end-user’s email address
- ◊ For contact and follow-up via telephone: end-user’s office or cellular phone number

The Ninja base system App, Agent, and Platform do not collect, query, search, catalog, copy, nor in any other way access information and data that can be classified or considered PII, ePHI, Financial, Payment Card, Proprietary, Secure, or Sensitive.

The information that the Ninja base system Agent is aware of, and does capture, is intrinsic to the Microsoft Operating System, its kernel, and its Event Log subsystem. This includes any events that aid in the administration, management, and troubleshooting of an endpoint system.

Dependent on the level of verbosity or debug information needed for troubleshooting, the actual information can range based upon condition and circumstance. As the information gather originates from the endpoint systems kernel messaging and Event Log subsystem, it is important to note that the configuration of local software can impact what will be present in the information collection.

"…Who has access to our data?..."

- No one else has access to any data or information shared, transmitted, or used by the Ninja platform/web service/portal/endpoint agents/or other components
- ***AND only*** the customer/client has access to their data
- ***AND only*** when requested by, and permitted by, the customer/client, will ***Ninja*** technical support staff critical to the maintenance and functions of the Ninja platform access the customer's/client's data

"…Can the development environment, or development staff, access production?..."

Environments

Systems and services from the development environment cannot access the production environment, and conversely no system or service from the production environment can access the development environment. The environments are separated through the use of Network ACLs, Security Groups, and distinct logical networks.

Staff

The production environment can only be accessed by executive management approved staff that are required for the specific purposes of supporting our MSP partners and their support requests. Access to the production environment requires Multi-Factor Authentication and is based upon approved Roles with specific privileges and permissions.

"…What does the Ninja base system implement for cloud security?..."

AWS

Ninja deploys GuardDuty and reviews the alerts and security findings.

Threat Stack

BowBlack Ninja base system leverages Threat Stack's Cloud Security Operations (SecOps) Program.

Oversight

In realtime, Ninja base system is able to perform security auditing, monitoring, and alerting for:

- ◊ Intrusions
- ◊ Configuration changes
- ◊ File alteration (e.g., system/application executables, system/application libraries, malware, ransomware, viruses)
- ◊ Privileged execution
- ◊ Login failures
- ◊ Account lockouts

Insight

Ninja base system receives reports on trends, atypical activity or behavior, and a summary of security activity.

SecOps

Threat Stack provides a 24x7x365 Security Operations Center that reacts to and reviews alerts, escalating to staff as necessary.

"…Do you have formal documented IT change control procedures?..."

Corporate IT

Change Management: The IT Staff must document hardware and configuration changes to all network devices, servers, or other critical equipment.

Documentation: Each change must be documented in the company's approved change management system. Required information includes, but is not limited to:

- ◊ Description of the Proposed Change
- ◊ Business Case for the Change
- ◊ Scope of Users/Departments that will be Impacted
- ◊ Impact the change will have
- ◊ Implementation Procedure
- ◊ Rollback Procedure

Approval: Changes that will impact critical systems require the approval of the IT Manager, and any relevant department managers.

Communication and Scheduling: Changes that will directly impact functionality of a system (UI changes, login procedures, etc.) must be communicated to any users that will be impacted. If downtime is expected, an outage window should be communicated 24-hours in advance, unless the change is being made to correct a critical issue.

Review: Once changes are complete, the procedure should be reviewed to ensure that all steps were taken, document any deviations from the outlined steps, and to document any issues that arose, including their solutions.

Code Releases

Documentation for this is available upon request. (SA 03 v0.3 SDLC - Change Management.pdf)

"…Do you have a Computer Security Incident Response Plan and Procedure?..."

Yes – the documentation for this is available by request. (IR 01 v0.3 Incident Response.pdf)

"…Do you perform security checks (e.g., background) for each new hire?..."

Background Checks

Our background checks are standardized and search through criminal history records, while cross referencing against the National Sex Offender List. The check also screens for all prior addresses based on social security numbers to target all of the correct databases.

Vendor

Ninja base system uses the services provided by Pre-Employ.

"…Do you have a privacy breach notification procedure?..."

Notification Process

Upon discovery of any data loss, leakage, or breach, an analysis of effected partners, clients, and prospective customers will be performed. All effected parties will be contacted directly by the business managers, account managers, and sales representatives with whom they have been in regular contact. Contact may include, but is not limited to, conference call, phone call, or email.

For further information, documentation regarding this procedure is available by request. (IR 01 v0.3 Incident Response.pdf)

"…Do you have a Business Continuity Plan/Disaster Recovery Plan/backup or redundancy policy or procedure?..."

BC/DR Plan

Yes – documentation regarding this procedure is available by request. (CP 01 v0.5 BC DRP.pdf)

Data Backup Method

AWS RDS Database Snapshots

“…Describe the product of service to be provided by BowBlack Ninja base system, including the problem to be solved or business need to be fulfilled by this relationship…”

Key points are available

“…On what systems are the application(s)/data stored? (e.g., Oracle, SQL, etc.)…”

AWS RDS PostgreSQL

“…Will all data elements be encrypted at all times, including in transit and at rest?...”

Yes. No personal information is collected, but any data Ninja does collect & transmit is encrypted. Ninja base system only functions on port 443. In the event that someone forgets to use HTTPS, the Ninja base system application listens on port 80 and will redirect traffic to port 443. The data is then encrypted in transit using only Perfect-Forward-Secrecy (PFS) TLS v1.2 cryptographic modules. Data stored in the database is encrypted at rest, compliant with FIPS 140-2 requirements - and at a minimum of AES 256.

“…Does your application support IPv6?...”

No.

“…What do you do with data on your systems once the contract is terminated?...”

We delete the data from our database.

“…What does Ninja do to protect against supply chain attacks?...”

We have an information security and regulatory compliance program that is based on the following four frameworks:

- NIST CSF/Cyber Security Framework

- DoD DFARS Clause 252.204-7012
- NIST 800-171
- NIST 800-53

Controls that protect the software delivered to our customers - our endpoint Ninja agents, Ninja NMS, and Ninja Data Protection agent - include:

- We protect and secure our source code:
    - through a management approval process to allow access
    - limiting access to only the repo's required by the requestor
    - lock down the actual access through layers of security which includes MFA/2FA
    - require review and approval of code changes before they can be merged for release
- We protect and secure our build pipeline:
    - each build server is locked down with limited network connectivity
    - access to the build servers requires VPN access, where the VPN encryption is FIPS 140-2 compliant
    - each build server has antivirus/anti-malware services running with regularly updated signatures
    - each build server receives updates based on a scheduled process to minimize impactto artifact builds while ensuring security updates
- We protect and secure the development of source code:
    - developer laptops are company issued
    - developer laptops are centrally managed and can be remotely locked or remotely wiped should they be lost or stolen
    - developer laptops have antivirus/anti-malware services with regularly updated signatures
    - developers cannot singularly merge code for release to customers, they can only make requests for the merge - which then launches a process of code review and approval
- We protect and secure the software:
    - the storage locations of the software are secure, as tested and verified by an external/3rd party security firm

- the storage locations block IPs such as TOR exit nodes and known malware/hacker networks
- access, modifications, changes to the storage locations is monitored and alerted in realtime
- network connections to the storage locations from suspicious IP's is monitored and alerted in realtime
- our software is signed and authenticated using FIPS 140-2 compliant SSL Certificates

FireEye/SolarWinds/Microsoft/Federal Government hack

More information for customers with concerns that BowBlack Ninja base system could be victim of similar attack:

From SolarWinds' own SEC filing, "…the vulnerability…was introduced as a result of a compromise of the Orion software build system and was ***not present in the source code repository of the Orion products***…" From the perspective of a "supply chain attack," this would be at the final stage of delivering a fully bundled software artifact to customers as an update. The hackers knew that inserting the code at this juncture of the build pipeline was ideal, since all smoke tests, integration tests, and regression tests would have already been performed by this point.

With respect to Ninja's security practices, and those specific to our software, we have worked hard to put together a holistic and company-wide program, and have detailed our program in the attached Ninja base system Information Security & Regulatory Compliance Q1-2021 document. In particular, one of the four frameworks we implement is actually very prescriptive with respect to software development and security:

NIST 800-53 framework:

o Requirements:

§ SA-11 (1): *Developer Security Testing And Evaluation | Static Code Analysis* - The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

§ SA-11 (2): *Developer Security Testing And Evaluation | Threat And Vulnerability Analyses* - The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.

§ SA-11 (3): *Developer Security Testing And Evaluation | Independent Verification Of Assessment Plans / Evidence* - The organization:

· SA-11 (3)(a) Requires an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and

· SA-11 (3)(b) Ensures that the independent agent is either provided with sufficient information to complete the verification process or granted the authority to obtain such information.

§ SA-11 (4): *Developer Security Testing And Evaluation | Manual Code Reviews* - The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques].

§ SA-11 (5): *Developer Security Testing And Evaluation | Penetration Testing* - The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [Assignment: organization-defined breadth/depth] and with [Assignment: organization-defined constraints].

§ SA-11 (6): *Developer Security Testing And Evaluation | Attack Surface Reviews* - The organization requires the developer of the information system, system component, or information system service to perform attack surface reviews.

§ SA-11 (7): *Developer Security Testing And Evaluation | Verify Scope Of Testing / Evaluation* - The organization requires the developer of the information system, system component, or information system service to verify that the scope of security testing/evaluation provides complete coverage of required security controls at [Assignment: organization-defined depth of testing/evaluation].

§ SA-11 (8): *Developer Security Testing And Evaluation | Dynamic Code Analysis* - The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

§ SA-15 (2): *Development Process, Standards, And Tools | Security Tracking Tools* - The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process.

§ SA-15 (3): *Development Process, Standards, And Tools | Criticality Analysis* - The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle].

§ SA-15 (4): *Development Process, Standards, And Tools | Threat Modeling / Vulnerability Analysis* - The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [Assignment: organization-defined breadth/depth] that:

· SA-15 (4)(a) Uses [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];

- SA-15 (4)(b) Employs [Assignment: organization-defined tools and methods]; and
- SA-15 (4)(c) Produces evidence that meets [Assignment: organization-defined acceptance criteria].

§ SA-15 (5): *Development Process, Standards, And Tools | Attack Surface Reduction* - The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [Assignment: organization-defined thresholds].

§ SA-15 (6): *Development Process, Standards, And Tools | Continuous Improvement* - The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process.

§ SA-15 (8): *Development Process, Standards, And Tools | Reuse Of Threat / Vulnerability Information* - The organization requires the developer of the information system, system component, or information system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.

In general terms, this speaks to our security practices and implementations:

We protect and secure our source code:

o through a management approval process to allow access

o limiting access to only the repo's required by the requestor

o lock down the actual access through layers of security which includes MFA/2FA

o require review and approval of code changes before they can be merged for release

We protect and secure our build pipeline:

o each build server is locked down with limited network connectivity

o access to the build servers requires VPN access, where the VPN encryption is FIPS 140-2 compliant

o each build server has antivirus/anti-malware services running with regularly updated signatures

o each build server receives updates based on a scheduled process to minimize impact to artifact builds while ensuring security updates

o code is smoke-tested, functionally tested, integration-tested, and regression-tested

We protect and secure the development of source code:

o developer laptops are company issued

o developer laptops are centrally managed and can be remotely locked or remotely wiped should they be lost or stolen

- developer laptops have antivirus/anti-malware services with regularly updated signatures
- developers cannot singularly merge code for release to customers, they can only make requests for the merge - which then launches a process of code review and approval

We protect and secure the software:

- the storage locations of the software are secure, as tested and verified by an external/3rd party security firm
- the storage locations block IPs such as TOR exit nodes and known malware/hacker networks
- access, modifications, changes to the storage locations is monitored and alerted in real-time
- network connections to the storage locations from suspicious IP's is monitored and alerted in real-time
- our software is signed and authenticated using FIPS 140-2 compliant SSL Certificates

"…How is Secure Custom Fields / Credential Store data stored?..."

BowBlack Ninja base system implements the encryption technology of a cluster of Hardware Security Modules (HSM) in each of our environments, of which all underlying hardware has been FIPS certified:

- Certificate #3521 - September 8, 2019 (active until 1/17/2023)
- Certificate #3254 - August 2, 2018 (active until 8/1/2023)
- Certificate #2850 - February 27, 2017 (active until 2/26/2022)

These HSM clusters are used to generate unique data encryption keys (DK) for each account, which are then used to encrypt and decrypt all secure notes, secure fields, and credentials.

The HSM clusters are physically inaccessible by any Ninja employees, and further, the HSM clusters themselves have been certified as FIPS 140-2 Level 3 [meaning that even in the event of physical theft and dismantling of the hardware, there is absolutely no method by which the keys can be retrieved].

The administration, management, and access of the HSM clusters and any credentials therein requires:

- Multi-Factor Authentication via U2F/hardware tokens
- Provisioning of complementary access and services Roles
- Logging and auditing of all activity

In addition, all access to the HSM clusters, the Ninja base system cloud environments, and the SaaS services are monitored 24x7x365 with a third-party Security Operations Center (SOC) partner.

For RMM platform, Ninja base system has brought forward the same philosophy on cyber-security by:

- Requiring BowBlack Ninja base system users to configure MFA by default
- Requiring MFA re-authentication for escalated privilege activities
- Requiring endpoint validation/approval
- Implementing endpoint identification and fingerprinting

- Implementing endpoint clone detection
- as well as other security-conscious/least-privilege-access implementations throughout