ushur

Securing Your Digital Transformation

Ushur Security Framework

Table of Contents

Introduction

> Security is always excessive until it's not enough.
>
> Robbie Sinclair, Head of Security, Country Energy, NSW Australia

That's a motto we live by. The cost of known data breaches since 2012 far exceeds $50 billion, according to a study by CGI and Oxford Economics.

As businesses, solutions, and customers rapidly migrate to the Cloud, organizations are starting to reap the tangible benefits of digital transformation. The sheer number of expert-designed, collaborative platforms is a boon for innovation and new growth, and businesses that have traditionally operated in siloed, brick and mortar facilities stand to gain the most from this bonanza.

For a business that's evaluating a cutting-edge technology, how a solution provider protects and secures information needs to be answered transparently, coherently, and completely. Otherwise, the risk of a major data breach is only a matter of when, not if.

Of equal importance is a company's ability to ensure privacy. Given strict and diverse regulatory frameworks, it's imperative for a solution provider to demonstrate future-proofed and comprehensive privacy protocols.

With the emergence of the Cloud, the narrative emphasis has been on cybersecurity, but secured data demands a turnkey, future-proofed approach.

There are three key components of any good information security plan:

- Cyber Hygiene
- Physical Security
- Incident Management

Introduction

Ushur is committed to providing the highest level of service for each element, and these will be addressed throughout this document in terms of security and privacy design. Our complete solutions for intelligent automation attract and retain Global 2000 enterprises because we innately understand security and reflect that in our people, processes, and technology.

A turnkey security and privacy plan seamlessly integrates proactive, adaptive, and reactive security models. In this overview of our security framework, we discuss both the challenges of delivering security and our comprehensive prevention, detection, mitigation, and management strategy, broadly covering the following topics:

- Digital Security
- Organizational Security
- Vendor and Third-party Security, Privacy, & Compliance Management

While we intend to provide a high-level view in this document, we know that the devil is in the details; we've added resources to allow you to deep-dive on salient topics.

Infrastructure Security

If your security is reactive, you've already lost. Luckily, as experts in workflow automation, we believe and invest in proactivity. Several of our core partners are insurance giants whose focus on and need for security and safeguarding customer data such as personally identifiable information (PII) is legendary.

Ushur uses a **360° architecture** to head-off potential violations, enforce strict policies, prepare and protect information, and actively perform higher-level analysis for sensitive areas.

In the Infrastructure Security space, we often reference these broad categories of prevention, monitoring, encryption, and detection in the context of Gates. At each Gate, we have developed extensive protocols to ensure compliance with our data security and integrity needs.

This is a flanking architecture: it protects the Entry Gate from potential violations; enforces policies at the Exit Gate, where it prevents violations; prepares and protects information at the South Gate, where there is potential for security penetrations; and notifies the North Gate for higher-level analysis and further enforcement of security policies.

The diagram below lays out this architecture visually, and we continuously upgrade our policies and processes with the latest industry recommendations.

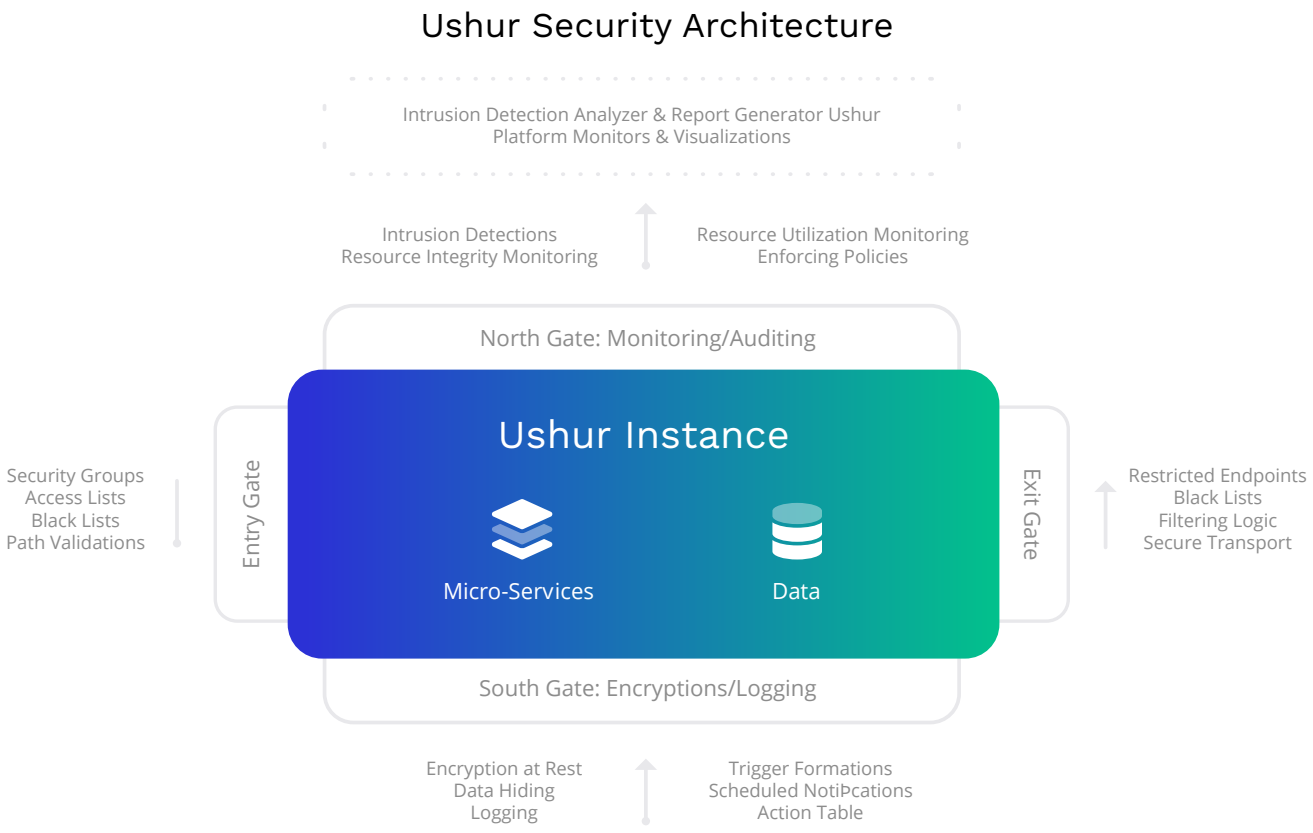

Figure 1: Ushur's 360° architecture

Infrastructure Security

At Ushur, our approach is grounded in a least privilege management design. We leverage Cloud tools such as Security Groups and Access Lists and granularly enforce our own Access Lists, Deny Lists, and other validations via proxies and gateway-level enforcers. We employ remote identity validations and path validations (i.e. only expected paths are permitted into the system). The rate of incoming traffic can be carefully controlled and regulated, at the per-remote-endpoint (integrated endpoint on a per-enterprise) level.

For Data Loss Prevention (DLP), we monitor internal resources including files for integrity, log-file sizes for overflows, delay monitoring from logs, and platform latencies. Internal agents run on behalf of external monitors, such as intrusion detection agents and resource monitoring agents, to ensure that any sort of intrusion is swiftly dealt with. When sending outbound traffic, we enforce restrictions on specific endpoints, regulate outgoing traffic, operate Deny Lists, and apply the appropriate filters on endpoints and content, imposing secure transport.

Vital parameters are incessantly monitored to ensure that illegitimate access is preempted.

Network Security

Network threats evolve rapidly, and we have designed a robust and adaptive strategy. Our network security and monitoring protocols are designed to play multifaceted offense and defense and rely on industry-leading implementation, segmentation, and auditing.

We use industry-leading tools to protect our network from unauthorized access. Using VPN (Virtual Private Network) techniques, we can ensure point-to-point and site-to-site connection.

Segmentation is a critical facet of our approach to data protection. Our systems are segmented into separate networks to silo and protect sensitive data. Systems supporting testing and development are hosted separately from systems supporting production infrastructure. We have dedicated resources for each customer, and only internal tools networks have restricted and limited access to these customer resources for deployment and monitoring.

Adversaries don't sleep, and neither do we. We run extensive Cloud infrastructure security auditing regularly to identify and address activity before it becomes harmful. When we notice abnormal or suspicious activity in our production environment, our system issues rapid diagnostic notifications. Vital parameters are incessantly monitored to ensure that illegitimate access is preempted.

Network Redundancy

When a business loses even momentary access to critical information, the cost can be incalculable. We employ a distributed architecture to shield our services and ultimately clients from the effects of potential server failures in our Cloud infrastructure. We ensure cross-region replication and have active-passive availability within the platform. This redundancy ensures partners can access services and carry out their mission-critical activities without any interruption or downtime.

Distributed Denial of Services (DDoS) Prevention

DDoS (Distributed Denial of Services) attacks are evolving to include sophisticated components, and aggressive prevention is crucial. When successfully executed, these attacks are expensive to organizations and can destroy credibility. We actively prevent DDoS attacks on our servers, mitigating disruptions and bad traffic in real-time with AWS Shield. AWS Shield defends against network and transport layer DDoS attacks that target partner websites and applications. With our DDoS prevention scheme, partners and customers can be confident that their critical information remains highly available.

Intrusion Detection and Prevention

Our cloud provider (AWS[1]) gives us best-in-class security features that we deploy for our intrusion detection at a particular host-level. AWS allows us to fine-grain identity and access controls in real-time; with increasing security automation, we are able to eliminate human error vectors, preemptively. Finally, AWS enables automatic encryption at the physical layer, with further encryption layers available.

In conjunction, we use an enterprise-grade network intrusion detection service (IDS) to monitor our infrastructure. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged and alerts are triggered using in-house tools. In response to the evolving nature of threats, we conduct operating system-level hardening and proactively service our host machine operating systems based on vulnerability analysis reports.

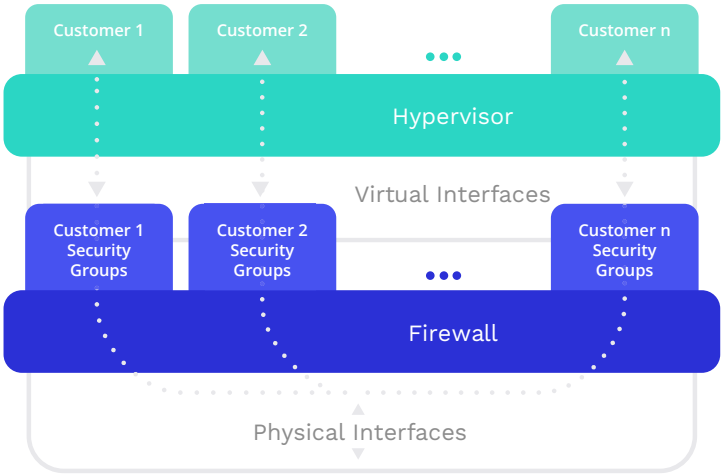

Figure 2: Amazon EC2 multiple layers of security

1 Amazon Web Services

Data Security

Secure by Design

Data is king, and Ushur was built to handle data in all forms. Whether structured or unstructured, this is the core of the workflow automation we enable, and we explicitly strive to keep customer data secure and private.

Our change management policy guides the addition of any new features and updates. This policy ensures all updates and amendments to our software made within the application are authorized before incorporation into production. Internal controls such as our Software Development Life Cycle (SDLC) and Secure Product Life Cycle (SPLC) mandates adherence to secure coding and product design guidelines; we screen all code and product changes for potential security issues with our code analyzer tools, vulnerability scanners, and extensive manual review processes.

Data Protection

Your service data is yours, and we ensure that a customer's service data is not accessible to another; each customer's service data is siloed, using a secure set of protocols.

Our security and privacy framework assists customers in maintaining compliance with data protection laws and regulations, including the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA). Adherence to these two regulatory schemes, in particular, gives Ushur partners the ability to freely and confidently conduct business in lucrative, highly-regulated markets.

Ushur has implemented the latest recommended procedures in response to these important legislative directives. For each new product and enhancement, we proactively apply the Data Protection by Design principles, a key component of GDPR requirements. Additionally, our innately transparent and needs-based data processing, secure data transfers with vetted third-parties, and commitment to proactively fighting potential breaches allow us to be nimble as the laws are amended and made more stringent.

Ushur prioritizes information security, and we have **baked in procedures to securely process customer communications, end-to-end**. Protecting end-user data guides how we send outbound emails to the end-user.

To learn more about how Ushur protects our EU-center partners and their customer data, please reference visit "Ushur GDPR-Compliant End-End Security" by reaching us at dpo@ushur.com.

Anonymization

To give our customers complete confidence, Ushur leads the industry by creating innovative tools for anonymization. With our benchmark of conservative, transparent, and delimited processing, Ushur enables the redaction of any personally identifiable information (PII) and sensitive personal information (SPI) shared with the platform, such as contact information, home addresses, etc., **by transforming its value into a pattern that does not contain comprehensible data, before being transferred to Ushur servers**.

Encryption

Encryption can occur at different layers and times, and Ushur recognizes and supports the fundamental importance of maintaining the appropriate encryption regardless of where your data is. We continuously update our encryption best practices, to defend your information in the face of evolving threats.

In-transit: By using robust encryption protocols, each piece of customer data is secured as it's transferred to our servers. This approach guarantees a secure connection that allows the authentication of all parties associated with the connection. The HTTP Strict Transport Security (HSTS) is enabled in all our web connections, requiring modern browsers to only support encrypted connections.

At-rest: We encrypt customer data at-rest through the use of industry standard algorithms with proactive key maintenance and rotation policies. Layers of encryption include at the application level as well as at the disk level. Ushur provides additional layers of security by encrypting the data encryption keys using main keys. The main keys and data encryption keys are physically separated and stored in different servers with secured access, something we will cover in detail in the Physical Security section of this report (Pg. 13). Our encryption at-rest is carefully updated whenever regulations are amended.

Administrative Access

Bad actors view access as a weak link to probe and exploit, and, ironically, gain access by facsimile. Therefore, smart administrative access implementation is the hallmark of a strong security framework.

At Ushur, access to non-development environments and to data is maintained through a central directory and authenticated via a combination of methods including multi-factor authentication. Furthermore, we facilitate access through a dedicated private network with stricter rules and hardened devices. All operations are logged and regularly audited, allowing us to detect aberrant access patterns with alacrity.

Operational Security & Reliability

Operational security relies on dedicated systems and disciplined implementation and maintenance. Proactivity, once again, is the keystone. We monitor aggressively and perform frequent and regular vulnerability audits. Based on our experience working with large enterprise-scale businesses, we've developed a full-fledged incident management ecosystem to address threats in real-time. In operational security, redundancy is a friend, and we ensure your consistent, timely access to your data through our rugged disaster recovery and business continuity program.

Logging and Monitoring

We continuously monitor and analyze information gathered from services & internal traffic in our network. We record this information in the form of event logs, fault logs, audit logs, operator logs, and administrator logs. These logs are examined to detect anomalies such as attempts to access customer data or unusual activity in accounts. To protect log integrity, we store these logs in a secure server isolated from full system access and manage access control centrally, while ensuring its ready availability.

Audits for Vulnerability

Audit trails, electronic records that chronologically catalog events, provide support documentation and history that is used to authenticate operations and mitigate threats. Robust and accessible historical data allows Ushur to quickly red-flag abnormal changes, **allowing us to pivot from defense to offense against cyber-threats, security breaches, data corruption, and other information misuse**.

We regularly perform audit exercises in conjunction with authorized third-party vendors and publish regular reports. Our teams use in-house tools to perform extensive and routine automated and manual penetration testing. As soon as we identify a vulnerability requiring remediation, it's logged and triaged according to severity. The vulnerability is then assigned to the appropriate engineering team to redress.

Operational Security & Reliability

Incident Management

At Ushur, we've built and followed clear guidelines and procedures for handling different categories of incidents, including security events. Immediate corrective actions are taken according to the severity of each incident. We take incident ownership seriously, and our experience serving enterprise partners allows us to operate our incident management playbook at scale. For more information, please reference "Ushur Solution Document, v1.3" by emailing us at dpo@ushur.com.

Based on our experience working with large enterprise-scale businesses, we've developed a full-fledged incident management ecosystem to address threats in real-time.

We strive to intercept and remedy before we have an incident. Our high commitment to partner satisfaction means that the executive management team is closely involved in identifying corrective actions and future-proofing our solutions.

Disaster recovery and Business Continuity

Application data is housed on resilient storage that is replicated across different availability zones. If the primary availability zone goes down, the secondary availability zone takes over automatically, and your operations are carried out smoothly with negligible loss of time. Our customer platform **applications are highly available at any given moment with minimal downtime**. Cross-region availability is also baked-in in the event of an unforeseen disaster.

Organizational Security

Security starts with us - who we are and how we see the world. Security hygiene comprises the practices that members of an organization undertake to ensure that they are not the inadvertent source of a security breach. Decades after email was born, email phishing is still the Achilles heel of enterprises big and small, and Ushur invests heavily in organizational security education.

The integrity of partner data is mission-critical to our service, and we also make organizational security training a priority with our clients.

Security Awareness

Ushur starts protecting partner data at the human level. Every Ushur team member undergoes thorough background checks, vetted by expert external agencies. Team members then receive extensive security training as part of their onboarding. We keep security top-of-mind with frequent refresher courses on the latest best-practices, along with certifications for the appropriate individuals.

Endpoint Security

When enterprises lack a cohesive work product plan, preventing data breaches is like catching sand in a sieve. At Ushur, our work infrastructure has been designed to maximize security.

We use industry-leading Intercept X Endpoint by Sophos for enterprise-grade endpoint protection. Our workstations run continually updated OS versions and are configured with the latest antivirus software. Every Ushur device is configured internally to comply with our stringent security standards. All work product infrastructure is routinely monitored, updated, and serviced by Ushur's security team. This work product plan extends to how we communicate and conduct business, prioritizing customer information integrity.

The integrity of partner data is mission-critical to our service, and we also make organizational security training a priority with our clients.

Physical Security

On-Premises Access and Monitoring

Physical security is proactive security. The best cyber-security can be undone by poor physical security implementation. An ad hoc and outdated system of cameras, badge scanners, alarms, and security patrols describes how most high-tech businesses are protecting their physical spaces. And 'ad hoc' in security parlance is bad news.

At Ushur, **our physical security is an integral and integrated component of our security framework**. Only authorized personnel have access to office premises, through biometric controls. In theme with our business, an automated visitor log is maintained in perpetuity for each visitor, guest, and maintenance staff member. In addition to access control, video surveillance of the premises ensures our team can respond to physical breaches rapidly. We maintain historical records for sensitive areas.

Compliances and Certifications

Ushur is dedicated to providing our customers with the best-in-class security, compliance, data protection, and platform backed by robust, thoughtfully executed infrastructure. We maintain rigorous internal security practices and regularly engage third-party external experts to test our network security, routinely refining our technical, administrative, and physical safeguards.

Given our strong commitment to security, Ushur has been certified as certified as **SOC 2 Type 2-compliant.** SOC 2 is an auditing procedure that ensures service providers securely manage data to protect the interests of client organizations and the privacy of end users. Developed by the American Institute of CPAs (AICPA), SOC 2 defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality and privacy. Type II details the operational effectiveness of those systems. We've also sought and achieved compliance with standards across a diverse range of industries, reflecting the clients we serve.

In addition to our GDPR and CPCA compliance, as outlined in Data Protection (Pg. 7), we are TCPA- and HIPAA-compliant. Our HIPAA compliance in particular speaks to our deep commitment to privacy; as healthcare partners know, HIPAA is exceedingly stringent as medical data is sensitive and deeply personal. In addition to allowing us to serve clients in the healthcare space, our adherence to HIPAA informs how we protect data for all the customers we serve — zealously.

Conclusion

The utility of the Ushur platform implicitly and explicitly demands the security of our customer data; your data sanctity is paramount to us. We reaffirm our deep commitment to housing customer information and record access with the highest standards of security governance. Please reach out to our Information Security Office Team at iso@ushur.com, if you have any queries or questions that need clarification. We are here for you.

For general security concerns please contact iso@ushur.com

For specific questions on data protection & privacy please contact dpo@ushur.com

References

1. Ushur Solution Document, v1.3
2. Ushur Channel Security - Invisible App & Email, v1.4
3. Ushur GDPR-Compliant End-End Security
4. AWS Security Whitepaper
5. Cyber Breaches Cause Permanent Damage to Share Values
6. Remote Endpoint: Advanced Routing Configuration
7. Amazon Web Services Security
8. How AWS Shield Works
9. AWS Security Hub
10. AlertLogic Network Intrusion Detection System (IDS)
11. Sophos Intercept X Endpoint
12. Cloud Security Resources
13. General Data Protection Regulation
14. Health Insurance Portability and Accountability Act
15. California Consumer Privacy Act
16. Ushur SOC 2 Type 2 Certification
17. Preparing for Physical and Cybersecurity Convergence
18. Audit Trails: Managing the Who, What, and When of Business Transactions