



We take care of your network with a dedicated, experienced team, managing our enhanced network security programs for the ultimate Identity and Access Controls | Change, Vulnerability, Log/Event and Vendor Risk Management | Application, Physical, Endpoint, and Physical and People/HR Security | Governance + Compliance, and Disaster Recovery along with a host of additional programs we use to take care of your network.

## YOUR SECURITY COMPLIANCE STACK

**Kaseya VSA** (RMM)

**SentinelOne** [Supported by 24x7 SOC] (Next Gen antivirus)

**Cisco Umbrella** (Cloud Security)

**Cove Backup Manager** [Formerly N-able] (Server Backups)

**Connectwise Control** (Remote Control) *\*as requested by client*

**Datto SaaS Protection** (SAAS Backups)

**Duo Authentication** (2FA) *\*on all admin account and as requested by client.*

---

Industry leading protection, detection, and response

### APPLICATIONS BEING DEPLOYED TO YOUR ENVIRONMENT






- **Kaseya VSA** is a remote monitoring and management (RMM) tool that allows IT professionals to remotely monitor and manage devices and systems across multiple locations. With Kaseya VSA, IT teams can automate tasks, manage patches and updates, and provide remote support to their clients or end-users.
- **Cisco Umbrella** Flexible, cloud-delivered security. It combines multiple security functions into one solution, to extend data protection to devices, remote users, and distributed locations anywhere.
- **Cove** (formerly N-able) Backup Manager is a server backup solution that enables IT teams to easily back up and restore critical data and applications. With Cove Backup Manager, IT professionals can perform automated backups, monitor backup status, and quickly recover lost data to minimize downtime.
- **Connectwise Control** is a remote control tool that enables IT professionals to securely access and control remote devices from anywhere. With Connectwise Control, IT teams can remotely troubleshoot and resolve issues, provide remote support, and collaborate with team members in real-time.
- **Datto SaaS Protection** is a backup solution designed specifically for Software as a Service (SaaS) applications such as Microsoft 365 and Google Workspace. With Datto SaaS Protection, businesses can easily protect critical data and applications in the cloud and recover lost data quickly and easily.
- **Duo Authentication** is a two-factor authentication (2FA) solution that adds an additional layer of security to online accounts and applications. With Duo Authentication, users must provide a second form of authentication, such as a biometric scan or a code from a mobile device, to access their accounts or applications.
- **SentinelOne** An autonomous platform that protects against all types of attacks, online or offline, from commodity malware to sophisticated APT attacks. The breadth of Singularity XDR's capabilities (validation from MITRE, Gartner, Forrester, etc) checks all the boxes of antivirus solutions made for the enterprise. SentinelOne works as a complete replacement for legacy antivirus, next-gen antivirus, and EDR solutions, too with the benefit of 24x7 support from a dedicated Security Operations Center (SOC).

## WE TAKE OUR OWN SECURITY SERIOUSLY.

Braver protects ourselves internally by taking a comprehensive approach to network security, encompassing the five key elements of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. We regularly conduct risk assessments and vulnerability scans to understand our network's weaknesses and areas of concern.



Our security stack is continuously updated to stay ahead of the latest threats and vulnerabilities. We also implement regular security audits and assessments to identify and address any potential weaknesses in our system. With our security stack in place, we are confident in our ability to safeguard our network and protect the sensitive information and data of our users and clients.

| <br><b>IDENTIFY</b> | <br><b>PROTECT</b> | <br><b>DETECT</b> | <br><b>RESPOND</b> | <br><b>RECOVER</b>                               |
|--|---|--|---|---|
| Remote Monitoring and Management (RMM)   | Antivirus   Anti-Spam   Anti-Phishing   | Endpoint Detection and Response (EDR) with 24x7 SOC  | 24x7 Security Operations Centers (SOC)  | Communication Protocols- (Incidents are worked by engineers, Communicated by Service Delivery Managers)                             |
| Network/ Systems Discovery +   | Background Checks + Security Training for all New Hires   | Realtime SEIM monitored internally and by External MSSP  | Security Orchestration and Response (SOAR)  | Azure Backup + External BDR of all servers hourly   |
| Open DNS for DNS filtering   | System Hardening  | Network Scanning Identifying potential vulnerabilities in the system.                              | Developing a plan to address those vulnerabilities.   | Monthly Testing   Monthly Off site Spin up  |
| Regularly reviewing and updating the system's security controls to ensure they remain effective.     | Network Segmentation  | Internal + External Vulnerability Scanning by External MSSP  | Comprehensive Incident response plan  | Incident Analysis (Post incident review, Root cause analysis)   |
| Documentation System   | Implementing security controls to reduce the system's attack surface.                               | Yearly Internal penetration testing by External MSSP   | Triage Process - Ticket prioritization system   | Investigation (Identify root causes)  |
|  | Developing a plan to address those vulnerabilities.   | SaaS Monitoring  |   | Incident Documentation (Documentation of incidents, response actions, lessons learned, and recommendations for future improvements) |
|  | MFA   2FA on all AD Accounts  | Threat Hunting   |   |   |

Our network is protected by a comprehensive security stack that includes multiple layers of defense to ensure the utmost protection against potential cyber threats.

Our approach to network security is based on the principles of the NIST Cybersecurity Framework, and we are committed to staying up-to-date on the latest threats and vulnerabilities to ensure the safety and security of our network.



## BRAVER SECURITY POLICY OVERVIEW

Framework for managing security risks.

The Braver security tech stack is designed to provide a robust and comprehensive approach to ensuring the security of our systems and data. Our security policy is aimed at protecting the confidentiality, integrity, and availability of our systems and data, as well as ensuring the compliance of our operations with applicable regulations and standards.

**The following are key components of The Braver security policy:**

### INFORMATION SECURITY MANAGEMENT:

**Scope:** This policy covers the implementation of our information security management system (ISMS) based on the ISO 27001 standard.

**Policy outline:** We will regularly assess the risks to our systems and data, implement appropriate controls, and continually monitor and improve our security posture.

- Conduct regular risk assessments to identify potential vulnerabilities and threats.
- Implement security controls based on the ISO 27001 standard, such as access controls, encryption, and incident management procedures
- Assign responsibility for the implementation and maintenance of the ISMS to a dedicated team or individual
- Continuously monitor and improve the effectiveness of the ISMS through regular audits and reviews

### ACCESS CONTROLS:

**Scope:** This policy covers the implementation of access controls to ensure that only authorized personnel have access to our systems and data.

**Policy outline:** We will implement role-based access control (RBAC), two-factor authentication (2FA), and access logs to ensure the confidentiality, integrity, and availability of our systems and data.

- Implement role-based access control (RBAC) to limit access to only authorized personnel
- Implement two-factor authentication (2FA) for all privileged accounts
- Implement access logs to monitor and detect any unauthorized access attempts
- Regularly review access control policies and procedures to ensure their effectiveness

### DATA PROTECTION:

**Scope:** This policy covers the implementation of data protection controls to ensure the confidentiality, integrity, and availability of our data.

**Policy outline:** We will implement encryption, data backup and recovery, and data retention policies to protect our data from unauthorized access, loss, or damage.

- Implement encryption for sensitive data at rest and in transit
- Implement data backup and recovery procedures to ensure the availability of critical data
- Implement data retention policies to ensure the secure disposal of data when no longer needed
- Conduct regular audits and reviews of data protection policies and procedures to ensure their effectiveness

### NETWORK SECURITY:

**Scope:** This policy covers the implementation of network security controls to protect our systems and data from unauthorized access and attacks.

**Policy outline:** We will implement firewalls, intrusion detection and prevention systems (IDPS), and vulnerability

management to detect and prevent unauthorized access and attacks.

- Implement firewalls to prevent unauthorized access to our network
- Implement intrusion detection and prevention systems (IDPS) to detect and respond to potential attacks
- Regularly scan and assess our network for vulnerabilities and implement appropriate patches and updates
- Regularly review and update network security policies and procedures to ensure their effectiveness

## INCIDENT MANAGEMENT:

**Scope:** This policy covers the implementation of incident management procedures to ensure timely detection, response, and resolution of security incidents.

**Policy outline:** We will implement incident reporting, investigation, and escalation procedures to ensure that we can respond effectively to security incidents and minimize their impact.

- Implement incident reporting procedures to ensure timely detection and response to security incidents
- Assign responsibility for incident management to a dedicated team or individual
- Implement incident investigation and escalation procedures to ensure that incidents are resolved effectively
- Conduct regular reviews and updates to incident management policies and procedures to ensure their effectiveness

## THIRD-PARTY SECURITY:

**Scope:** This policy covers the implementation of third-party security controls to ensure the security of our systems and data when working with external vendors and partners.

**Policy outline:** We will conduct due diligence, security assessments, and contractual requirements to ensure that our third-party vendors and partners meet our security standards.

- Conduct due diligence on third-party vendors and partners to ensure they meet our security standards
- Implement contractual requirements for third-party vendors and partners to ensure they maintain appropriate security controls
- Regularly review and assess the security of our third-party vendors and partners
- Conduct regular audits and reviews of third-party security policies and procedures to ensure their effectiveness

## COMPLIANCE:

**Scope:** This policy covers the compliance with applicable regulations and standards, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).

**Policy outline:** We will ensure compliance with applicable regulations and standards, implement appropriate controls, and conduct regular audits to ensure that we remain compliant.

- Ensure compliance with applicable regulations and standards, such as the GDPR and PCI DSS
- Implement appropriate controls to ensure compliance with regulations and standards
- Conduct regular audits and reviews to ensure compliance is maintained
- Assign responsibility for compliance to a dedicated team or individual

## BACKUP AND DISASTER RECOVERY:

**Scope:** This policy covers the implementation of backup and disaster recovery procedures to ensure the availability and recoverability of our systems and data in the event of a disaster or unexpected downtime.

**Policy outline:** We will implement regular backups, offsite storage, and testing of our backup and recovery procedures, and develop a disaster recovery plan to ensure the effective restoration of our critical business functions, data, and applications.

- Regularly backup critical systems and data and store backups offsite
- Implement disaster recovery procedures to ensure the timely restoration of critical business functions, data, and applications in the event of a disaster or unexpected downtime
- Conduct regular testing of backup and disaster recovery procedures to ensure their effectiveness
- Regularly review and update backup and disaster recovery policies and procedures to ensure their effectiveness

