

Protected business

SecureFabric SME

No one can stop zero-day malware from entering your network, but Liquid's SecureFabric can prevent it from causing any damage.

Why the need for SecureFabric?

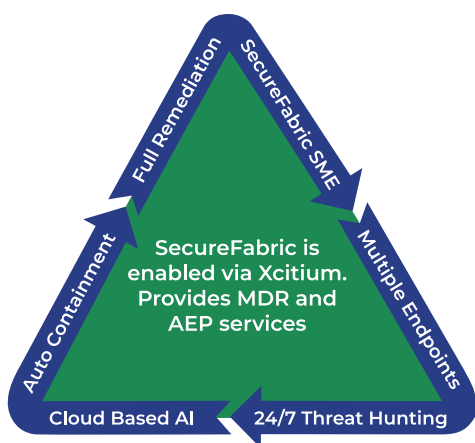
It is a risk mitigation measure – prevents multiple types of cyber-attacks such as intrusions attempts and enables the detection of events that may lead to compromise of your private network and assets.

Compliance Requirement – 24 x 7 x 365 monitoring is needed to align with industry cyber security standards such as ISO27001 or NIST CSF. The same is also required to comply with legislation, regulatory requirements, or for compliance to some industry business practices such as PCI DSS.

Address Cyber Security Resiliency – Enables situational awareness enabled via threat intelligence and actionable reporting, leading to proactive and pre-emptive response rather than being reactive.

SecureFabric Benefits

- Centralised Event and Incident Monitoring 24 x 7 x 365
- Event Logging and Correlation
- Threat Intelligence and Actionable Reporting
- Event Analysis and Incident Response
- Advanced Endpoint Protection and Endpoint Detection and Response (EDR)
- Managed Detection and Response (MDR)
- Incident Management and related Ticketing
- Expertise when in need, including Incident Response
- Increased Threat and Risk Mitigation
- Increased Compliance Adherence



SecureFabric Features

- Advanced Endpoint Protection
- Endpoint Detection and Response
- Managed Detection and Response
- Network Intrusion Detection sensors
- Always-on 24 x 7 x 365 monitoring
- Real-time remediation on endpoints
- Reduce attack dwell time to seconds
- Co-delivery between the Liquid team and Xcitium Security Experts at the backend

Protected business

SecureFabric SME

Threats mitigated by SecureFabric

- Lack of monitoring equals lack of threat visibility
- Organisations that don't have sufficient monitoring lacks visibility and situational awareness, making them vulnerable to compromise and exploitation.
- Lack of timeous threat identification leads to inadequate management and control thereof
- Inadequate threat identification leaves organisations vulnerable to attacks as they tend to be reactive rather than pro-active.
- Lack of detection leads to unauthorized activities
- Organisations without appropriate detection and response solutions are vulnerable to lateral attacks within the network as these are typically not even noticed.
- No threat intelligence and situational awareness equals reactive rather than proactive response
- Actionable intelligence in the form of alerts, dashboards and reporting is needed to enable proactive and even pre-emptive action.
- Inadequate response leads to increased recovery costs
- Too many organisations find out during an incident that their response processes are inadequate, leading to irrecoverable damage and costs.
- Recurring incidents are likely without effective incident processes and in particular review of previous incidents
- Incidents tends to re-occur if processes are immature.
- Lack of expertise
- Organisations that don't have the required skill and capacity to deal with Cyber Security threats are vulnerable and compromised at some point.

Included in the three(3) LIT SecureFabric Small Medium Enterprise(SME) Service Options

Advanced Endpoint Protection	Managed Detection and Response Plus	Managed Detection and Response Advanced
<ul style="list-style-type: none"> • Xcitium Advanced Endpoint Protection includes Zero Trust Isolation and Containment • Malware & Ransomware Protection (100%) • Valkyrie Cloud File Verdict Analytics and Support 	<ul style="list-style-type: none"> • 24/7/365 Monitoring and Alerting • EDR Data Collection and Analysis (document malware actions) • Attack Surface Reduction • Endpoint Vulnerability Identification and Patch Recommendations • Endpoint Remediation Support • Profile & Policy Management • Endpoint Threat Content Updates • Simple Rule Development • Weekly/Monthly Reporting • Quarterly Review Meetings 	<ul style="list-style-type: none"> • Threat Hunting • Custom Rule Development and Support • Digital Forensics/Incident Response <p>Network MDR</p> <ul style="list-style-type: none"> • Xcitium Network Sensor • Network Log Traffic Visibility • Intrusion Detection • Additional Log Source - Win Events, Linux logs, Firewall logs • Cloud Monitoring - AWS Cloudtrail • Office 365 Monitoring

Note: Advanced Endpoint Protection(AEP) is part of our Managed Security Services

How to get the service

Visits our site cybersecbu@liquid.tech



Protected business **SecureFabric SME**

Service options

Our offering is enabled via Xcitium, white-labelled and co-managed by the Liquid team for our customers, and is referred to as SecureFabric.

The LIT SecureFabric SME service options are:

SecureFabric SME AEP

– Advanced Endpoint Protection(AEP), includes advance endpoint security and patented malware containment

SecureFabric SME MDR Plus

– AEP + Endpoint Detection and Response(EDR)/Managed Detection and Response(MDR)

SecureFabric SME MDR Advanced

– AEP + EDR + MDR + intrusion Detection Systems (IDS) + Deep Packet Inspectioin (DPI) & additional security event log sources, e.g. firewall.