Elisity® Cognitive Trust™

Accelerate your Cybersecurity Maturity Model Certification journey (CMMC 2.0)

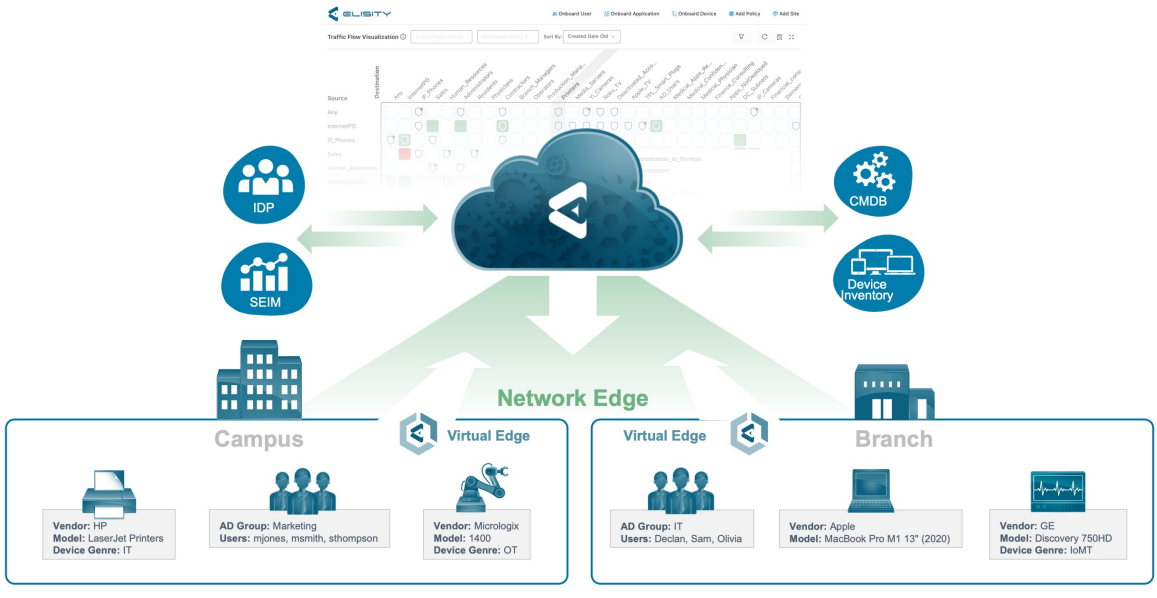
The Zero Trust Access platform for the Defense Industrial Base

- Reach your required CMMC level faster with our solution and support
- Manage risk effectively and efficiently to address the threats of ransomware attacks, advanced persistent threats, and insider threats
- Easy to deploy and operate, with zero friction implementation over existing infrastructure

Elisity Cognitive Trust delivers intelligent Zero Trust Access for the defense industrial base (DIB) to safeguard and protect federal contract information (FCI) and controlled unclassified information (CUI) in your network and datacenter. The capabilities of our solution directly enable nearly half of currently published CMMC 2.0 practices, helping DIB companies reach their required CMMC level faster to reduce the risk posed by advanced persistent threats and ransomware attacks.

The platform is delivered as a cloud-based service and leverages existing access-layer switching infrastructure as Policy Enforcement Nodes, eliminating the need for Network Access Control solutions and other rigid network security constructs that fail to provide any context around the identity of assets on the network.

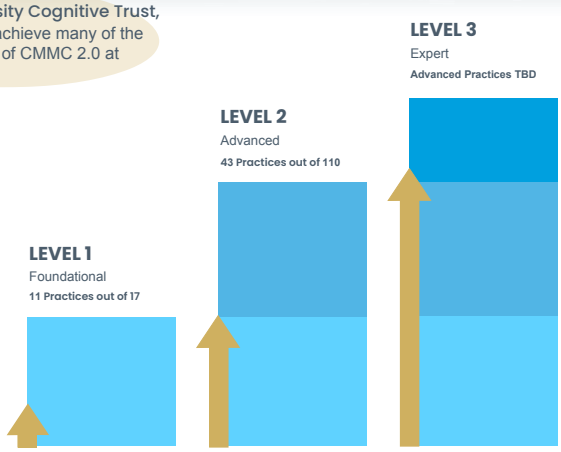
Secure access for employees, third party vendors, devices, and applications, is achieved with a simple, frictionless, and ubiquitous solution. Elisity Cognitive Trust leverages zero trust network access (ZTNA) and software defined perimeter capabilities (SDP), and integrates with leading identity providers (IDP) in the cloud or on-premise to enable macro, micro, and transactional segmentation, protecting FCI and CUI from unauthorized access from outside and inside the network. Access policies are adaptive, following users, devices, and applications anywhere they are attached to the network.



Cloud-delivered | Visibility and Classification | Identity-based Policy Graph | Realtime Policy Distribution

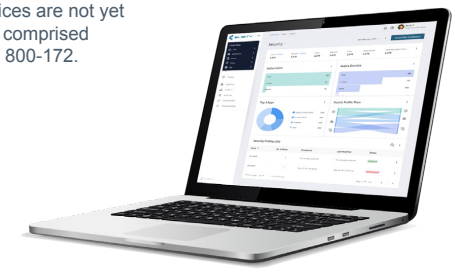
Why Elisity Cognitive Trust?

By implementing Elisity Cognitive Trust, your organization can achieve many of the technical requirements of CMMC 2.0 at each level.



Many of the Security Controls at level 1 and 2 involve administrative practices and process implementations that rely on these foundational technical requirements, but are not directly solved for by these practices.

Note that Level 3 practices are not yet established, but will be comprised of a subset of NIST SP 800-172.



FAR Federal Acquisition Regulation **Clause 52.204-21**

NIST National Institute of Standards and Technology **SP 800-171 Security Requirements**

LEVEL 1	**Technical Controls** 52.201-21(b)(1)(i) 52.201-21(b)(1)(ii) 52.201-21(b)(1)(iii) 52.201-21(b)(1)(v) 52.201-21(b)(1)(vi) 52.201-21(b)(1)(x) 52.201-21(b)(1)(xi) 52.201-21(b)(1)(xii) 52.201-21(b)(1)(xiii) 52.201-21(b)(1)(xiv) 52.201-21(b)(1)(xv)		
LEVEL 2	**3.1 - Access Control** 3.1.1, 3.1.2, 3.1.3 3.1.5, 3.1.7, 3.1.12 3.1.14, 3.1.16, 3.1.17 3.1.18, 3.1.20, 3.1.22	**3.5 – Identification and Authentication** 3.5.1, 3.5.2	**3.9 – Personnel Security** 3.9.2
	3.3 – Audit and Accountability 3.3.1, 3.3.2, 3.3.3 3.3.6, 3.3.8, 3.3.9	**3.6 – Incident Response** 3.6.1, 3.6.2	**3.11 – Risk Assessment** 3.11.3
	3.4 – Configuration Management 3.4.1, 3.4.2, 3.4.4 3.4.5, 3.4.6, 3.4.7 3.4.8	**3.7 – Maintenance** 3.7.2, 3.7.6	**3.13 – Systems and Communication Protection** 3.13.1, 3.13.2, 3.13.3 3.13.4, 3.13.5, 3.13.6 3.13.13, 3.13.14, 3.13.15 3.13.16

About Elisity

Cognitive Trust is a cloud-managed, and cloud-delivered solution for identity-based microsegmentation and least privilege access of users, applications, and devices (managed and unmanaged).Our solution architecture leverages pre-existing investments in switching infrastructure by turning your access switches into intelligent policy enforcement points. Cognitive Trust passively gleans and continuously verifies the identity of devices, users, and applications traversing the network, to enforce policies as close to the assets as possible. A wide array of integrations with user, application, and device identity sources is supported so organizations can quickly gain visibility into network assets and traffic flows, assess risks, and begin building policies enforced at OSI L2/ L3/L4, to secure resources from malicious network traffic.

Follow on Twitter and LinkedIn or go to www.elisity.com.

www.elisity.com
info@elisity.com
sales@elisity.com

100 Century Center Ct
Suite 710
San Jose, CA 95112