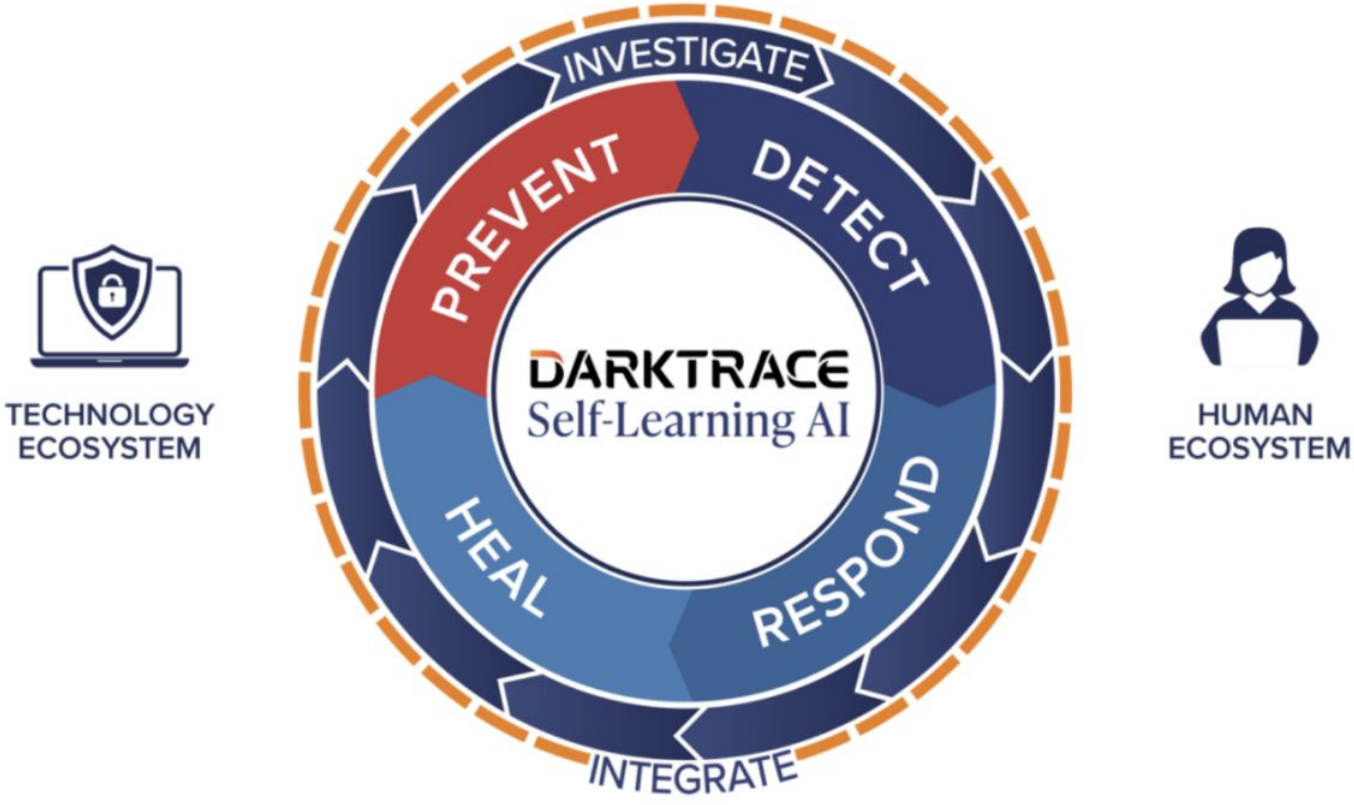

DARKTRACE
©2022 DARKTRACE

Network Security

- Protection against network vulnerabilities
- Visibility into network traffic
- Identification of malicious activities
- Insights for network optimization
- Protect from malicious emails
- Protect from phishing attempts

Detection and Response



Threat Visualizer

Darktrace's Threat Visualizer provides real-time visibility of your entire digital infrastructure, surfacing insights across email, cloud, and the corporate network in a single pane of glass. Cyber-threat visualization and investigation is simplified with this intuitive and easy-to-use graphical interface.

The Threat Visualizer allows the user to 'go back in time' to when an incident took place, and witness events as they unfold in real time. Only the most relevant threats are presented, allowing for incident prioritization, with the option to drill down into any single event in finer detail.

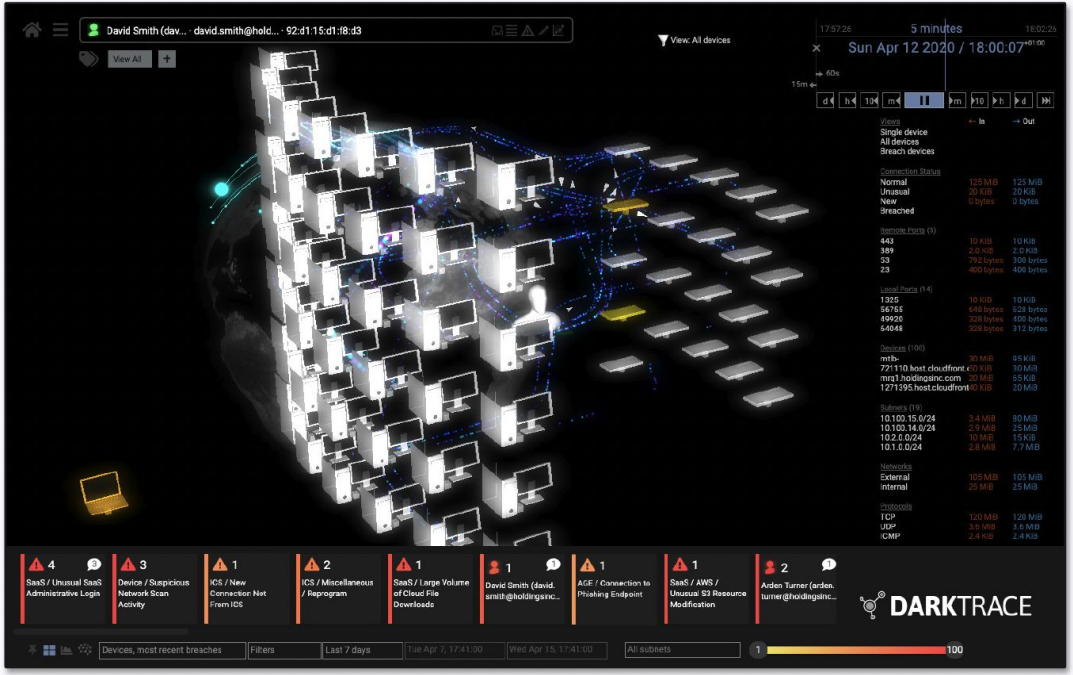
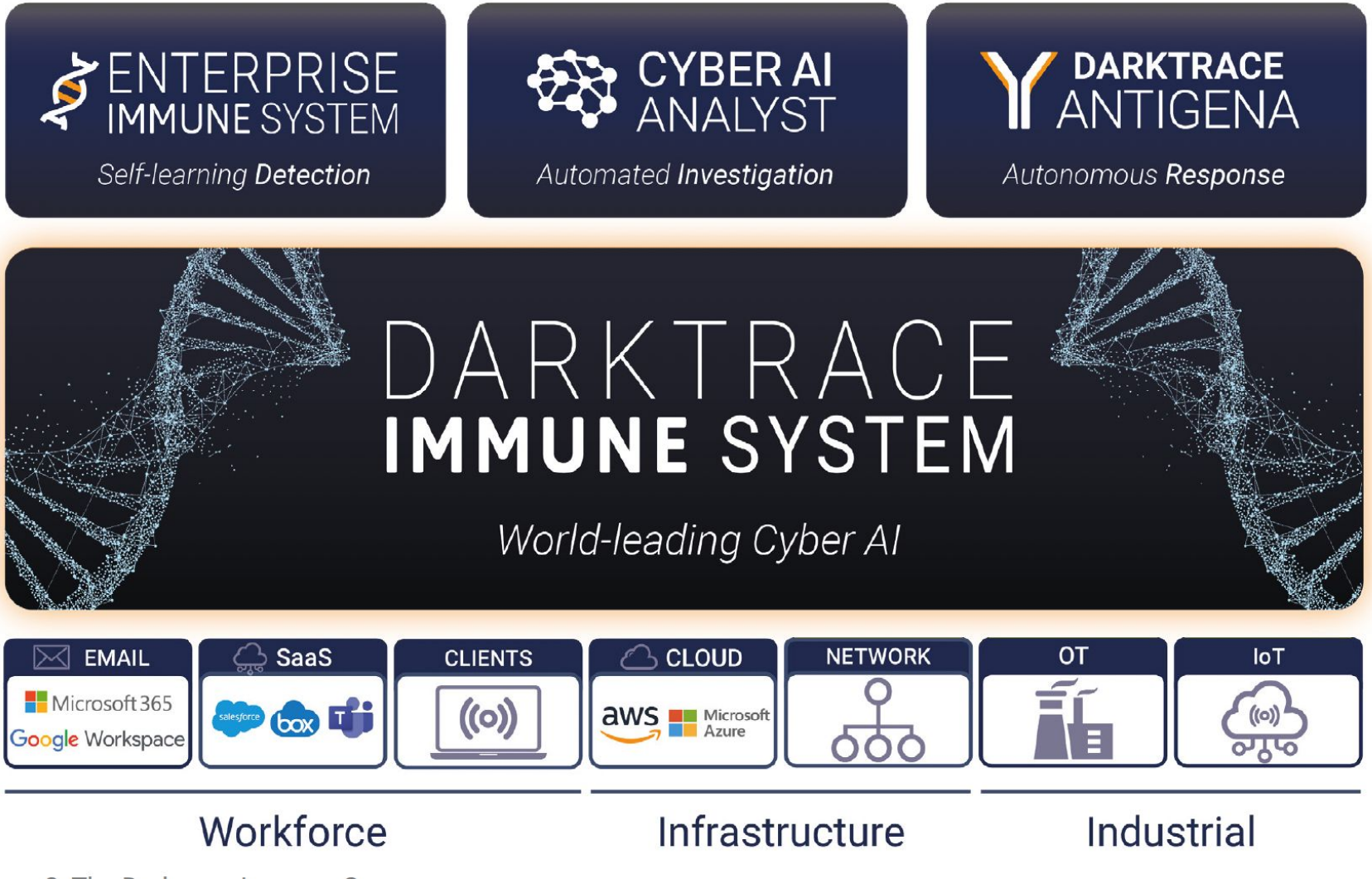
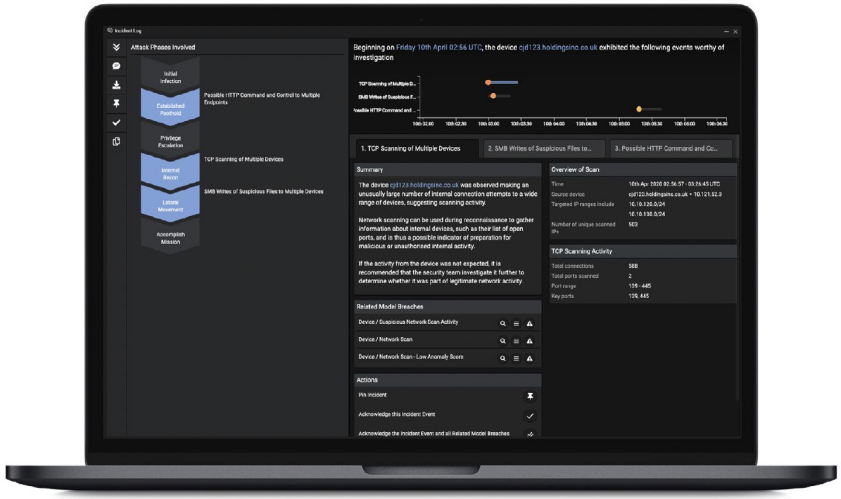


Figure 1: The threat tray at the bottom of the Threat Visualizer surfaces threats identified across the digital business

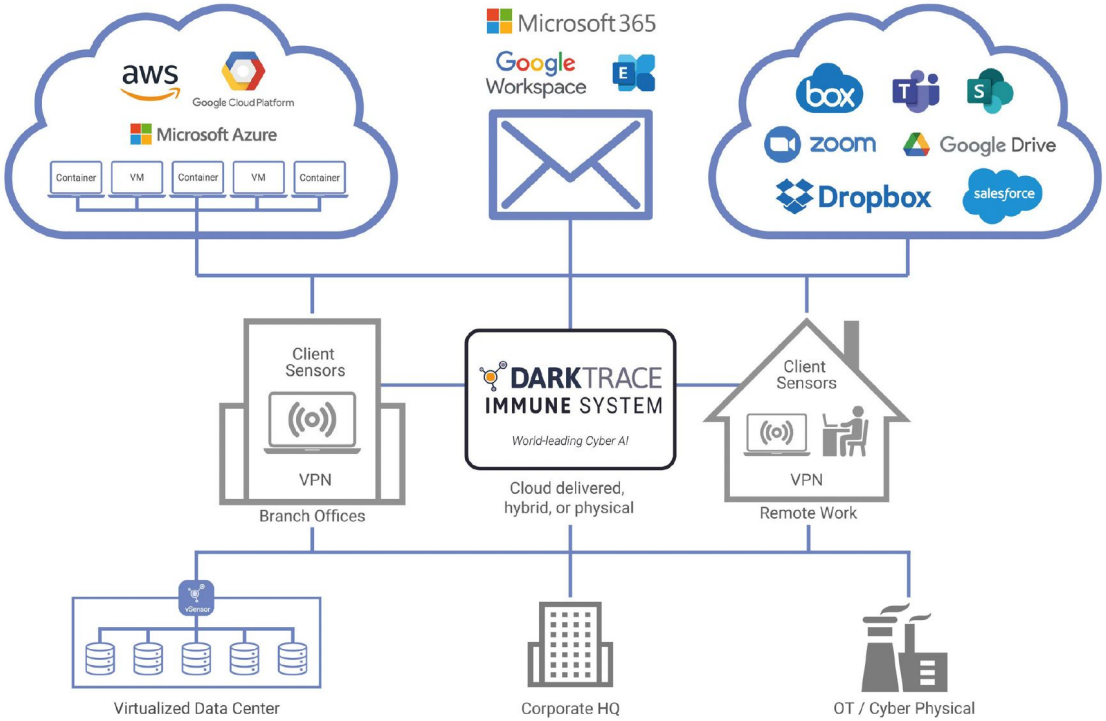

ENTERPRISE IMMUNE SYSTEM
Self-learning Detection
CYBER AI ANALYST
Automated Investigation
DARKTRACE ANTIGENA
Autonomous Response
DARKTRACE
IMMUNE SYSTEM
World-leading Cyber AI
EMAIL
Microsoft 365
Google Workspace
SaaS
salesforce
box
CLIENTS
CLOUD
aws
Microsoft Azure
NETWORK
OT
IoT
Workforce
Infrastructure
Industrial

Cyber AI Analyst



While Darktrace's Immune System and Antigena speed up 'time to detection and response', Darktrace's Cyber AI Analyst drastically reduces 'time to meaning' by fully automating threat investigations for the first time.

Self-Learning Detection & Response

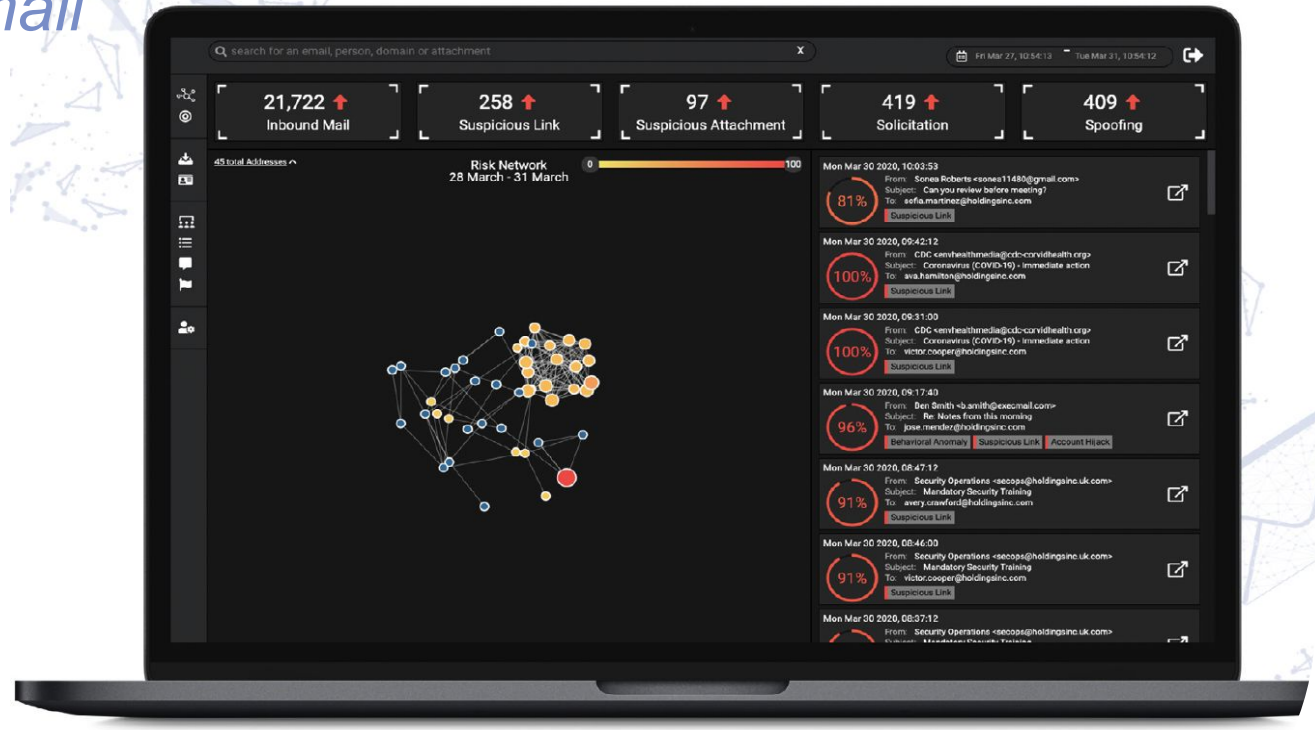


Darktrace's Immune System is a cybersecurity solution designed to unify detection and response across various digital environments. Here are the key points:

1. Unified Protection: Threat actors no longer limit their attacks to a single technology. To defend against this, it's crucial to have unified protections across the entire digital business.
2. Darktrace's Approach: Darktrace's Immune System spans multiple areas, including email, cloud, SaaS applications, industrial systems, endpoints, and the corporate network. It provides insights in a unified view, correlating events and indicators across diverse environments.
3. Single AI Engine: Darktrace's design principle recognizes that a device or user's normal patterns manifest in different parts of an organization. Therefore, a single AI engine correlates related security events in real time.
4. Moving Beyond Per-Technology Security: Traditional per-technology security approaches are no longer effective.

Cyber AI for Email

Antigena Email works by learning the dynamic patterns of every internal and external user, analyzing both inbound and outbound email together with lateral, internal-to-internal communications. By treating recipients as dynamic individuals and peers, Antigena Email can spot subtle deviations from ‘the norm’ that reveal seemingly benign emails to be unmistakably malicious.



Cyber AI for the Internet of Things
Aka Internet of Threats!

To address IoT security, we need to take a bigger picture view – not only looking at vulnerabilities or managed devices, but also complex behaviors that show up across the digital business. With Cyber AI, organizations can monitor 100% of their devices, wherever they are on the network. Learning a normal 'pattern of life' for every device, the
Darktrace Immune System can spot the full range of attacks targeting the Internet of Things

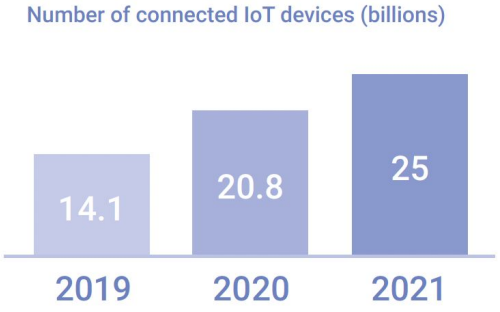


Figure 15: A compromised smart printer and anomalous connections represented with yellow lines

Cyber AI for the Network

Darktrace's self-learning AI is designed to protect the dynamic systems and workers in your organization – no matter where they operate, or the nature of their applications. Unlike legacy on-prem defenses, Darktrace's understanding of normal behavior in the network is augmented by behaviors in cloud, SaaS, and email services as well. This additional context enables Darktrace to detect the full range of cyber-threats in the network, from 'low and slow' data theft and compromised credentials, to machine-speed ransomware.

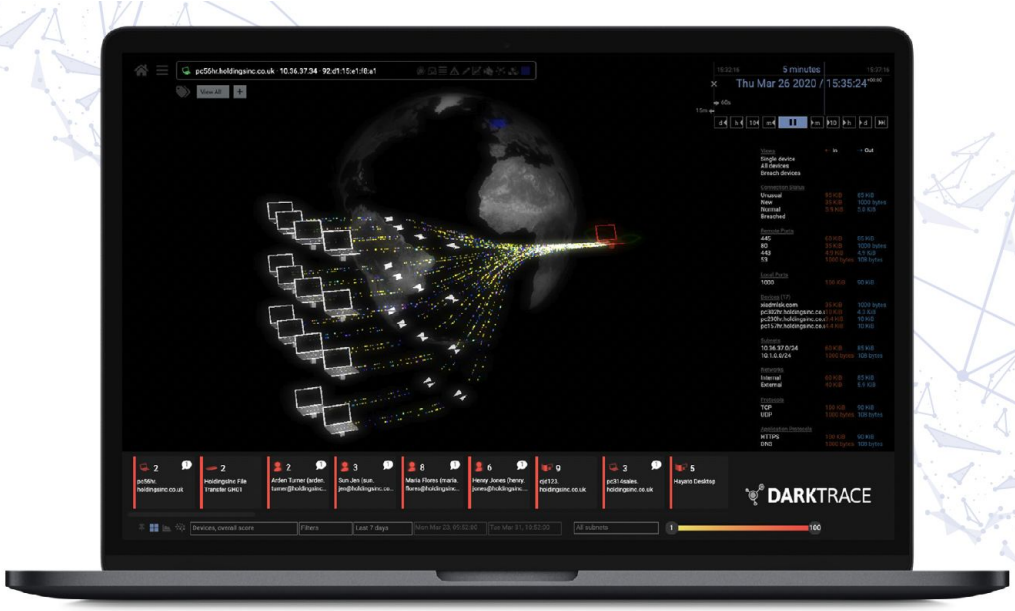


Figure 21: Darktrace detecting a laptop carrying out a network scan

Costs and Savings

- Savings on Cyber Insurance
- Greatly reduce risks of paying ransom for our data due to ransomware
- Saving countless hours of staff resetting compromised passwords and securing accounts
- Eric and I sleep better at night
- Initial costs were over $500,000 per year

Annual costs for 36 months

Pricing Details

The pricing below represents a **36-month** software license based on your full network deployment for your 1,500 IP's, 813 Emails accounts, one medium appliance, and one small email appliance.

Term: **36 months**
Standard payment terms: **Annual in advance** net 30
Discount available if contract signed by: **6/14/24**

Package	List Cost	Discounted Price 87%
Platform Standard City Only (Network and Email)	**$10,685 per month**	**$1,381 per month**

City:
$16,572 / year

Pricing Details

The pricing below represents a **36-month** software license based on your full network deployment for your 10,500 IP's, 11,187 Emails accounts and one X2 appliance.

Term: **36 months**
Standard payment terms: **Annual in advance** net 30
Discount available if contract signed by: **6/14/24**

Package	List Cost	Discounted Price 87%
Platform Standard School Only (Network and Email)	**$74,798 per month**	**$9,669 per month**

BOE:
$116,028 / year

THANKS!

Any questions?